

Towards a Privacy-Preserving Federated *Identity as a Service-Model*

Secure and Privacy-Preserving Identity Management
in the Cloud

Bernd Zwattendorfer

Towards a Privacy-Preserving Federated *Identity as a Service-Model*

Secure and Privacy-Preserving Identity Management
in the Cloud

Ph.D. Thesis

at

Graz University of Technology

submitted by

Bernd Zwattendorfer

Institute for Applied Information Processing and Communications (IAIK),
Graz University of Technology
A-8010 Graz, Austria

May 2014

© Copyright 2014 by Bernd Zwattendorfer

Assessors

Prof. Reinhard Posch

Prof. Kai Rannenberg

Advisor

Dr. Arne Tauber



Sicheres Identitätsmanagement in der Cloud

Doktorarbeit
an der
Technischen Universität Graz

vorgelegt von

Bernd Zwattendorfer

Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK),
Technische Universität Graz
A-8010 Graz

Mai 2014

© Copyright 2014, Bernd Zwattendorfer

Diese Arbeit ist in englischer Sprache verfasst.

Begutachter

Prof. Reinhard Posch
Prof. Kai Rannenberg

Betreuer

Dr. Arne Tauber



Abstract

Identity management related to unique identification and secure authentication of citizens is one of the core concepts required for secure and reliable e-Government. A lot of European countries have already rolled-out different kinds of electronic identity (eID) solutions to enable secure and unique identification and authentication of citizens in online processes. However, these eID solutions are usually tailored to support domestic needs and requirements only, hence they lack in cross-border applicability. To bypass this issue, the European Commission launched the large scale pilot project STORK (Secure Identities Across Borders Linked). STORK aimed on interconnecting different national eID solutions and making the individual solutions interoperable. In this thesis, the main concepts for achieving eID interoperability across Europe and in particular the common middleware approach developed by Austria and Germany are described.

Cross-border services in general and cross-border electronic identity are main pillars to strengthen the European digital internal market to become a more dynamic and knowledge-based society. Another possibility to achieve this is cloud computing. Cloud computing and its flexible business model of consuming IT resources just on demand promises a lot of benefits and advantages, which also governments can benefit from. Since more and more applications (also from the e-Government sector) are migrated into the cloud, secure identification and authentication are also vital in the cloud domain. In this thesis, the topics of cloud computing and electronic identity are combined. For instance, it is demonstrated how highly secure national eID solutions can be used for unique qualified identification and authentication at different cloud service providers. Furthermore, it is illustrated how existing identity management-systems could be moved into the public cloud by still preserving citizens' privacy since privacy is one of the main obstacles when adopting cloud computing. As a sample use case, the complete Austrian eID system is ported into the public cloud in a privacy-preserving manner.

Finally, a new cloud identity management model (*Privacy-Preserving Federated Identity as a Service-Model*) based on the federation between different cloud identity brokers is proposed. In a proof of concept implementation it is shown that federating identity brokers enables users greater flexibility in identity/attribute provider selection by still preserving privacy. The applicability of this approach is further demonstrated by moving parts of the STORK framework into the public cloud without disclosing any sensitive information to the cloud service provider.

Kurzfassung


Identitätsmanagement in Verbindung mit eindeutiger Identifizierung und sicherer Authentifizierung von Bürgerinnen und Bürgern ist eines der Kernkonzepte, welches für ein sicheres und zuverlässiges E-Government benötigt wird. Viele europäische Länder haben bereits unterschiedliche Arten von eID-Lösungen national ausgerollt, die eine sichere und eindeutige Identifizierung und Authentifizierung von Bürgerinnen und Bürgern bei Online-Anwendungen ermöglichen. Diese eID Lösungen sind dabei aber üblicherweise auf die Anforderungen und Bedürfnisse der jeweiligen Ländern zugeschnitten und nicht für eine Anwendung im grenzüberschreitenden Bereich geeignet. Um diesen Missstand zu umgehen, hat die Europäische Kommission das Großpilotprojekt STORK (Secure Identities Across Borders Linked) gestartet. Das Ziel von STORK war, unterschiedliche nationale eID Lösungen miteinander zu verbinden und die individuellen Lösungen interoperabel zu gestalten. In dieser Arbeit werden die wesentlichen Konzepte für das Erreichen von Interoperabilität von eIDs in Europa und im Speziellen die gemeinsame Middleware-Architektur, die von Österreich und Deutschland entwickelt wurde, beschrieben.

Grenzüberschreitende Dienstleistungen im Allgemeinen und grenzüberschreitendes Identitätsmanagement sind wichtige Säulen um den digitalen europäischen Binnenmarkt zu stärken und um eine dynamischere und wissensbasierte Gesellschaft zu werden. Eine andere Möglichkeit, um das zu erreichen, ist Cloud Computing. Cloud Computing und sein flexibles Geschäftsmodell, bei dem IT Ressourcen nur bei Bedarf bereitgestellt werden, versprechen zahlreiche Vorteile, von denen auch Behörden profitieren können. Nachdem immer mehr Anwendungen auch aus dem E-Government Sektor in die Cloud migriert werden, ist eine sichere Identifizierung und Authentifizierung auch in diesem Bereich unverzichtbar. Deshalb werden auch in dieser Arbeit die Themen Cloud Computing und Identitätsmanagement miteinander kombiniert. Zum Beispiel wird demonstriert, wie hochsichere nationale eID Lösungen zur qualifizierten und eindeutigen Identifizierung und Authentifizierung bei verschiedenen Cloud Dienste-Anbietern verwendet werden können. Darüber hinaus wird gezeigt, wie existierende Identitätsmanagementsysteme in eine Public Cloud bei gleichzeitiger Wahrung des Datenschutzes von Bürgerinnen und Bürgern migriert werden könnten, nachdem Datenschutz eines der wesentlichen Hindernisse bei der Verwendung von Cloud Computing ist. Als ein beispielhafter Anwendungsfall wird das komplette österreichische eID-System – bei gleichzeitiger Berücksichtigung des Datenschutzes – in eine Public Cloud konzeptionell migriert.

Letztendlich wird ein neues Identitätsmanagement-Modell für die Cloud vorgestellt (*Privacy-Preserving Federated Identity as a Service-Model*), welches auf der Föderation von unterschiedlichen Cloud Identity Brokern basiert. In einer Implementierung zum Nachweis der Machbarkeit des Modells wird gezeigt, dass die Föderation von Cloud Identity Brokern Bürgerinnen und Bürgern ein höheres Maß an Flexibilität bei der Auswahl von Identitätsdienstleistern bei gleichzeitiger Beachtung von Datenschutzrichtlinien bietet. Die Verwendbarkeit dieses Modells wird weiters demonstriert, indem Teile des STORK Interoperabilitätsrahmenwerks in eine Public Cloud migriert werden, ohne dem Cloud Dienstleister sensible Daten preiszugeben.


Statutory Declaration

I declare that I have authored this thesis independently, that I have not used other than the declared sources / resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

Signature Value	kkHkBXeGFelqArPCNODcrBclnBy3l0nIovmQbAt9tYi7BGg0WXdyH/+TlCmwJlkHwIkgGTeGV6QnBsnQ/2ipfA==	
	Signatory	Dipl.-Ing. Bernd Zwattendorfer
	Issuer-Certificate	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serial-No.	1051612
	Method	urn:pdfsigfilter:bka.gv.at:binaer:vl.1.0
	Parameter	etsi-moc-1.1:ecdsa-sha256@19cl9c9
Verification	Signature verification at: http://www.signature-verification.gv.at	
Note	This document is signed with a qualified electronic signature. According to § 4 art. 1 of the Signature Act it in principle is legally equivalent to a handwritten signature.	
Date/Time-UTC	2014-05-26T13:40:00Z	

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Signaturwert	lnsZFZiy02Z7Pxt/erUHktTqHnuT7gsSB6WxQy7otIN3UPk-j0pKyCx6Ugj26D/C+mgzCWYmm7mAiUGXgVt3Uqg==	
	Unterzeichner	Dipl.-Ing. Bernd Zwattendorfer
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1051612
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:vl.1.0
	Parameter	etsi-moc-1.1:ecdsa-sha256@7a995ced
Prüfinformation	Signaturprüfung unter: http://www.signaturpruefung.gv.at	
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument ist gemäß § 4 Abs. 1 Signaturgesetz einem handschriftlich unterschriebenen Dokument grundsätzlich rechtlich gleichgestellt.	
Datum/Zeit-UTC	2014-05-26T13:40:46Z	

Contents

Table of Contents	i
List of Figures	vii
List of Tables	xi
List of Listings	xiii
List of Schemes	xv
1 Introduction	1
1.1 Motivation and Problem Statement	1
1.2 Structure	2
2 E-Government	5
2.1 E-Government in General	5
2.1.1 Definition	5
2.1.2 E-Government Stakeholders	6
2.1.3 E-Government Stages	7
2.1.4 Benefits and Challenges	9
2.1.5 E-Government Services and Applications	10
2.2 E-Government in Austria	12
2.2.1 Basic Objectives	12
2.2.2 Main Pillars	13
2.2.3 Technical Core Concepts	15
2.2.4 Sample E-Government Procedure	20
2.3 Chapter Conclusions	22
3 Electronic Identity	23
3.1 Electronic Identity in General	23
3.1.1 Identity and Digital Identity	24
3.1.2 Identification, Authentication, and Authorization	25
3.1.3 Electronic Identity (eID)	29
3.1.4 Identity Management	30
3.1.5 Identity Threats	35

3.1.6	Trust Management	35
3.2	Challenges for Electronic Identity	36
3.3	Identity Models	37
3.3.1	Isolated Model	37
3.3.2	Central Model	37
3.3.3	User-Centric Model	39
3.3.4	Federated Model	39
3.4	Single Sign-On and Single Logout	40
3.4.1	Single Sign-On	40
3.4.2	Single Logout	42
3.5	Identity Protocols	42
3.5.1	Terminology	43
3.5.2	SAML	44
3.5.3	OpenID	47
3.5.4	OAuth	47
3.5.5	OpenID Connect	48
3.5.6	WS-Federation	49
3.5.7	CAS	49
3.5.8	Comparison of Identity Protocols	50
3.6	Electronic Identity in Austria	55
3.6.1	The Austrian eID Concept	55
3.6.2	The Austrian Citizen Card Concept	57
3.6.3	The Austrian eID Architecture	60
3.6.4	Identification and Authentication of Austrian Citizens	61
3.6.5	Legal Persons and Electronic Mandates	64
3.6.6	Identification and Authentication of Foreign Citizens	66
3.6.7	A Single Sign-On Architecture	67
3.7	Chapter Conclusions	71
4	Cross-Border E-Government	73
4.1	EU Activities	73
4.1.1	Strategic Commitments	73
4.1.2	Initiatives	76
4.1.3	Programmes	79
4.2	Interoperability	81
4.2.1	Definition	81
4.2.2	The Need for Interoperability	82
4.2.3	European Interoperability Strategy (EIS)	82
4.2.4	European Interoperability Framework (EIF)	83
4.3	Large Scale Pilot Projects	84
4.3.1	STORK	84
4.3.2	STORK 2.0	85
4.3.3	SPOCS	85
4.3.4	epSOS	86
4.3.5	PEPPOL	86
4.3.6	e-CODEX	87
4.3.7	e-SENS	87
4.3.8	Comparison between STORK and epSOS	87
4.4	Chapter Conclusions	88

5	Cross-Border Electronic Identity	91
5.1	Electronic Identities in Europe	92
5.1.1	Belgium	92
5.1.2	Estonia	93
5.1.3	Germany	93
5.1.4	Italy	94
5.2	Possible Approaches for Cross-Border eID	95
5.2.1	Unifying European Electronic Identity	95
5.2.2	Interoperability of European Electronic Identities	96
5.3	Challenges for Cross-Border Electronic Identity	97
5.3.1	Technical Challenges	97
5.3.2	Organizational Challenges	98
5.3.3	Legal Challenges	98
5.4	Early Interoperability Approaches	99
5.4.1	Modinis-IDM	99
5.4.2	FIDIS	99
5.4.3	Guide	100
5.4.4	PRIME, PrimeLife	100
5.4.5	Smart Card Interoperability	100
5.5	Secure Identity Across Borders Linked (STORK)	102
5.5.1	Goals and Challenges of STORK	102
5.5.2	STORK Quality Authentication Assurance Model	103
5.5.3	Basic Models	104
5.5.4	Interoperability Models	106
5.5.5	Architecture and Implementation	110
5.5.6	Integration of STORK in Austria	118
5.5.7	Pilot Applications	122
5.5.8	Cross-Border Legal Identity Management	123
5.6	Chapter Conclusions	125
6	Cloud Computing	127
6.1	Cloud Computing in General	127
6.1.1	Definition and Features	128
6.1.2	Cloud Computing Architectures and Models	129
6.2	Public Cloud Storage Services	131
6.2.1	Software-based Secure Cloud Storage Services	132
6.2.2	Hardware-based Secure Cloud Storage Services	133
6.3	Cloud Computing in E-Government	136
6.3.1	Benefits for E-Government	136
6.3.2	Issues and Challenges for E-Government	137
6.3.3	Evaluation of Cloud Computing Models for E-Government	138
6.3.4	The Public Cloud for E-Government	141
6.3.5	Requirements for E-Government Applications in the Public Cloud	144

6.3.6	Implementation Possibilities for E-Government Applications in the Public Cloud	147
6.4	Cloud Computing in E-Government in Europe	151
6.4.1	Austria	151
6.4.2	Denmark	152
6.4.3	Finland	152
6.4.4	France	152
6.4.5	Germany	152
6.4.6	Ireland	153
6.4.7	Spain	153
6.4.8	United Kingdom	153
6.4.9	Comparison across Europe	154
6.5	Cloud Computing in E-Government beyond Europe	155
6.5.1	America	156
6.5.2	Australia	156
6.5.3	Asia	156
6.6	Chapter Conclusions	158
7	Electronic Identity and Cloud Computing	159
7.1	Cloud Identity Models	160
7.1.1	Identity in the Cloud-Model	161
7.1.2	Identity to the Cloud-Model	161
7.1.3	Identity from the Cloud-Model	163
7.2	Electronic Identity to the Cloud	166
7.2.1	Problem Statement	166
7.2.2	Secure Cloud Authentication using the Austrian Citizen Card	167
7.2.3	Secure Cloud Authentication using the STORK Middleware	169
7.2.4	Lessons Learned	172
7.3	Electronic Identity from the Cloud	173
7.3.1	Problem Statement	174
7.3.2	Cryptographic Building Blocks	174
7.3.3	MOA-ID in the Public Cloud	179
7.3.4	The complete Austrian eID Architecture in the Public Cloud	185
7.3.5	Identity as a Service-Model for Electronic Identities	193
7.4	Chapter Conclusions	195

8	Federated Identity as a Service	197
8.1	Motivation and Problem Statement	197
8.2	Federated Identity as a Service-Model	198
8.3	Privacy-Preserving Federated Identity as a Service-Model	200
8.4	Proof of Concept Implementation	201
8.4.1	Requirements	202
8.4.2	Components	203
8.4.3	Communication Interfaces	204
8.4.4	Process Flows	205
8.4.5	Screenshots	208
8.4.6	Discussion	213
8.5	Applying the Federated IdMaaS-Model to the PEPS Approach	214
8.5.1	Setup	214
8.5.2	Process Flow	215
8.5.3	Discussion	217
8.5.4	Security and Privacy Discussion	217
8.5.5	Practicability Discussion	218
8.6	Evaluation of Cloud Identity Models	218
8.6.1	Evaluation Criteria	218
8.6.2	Evaluation	219
8.7	Chapter Conclusions	223
9	Summary and Conclusions	225
A	List of Acronyms	229
B	List of Publications	237
	Bibliography	241

List of Figures

2.1	E-Government Stakeholders [Brücher and Gisler, 2002]	8
2.2	Sample Layout of an Official Signature	17
2.3	Generic Public Administration Process Flow [Posch et al., 2011]	21
3.1	Digital Identity [Bertino and Takahashi, 2011]	25
3.2	Identification, Authentication, and Authorization [Andersson et al., 2011]	26
3.3	Stakeholders in an identity management system [Bertino and Takahashi, 2011]	31
3.4	Identity Lifecycle [Bertino and Takahashi, 2011; Andersson et al., 2011]	32
3.5	Isolated Model	38
3.6	Central Model	38
3.7	User-Centric Model	39
3.8	Federated Model	40
3.9	Identity Protocols Application	43
3.10	SAML Architecture [Ivkovic and Zwattendorfer, 2009; Lockhart et al., 2008]	45
3.11	The Austrian eID Concept [Tauber et al., 2012]	57
3.12	The Austrian Citizen Card Model [Stranacher et al., 2013c; Hollosi et al., 2014]	59
3.13	The Austrian eID Architecture	60
3.14	Austrian eID architecture for Austrian citizen identification and authentication only [Sumelong et al., 2011]	62
3.15	Process flow of Austrian citizen identification and authentication	63
3.16	Process flow representing a legal person electronically	64
3.17	Process flow of foreign citizen identification and authentication	66
3.18	Current Cross-Sector Authentication [Zwattendorfer et al., 2011a]	68
3.19	Single Sign-On Cross-Sector Authentication [Zwattendorfer et al., 2011a]	69
3.20	Sequence diagram of the SSO process flow [Zwattendorfer et al., 2011a]	70
4.1	Interoperability Levels [European Commission, 2010d]	83
4.2	Circle of Trust in epSOS and STORK [Campari et al., 2010]	88
5.1	Proxy Model	105
5.2	Middleware Model	106
5.3	PEPS-PEPS Interoperability Model [Zwattendorfer et al., 2013c]	107
5.4	MW-MW Interoperability Model [Zwattendorfer et al., 2013c]	108
5.5	MW-PEPS Interoperability Model [Zwattendorfer et al., 2013c]	109
5.6	PEPS-MW Interoperability Model [Zwattendorfer et al., 2013c]	110

5.7	PEPS Architecture [Leitold, 2011]	111
5.8	MW Architecture [Leitold, 2011]	112
5.9	Component Diagram of the STORK Middleware [Zwattendorfer et al., 2013c]	114
5.10	VIDP Critical Interfaces [Zwattendorfer et al., 2013c]	115
5.11	Authentication of Austrian citizens in foreign member states [Tauber et al., 2012]	120
5.12	Acceptance of foreign citizens in Austria [Tauber et al., 2012]	121
5.13	PEPS-MW Model including legal identity representation [Zwattendorfer et al., 2012c]	124
6.1	Cloud Computing Service Models	130
6.2	Cloud Computing Deployment Models	131
6.3	Architecture for securely storing data in the public cloud using the Austrian citizen card [Zwattendorfer et al., 2013d]	134
6.4	Economic benefits of public clouds compared to private clouds [Harms and Yamartino, 2010; Zwattendorfer and Tauber, 2013, 2012c]	142
7.1	Identity in the Cloud-Model [Zwattendorfer et al., 2014]	161
7.2	Identity to the Cloud-Model [Zwattendorfer et al., 2014]	162
7.3	Identity from the Cloud-Model [Zwattendorfer et al., 2014]	163
7.4	Cloud Identity Broker-Model [Zwattendorfer et al., 2014]	164
7.5	Current Situation for Cloud Authentication [Zwattendorfer and Tauber, 2012b]	167
7.6	Authentication at Google and Salesforce.com using the Austrian citizen card [Zwattendorfer et al., 2012a]	168
7.7	Citizen card authentication to Google Apps [Zwattendorfer et al., 2012a]	169
7.8	Extended VIDP architecture supporting eID- based cloud authentication [Zwattendorfer and Tauber, 2012a]	170
7.9	Extended STORK MW Architecture for Cross-Cloud SSO [Zwattendorfer and Tauber, 2012b]	171
7.10	The Austrian eID Architecture in the Public Cloud	186
7.11	Process flow of Austrian citizen identification and authentication in the cloud approach	187
7.12	Process flow representing a legal person electronically in the cloud approach	189
7.13	Process flow representing identifying and authenticating a foreign citizen in the cloud approach	191
7.14	A user-centric and privacy-preserving Identity as a Service-Model for eIDs. [Slamanig et al., 2014]	194
8.1	Federated Identity as a Service-Model [Zwattendorfer et al., 2013a]	199
8.2	Privacy-Preserving Federated Identity as a Service-Model	201
8.3	Implementation Architecture of the Federated Cloud Identity Broker-Model	202
8.4	Authentication process flow	206
8.5	Step 1: Access protected resource	208
8.6	Step 3: Tell me your home broker	209
8.7	Step 4: Forward authentication request	209
8.8	Step 5.1: Show attributes and ask which identity provider or attribute provider to use	210
8.9	Step 5.2: Select individual attributes to retrieve from OpenID provider and attribute provider	210

8.10	Step 6: Redirect to OpenID provider for authentication	211
8.11	Step 7: Authenticate	211
8.12	Step 8: Return encrypted attributes	212
8.13	Step 12: Generate re-encryption key (<i>User</i> → <i>SP</i>)	212
8.14	Step 16: Successful authentication and illustration of transferred identity data and attributes	212
8.15	PEPS-PEPS process flow applying the <i>Privacy-Preserving Federated Identity as a Service-Model</i> [Zwattendorfer and Slamanig, 2013b]	216

List of Tables

3.1	Means of Identification according to [Clarke, 1994; Arora, 2008b]	27
3.2	Advantages and Disadvantages of SSO [Clercq, 2002; Tsolkas and Schmidt, 2010]	41
3.3	Terminology of different identity protocols	43
3.4	Functional evaluation criteria	51
3.5	Organizational evaluation criteria	52
3.6	Technical evaluation criteria	53
3.7	Comparison with respect to functional criteria	53
3.8	Comparison with respect to organizational criteria	54
3.9	Comparison with respect to technical criteria	54
6.1	Evaluation of Cloud Computing Deployment Models [Zwattendorfer and Tauber, 2012c, 2013]	140
6.2	Opposition of requirements and implementation possibilities	148
6.3	Comparison of cloud computing in e-Government across eight European countries [Zwattendorfer et al., 2013b]	155
7.1	Evaluation of the various approaches [Zwattendorfer and Slamanig, 2013a]	183
8.1	Data visible to the individual entities	213
8.2	Comparison of personal data disclosure between the current and the cloud-based PEPS-PEPS approach [Zwattendorfer and Slamanig, 2013b]	217
8.3	Comparison of the individual cloud identity management-Models based on selected criteria [Zwattendorfer et al., 2014]	220

List of Listings

3.1	Sample SAML Assertion	46
-----	---------------------------------	----

List of Schemes

7.1	Redactable Signatures [Zwattendorfer and Slamanig, 2013a]	175
7.2	Anonymous Signatures [Zwattendorfer and Slamanig, 2013a]	176
7.3	Anonymous Credentials [Zwattendorfer and Slamanig, 2013a]	176
7.4	Non-identity-based Proxy Re-encryption	177
7.5	Identity-based Proxy Re-encryption [Zwattendorfer and Slamanig, 2013a]	178
7.6	Fully Homomorphic Encryption [Zwattendorfer and Slamanig, 2013a]	178
7.7	Approach 1: Using Proxy Re-Encryption and Redactable Signatures [Zwattendorfer and Slamanig, 2013a]	180
7.8	Approach 2: Using Anonymous Credentials [Zwattendorfer and Slamanig, 2013a]	181
7.9	Approach 3: Using Fully Homomorphic Encryption [Zwattendorfer and Slamanig, 2013a]	182

Chapter 1

Introduction

Electronic Government (*e-Government*) facilitates governmental and public administrative procedures by the help of information and communication technologies (ICT). For instance, procedures can be processed automatically, which increases efficiency and productivity by saving costs at the same time. In addition, citizens and businesses profit from more comfortable public sector services because information and services can be delivered to citizens and businesses 24/7. They save time and costs because personal presence is not necessary anymore in most cases.

While e-Government was mostly tailored to national activities and more or less isolated solutions over the past years, the European Commission steadily aims on strengthening the European digital internal market by introducing cross-border services. The European Commission puts a lot of efforts into ICT-enabled public administration services to further enable cross-border e-Government and pan-European data exchange. These efforts for achieving pan-European e-Government services are supported by underlying strategic commitments, initiatives, and programmes.

One essential element within a sophisticated e-Government structure and concept is electronic identification (eID) and identity management. Unique identification of citizens is crucial when communicating with governments, especially when sensitive or personal data are involved and need to be processed. This thesis particularly deals with electronic identity. While European eID solutions are fully able to satisfy national demands and requirements for identification and authentication, they usually lack applicability in other countries. One main part of this thesis is to illustrate possibilities for achieving cross-border interoperability of electronic identities within the EU. Furthermore, it is shown how existing identity management and eID systems can be featured by cloud computing concepts. Thereby, existing cloud identity models are elaborated and new models are proposed, which are finally compared and evaluated.

1.1 Motivation and Problem Statement

Electronic Government helps to increase public administration efficiency and provides citizens and businesses user-friendly governmental procedures. To foster the European internal market and to make the EU a more knowledge-based society, the use of cross-border e-Government services is essential. One important part to achieve this is the cross-border acceptance of various heterogeneous national eID solutions within the EU. National eID solutions allow for unique identification and secure authentication of citizens. Many European states have issued electronic identities (eID) to its citizens since the early 2000s. Thereby, smart cards, USB crypto tokens, mobile phone eIDs, or any other high assurance credentials are used. However, due to country-specific requirements (legal, organizational, or technical) existing eID solutions reach their limits in cross-border acceptance and are usually not interoperable. To bypass these gaps for cross-border eID acceptance, the European Commission put a lot of effort in corresponding initiatives and projects. On legal and organizational level, the upcoming new eIDAS regulation

[European Commission, 2012b] will build the fundamental basis. On technical level, the European Commission launched the large scale pilot (LSP) projects STORK (Secure Identity Across Borders Linked) and STORK 2.0 to deal with technical issues on eID acceptance for natural and legal persons. One focus of this thesis is put on STORK. STORK aimed on building an eID interoperability framework to interconnect the heterogeneous eID landscape across Europe. However, such an aim raises new challenges during design and development of the interoperability framework and its integration into national infrastructure. In this thesis, the author describes how these faced challenges have been overcome. In particular, the author focuses on the common STORK middleware (MW) architecture that has been developed together by Austria and Germany and the integration of the STORK concepts into the existing Austrian eID infrastructure. In fact, by the help of STORK EU citizens are capable of authenticating at foreign online applications using the eID issued by their home country.

Identity management plays a key role in e-Government. Cloud computing and its flexible business model of consuming IT resources such as computing power or data storage just on demand is another concept which also governments and public authorities can benefit from. Giving the increasing number of cloud applications, also in the field of e-Government, identity management is also vital in the area of cloud computing. The other focus of this thesis is combining the topics of cloud computing and electronic identity. Considering that, most cloud service providers rely on weak authentication mechanisms such as username/password schemes. While username/password authentication may be sufficient for simple customized applications, cloud applications in more sensitive areas such as in e-Government require more reliable and secure mechanisms. Hence, in this thesis it is discussed how highly secure national eID solutions can be used for unique qualified identification and authentication at different cloud service providers. This offers cloud service providers the possibility to penetrate market areas where higher security requirements for identification and authentication must be met (e.g., the e-Government or e-Health sector).

To combine cloud computing and identity management, usually existing web identity management models are often just mapped to the cloud domain. Besides, several cloud identity management models have emerged. Thereby, the main aim is on operating an identity management system in the cloud due to its benefits. Outsourcing identity management systems to the cloud can bring up several benefits such as higher scalability or cost savings, since no in-house infrastructure needs to be hosted and maintained. Needless to say, the move of a trusted service such as an identity management system into the public cloud can bring up new obstacles – in particular in terms of privacy – since the cloud cannot be considered fully trustworthy. For instance, even when assuming that the identity management system in the cloud works correctly, it still has to be ensured that the cloud provider has no access to private citizen data during the authentication process. To bypass this issue, the author proposes different solutions for deploying identity providers or identity brokers in the public cloud by still preserving citizens' privacy. In particular, the author focuses on eID solutions to be applied in the public cloud in a privacy-preserving manner, since eIDs are the identification means to be used in e-Government scenarios which can include sensitive citizen data. Finally, the author proposes a new cloud identity model where identity brokers in the cloud are federated (*Privacy-Preserving Federated Identity as a Service-Model*). The federation allows both users and service providers greater flexibility in choosing their desired identity provider/identity broker in the cloud by preserving users' privacy at the same time.

1.2 Structure

The remainder of this thesis is structured as follows. Chapter 2 introduces e-Government in general. In particular, the term *e-Government* is defined, involved e-Government stakeholders are identified and their interactions discussed, and benefits and challenges of e-Government are elaborated. Based on this general introduction, e-Government in Austria is explained. Thereby, basic objectives and the main pillars of the Austrian e-Government (the organizational, legal, and technical framework) are elaborated.

Emphasis lies on the technical framework, thus also technical core components, which are deployed and used in Austria, are explained. Finally, the description of a sample e-Government procedure, namely the electronic application and issuance of a criminal record certificate, involving the technical core components rounds up this chapter.

Chapter 3 elaborates on electronic identity. First, identity related terms such as identification, authentication, identity management, etc. are introduced and discussed. It is continued by discussing challenges, which need to be coped with, when dealing with electronic identity. After that, different existing identity models and their advantages and disadvantages are elaborated. The subsequent section briefly overviews the terms single sign-on (SSO) and single logout (SLO). Afterwards, different protocols for exchanging identity and authentication information between entities are evaluated. Finally, electronic identity concepts applied on national level in Austria are discussed. This includes the description of the Austrian citizen card and eID concept as well as the explanation of the technical eID architecture to be adopted for citizen identification and authentication.

Cross-border e-Government and corresponding initiatives and activities on EU level are discussed in Chapter 4. In detail, the first section overviews the EU's strategic commitments, initiatives, and programmes aiming on cross-border e-Government. Thereby, the most important EU activities over the past years and at the present time are described. As a result out of these activities, interoperability can be identified as one of the biggest challenges to implement successful e-Government across borders. Thus, the next section defines interoperability and discusses the European Interoperability Strategy (EIS) and the European Interoperability Framework (EIF), which both aim on facilitating the implementation of interoperable pan-European public services. Finally, the last section details the EU's interoperability efforts by describing different large scale pilot (LSP) projects, which are co-funded by the EU and aim on getting hands-on experience in real-life applications and scenarios in different areas.

Chapter 5 tackles the challenge of eID interoperability across Europe. To illustrate the differences of the existing eID landscape in Europe, four different countries with respect to their eID solutions are described in the first section. Based on that, the two basic possibilities for achieving cross-border eID acceptance, namely either rolling-out a unified electronic identity across Europe or making the existing national eID solutions interoperable, are introduced. Focus of this chapter is put on interoperability, thus challenges on technical, organizational, and legal level, which need to be considered and bypassed when aiming on cross-border eID interoperability, are summarized and listed. The subsequent section briefly describes early eID interoperability approaches that were conducted over the past years. Finally, details on the last and most popular eID interoperability approach STORK, which was co-funded by the European Commission, are given. Details include descriptions of the four different STORK interoperability models, their implementation, as well as the integration of the STORK framework in Austria.

The term *cloud computing* is elaborated in more detail in Chapter 6. First, cloud computing is explained and defined and different cloud computing models are discussed. In the next section, public cloud storage services, which constitute a popular use case of cloud services, and how they can be made more secure are described. Finally, the subsequent sections elaborate on the use and applicability of cloud computing in e-Government in and beyond Europe.

In Chapter 7 electronic identity and cloud computing are combined to illustrate the benefits that can be achieved by adopting cloud computing concepts in identity management. First, different cloud identity models are discussed that have already evolved over time. After that it is shown how various national eID solutions can be used for secure cloud authentication at Software as a Service (SaaS) applications. How existing identity management solutions and systems using eIDs can be ported into the public cloud is shown in the next section. Thereby, the complete Austrian eID system is migrated into the public cloud by keeping the same level of security and privacy for Austrian citizens as in the currently deployed system. Finally, a general user-centric *Identity as a Service*-architecture for eIDs enabling selective attribute disclosure and thus preserving users' privacy is proposed. This model particularly can be applied in semi-trusted environments such as the public cloud.

Finally, in Chapter 8 a new cloud identity management model is proposed. The motivation for this new model and the problem statement is elaborated in more detail in the first section of this chapter. The new so-called *Federated Identity as a Service-Model* is described next, whereas the enhanced version preserving users' privacy by using proxy re-encryption is explained in the subsequent section. A proof of concept implementation of this *Privacy-Preserving Federated Identity as a Service-Model* is described in the next section. Afterwards, the concept of the *Privacy-Preserving Federated Identity as a Service-Model* is applied to an existing use case, namely to the STORK PEPS approach. Finally, all cloud identity models described in Chapter 7 and in Chapter 8 are discussed and evaluated based on selected criteria.

Chapter 2

E-Government

Electronic Government (*e-Government*) is the facilitation of governmental and public administrative procedures by the help of information and communication technologies (ICT). Citizens and businesses get a more comfortable access to public sector information and services, since information and services can be delivered to citizens and businesses 24/7. They further save costs and time, as showing up at public authorities is not necessary any more in many cases. Furthermore, also public authorities profit themselves when providing information and services electronically. Procedures can be processed automatically, which increases efficiency and productivity by saving costs at the same time. In this chapter, an introduction to e-Government is given. Focus is put on e-Government in Austria.

The chapter is structured as follows. Section 2.1 introduces e-Government in general. In particular, the term e-Government is defined, involved e-Government stakeholders are identified and their interactions discussed, and benefits and challenges of e-Government are elaborated. At the end of this section, e-Government services and application domains are addressed. In the subsequent Section 2.2, e-Government in Austria is explained. Thereby, basic objectives and the main pillars of the Austrian e-Government (the organizational, legal, and technical framework) are elaborated. Emphasis lies on the technical framework, thus also technical core components, which are deployed and used in Austria, are explained. Finally, the description of a sample e-Government procedure, namely the electronic application and issuance of a criminal record certificate, involving the technical core components rounds up this chapter.

2.1 E-Government in General

E-Government mainly defines the execution and facilitation of governmental processes by the use of information and communication technologies (ICT). Thereby, e-Government includes electronic procedures between different stakeholders e.g., between public authorities and citizens or businesses as well as between public authorities amongst each other. In this section, a brief overview of e-Government in general, their stages, benefits and challenges, and their application areas are given.

2.1.1 Definition

According to Relyea [2002], the Government Information Technology Services Board [1997] were the first – for this time – that introduced the new term *e-Government*. Although they wrote a lot regarding the benefits and the increased productivity for governments and its stakeholders by providing public services electronically, no clear definition on the term *e-Government* had been given. Therefore, in the following the author gives a couple of definitions on *e-Government* to provide a common understanding of this term.

Moon [2002], for instance, defines e-Government in a broad context, meaning that according to him e-Government *”includes the use of all information and communication technologies, from fax machines to wireless palm pilots, to facilitate the daily administration of government”*. However, not all definitions found in the literature are in accordance with this definition. Fang [2002] sees e-Government more narrow and tailored to Internet applications only. Fang [2002] defines e-Government *”as a way for governments to use the most innovative information and communication technologies, particularly web-based Internet applications, to provide citizens and businesses with more convenient access to government information and services, to improve the quality of the services and to provide greater opportunities to participate in democratic institutions and processes”*. Although both definitions have a different scope in terms of technologies, they both see a facilitation of and thus more efficient governmental processes by the use of e-Government.

Two very concise but still very precise definitions of e-Government were given by Silcock [2001] and Herson [2000]. For Silcock [2001], e-Government *”is the use of technology to enhance the access to and delivery of government services to benefit citizens, business partners and employees”*. In addition, a similar definition is given by [Herson, 2000]: *”E-government is simply using information technology to deliver government services directly to the customer 24/7. The customer can be a citizen, a business or even another government entity”*. These few examples already show that diverse definitions exist in the respective literature. A comprehensive overview and discussion on existing e-Government definitions is given in Yildiz [2007].

Nevertheless, all these definitions have in common that e-Government provides public sector services to

- several stakeholders (e.g., citizens, businesses, other governments, or employees) by using
- information and communication technologies (ICT) by
- providing various benefits to its stakeholders at the same time.

In the following subsections the author gives details on the stakeholders involved in e-Government processes (cf. Subsection 2.1.2), the gained benefits (cf. Subsection 2.1.4.1), and possible applications (cf. Subsection 2.1.5). Thereby, by providing further details on e-Government applications the author limits his scope to Internet- and web-based applications, as they provided the most potential in terms of benefits over the past years. In addition, at this point it is important to mention that e-Government does not only have a technological dimension but also a policy dimension to support and enforce e-Government concepts. Several policy environments in chronological order have been identified by Relyea [2002]. The author will discuss policy aspects – particularly in the European context – in Section 4.1.

2.1.2 E-Government Stakeholders

E-Government affects several stakeholders. The most important ones have already been mentioned, but for the sake of completeness they are [Fang, 2002]:

- Citizens (natural persons)
- Businesses (legal or natural persons)
- Governments (and all corresponding public entities)
- Employees (public servants, etc.)

Nevertheless, Fang [2002] and Yildiz [2007] mention additional e-Government stakeholders in their work. Fang [2002] additionally sees a relationship to non-profit organizations, whereas Yildiz [2007] also refers to civil society organizations. However, in this thesis the author focuses on the four stakeholder groups mentioned before only.

Based on the included stakeholders, e-Government can be classified into different categories. These categories more or less reflect the interactions and communication channels between a governmental organization and another stakeholder. Hence, the following categories, which could also be named vice versa, can be distinguished [Alshehri and Drew, 2010; Brücher and Gisler, 2002; Fang, 2002; Yildiz, 2007]:

G2C (Government-to-Citizen): According to Alshehri and Drew [2010], the main goal of e-Government is to serve citizens. Hence, the G2C model reflects the interaction between governments and citizens. Depending on the maturity of e-Government applications, citizens can either simply get information from public authority websites or are able to run through complete and fully-fledged online e-Government transactional processes. Both citizens and governments can benefit from this electronic communication e.g., as time and costs can be reduced on both sides.

G2B (Government-to-Business): The G2B model includes the communication between governments and businesses. Several services (e.g., tax services, services for renewing or obtaining permits or licenses, etc.) are exchanged between governments and businesses. Referring to Alshehri and Drew [2010], e-Procurement – electronic tendering by the use of ICT – is also one promising example for this category.

G2G (Government-to-Government): G2G includes all communication between governmental entities e.g., the communication between local governments and federal or national governments. Incorporating ICT in their processes can increase efficiency and reduce costs.

G2E (Government-to-Employee): G2E can be seen either as an internal part of G2G or as an external part. G2E refers to the interactions between governments and its employees such as public servants. By the help of ICT, governments can offer their employees several applications facilitating access to internal services such as reviewing salary payment records or other services [Alshehri and Drew, 2010].

Again, as also other stakeholders may be involved in e-Government processes, additional categories can exist. Fang [2002] and von Lucke and Reinermann [2000] mention in their publications also the categories G2N (Government-to-Nonprofit) and N2G (Nonprofit-to-Government) for communications between governments and non-profit organizations. In addition, Yildiz [2007] introduces the category Government-to-Civil Society Organizations (G2SC) for the interaction between governments and civil society organizations. However, these additional categories will not be further considered in this thesis.

All the aforementioned categories can be divided – on a higher abstraction level – into two classes. Brücher and Gisler [2002] and Fang [2002] entitle these two classes as *internal e-Government* and *external e-Government*. Internal e-Government includes the categories G2G and G2E (all government internal communication), whereas external e-Government refers to the categories G2C and G2B (all government external communication). Figure 2.1 illustrates the e-Government categories and classes. For simplicity, G2N, N2G, and G2CS are not shown.

2.1.3 E-Government Stages

E-Government applications, which are provided to stakeholders, can be classified into different stages or interaction degrees respectively. These stages actually describe the level of maturity of an e-Government application. For instance, e-Government applications can just provide information to e-Government

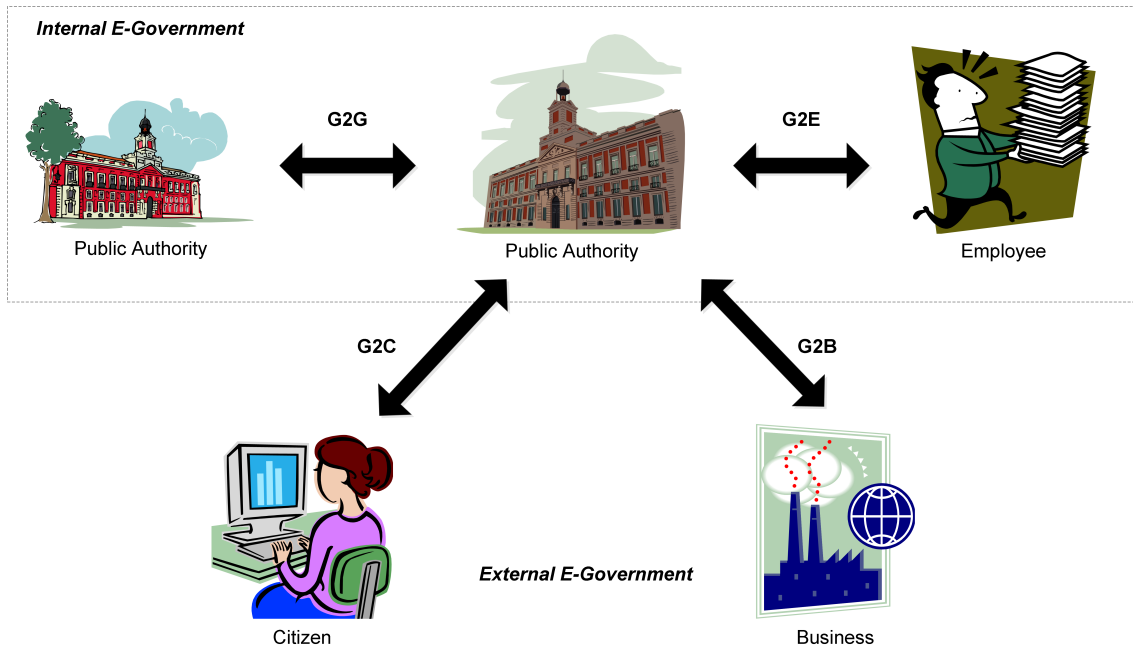


Figure 2.1: E-Government Stakeholders [Brücher and Gisler, 2002]

procedures e.g., which documents need to be provided when filing an application in a public authority's office. Another possibility is a fully-fledged e-Government application, meaning that a complete e-Government procedure – beginning from the application till the delivery of the decision – can be processed completely electronically. In the following, the author describes four different stages or interaction degrees based on the work and models of Brücher and Gisler [2002]; Moon [2002]; Layne and Lee [2001]. They vary actually in the number of stages (mostly between three and five). A review of different stage models in the existing literature is given in Alshehri and Drew [2011]. Most models discussed in these papers rely on four stages, hence the author also has chosen to classify e-Government applications into four stages.

Information stage: In this stage, stakeholders are just able to retrieve information from governmental web sites. Such sites provide information on e.g., which documents are required when filing an application in a government's office, which forms need to be filled out, or which fees may apply.

Communication stage: In this stage, the communication between the government and the stakeholder is focused on. For communication, different channels are possible. Traditional communication channels are e-mail or phone. Newer channels are online forms for inquiries or complaints, or discussion forums.

Transaction stage: The transaction stage can be seen as an enhancement to the communication stage. Besides communication, this stage also includes services arising in an e-Government process. Examples are electronic filing of applications or electronic voting possibilities.

Integration stage: This stage refers to fully-fledged e-Government services or applications, where an e-Government procedure can be processed fully online without breaking media. This means, for instance, that electronic applications are also processed electronically in the back-office and corresponding decisions can be delivered electronically. Thus, during the whole procedure processing paper prints are avoided.

2.1.4 Benefits and Challenges

The adoption of e-Government services has several benefits for the individual stakeholders. Nevertheless, there are also some barriers and challenges that must be come by when implementing or installing e-Government services. In the following subsections, a couple of benefits and advantages, but also challenges are briefly elaborated.

2.1.4.1 Benefits

Hernon [2000] outlines the main benefits of e-Government in one sentence. According to him, e-Government *"delivers services in a manner that is most convenient for the customer, while at the same time allowing government to provide those services at a significantly cheaper cost"*. This means that e-Government has the ability to increase stakeholders' convenience by decreasing costs at the same time. Of course, several additional benefits exist. Based on the work of Alshehri and Drew [2011]; Brücher and Gisler [2002]; Carter and Bélanger [2005]; Müller [2004]; Moon [2002] the most important benefits of e-Government are listed:

- Improved and better service delivery
- More effective and efficient processing (higher productivity)
- Reduction of time need for all stakeholders
- Reduction of costs for all stakeholders
- Increased convenience

Due to the provision of e-Government services, quality of governmental service delivery is improved. Services can be still offered in a traditional way (e.g., paper-based and during office hours) and in addition electronically [Müller, 2004]. The use of ICT enables more effective and efficient processing of bureaucratic procedures [Brücher and Gisler, 2002; Moon, 2002] because e.g., procedures can be automatically processed. At the same time, this reduces time and costs for governments as well as citizens or businesses [Brücher and Gisler, 2002]. Especially citizens and businesses benefit from the 24/7 availability of services, which clearly increases stakeholders' convenience. In addition, governments are also able to reduce the number of employees required to be present during office hours [Moon, 2002].

2.1.4.2 Challenges

The implementation of successful e-Government services is sometimes not easy to achieve. Several challenges or barriers must be overcome. In the following, some examples for such challenges or barriers are listed. Furthermore, challenges may arise in different areas and levels e.g., on technical, organizational, or legal level. In the following, possible challenges or barriers based on these three levels are listed. A very detailed list of barriers can be found in Ebrahim and Irani [2005].

Technical challenges/barriers: Alshehri and Drew [2011] and Brücher and Gisler [2002] see technical challenges especially in the heterogeneity of IT infrastructures. Countries, which have a federated structure, generally have no common guidelines or regulations for individual municipalities or cities, how their IT infrastructure should look like. Moreover, federal states, municipalities, or cities are usually free to choose their desired technologies [Brücher and Gisler, 2002]. Hence, integration of different technologies and systems fail due to interoperability issues.

According to Alshehri and Drew [2011] and Moon [2002], security constitutes the biggest technical challenge for the implementation of e-Government services. As e-Government deals with

sensitive and personal data, such data must be particularly protected from unauthorized access. Although appropriate technological measures such as electronic signatures or encryption mechanisms exist, security challenges may still be present.

Organizational challenges/barriers: Even if challenges can be solved by technical means, still organizational barriers can exist. Alshehri and Drew [2011] name a couple of organizational barriers in their publication. Referring to them, missing support of the top management can be an issue. Support and acceptance of the adoption of e-Government services are essential for the implementation of e-Government in general. Missing acceptance can easily lead to financial bottlenecks during implementation.

Weak collaboration and cooperation between involved stakeholders or lack of technological staff are further barriers according to Alshehri and Drew [2011] and Moon [2002]. If not all stakeholders are working together, personnel resources and budget can be wasted. In addition, qualified and technical-skilled personnel are required to develop, setup, and maintain e-Government services [Alshehri and Drew, 2011]. Furthermore, qualified staff is necessary to support training and education programmes for governmental employees. Beyond these challenges, Alshehri and Drew [2011] also see different cultures and social skills as a barrier.

Legal challenges/barriers: Brücher and Gisler [2002] see the equal treatment of stakeholders as one major legal challenge. In contrast to the private sector, where companies can focus on specific customer groups, in the public sector such specialization is not possible [Brücher and Gisler, 2002]. Governments need to provide their services to all social classes e.g., including elderly or disabled people. This requirement must be also fulfilled in e-Government services.

Another legal challenge is privacy [Moon, 2002]. Appropriate policies, regulations, or laws must exist that only a minimum required amount of data are processed in e-Government services [Alshehri and Drew, 2011]. For instance, in the European Union the data protection directive [European Parliament and Council, 1995] constitutes such a law for protecting citizens' privacy¹.

2.1.5 E-Government Services and Applications

E-Government services and applications have various facets. Nearly every existing and paper-based governmental service can be modeled electronically. In most cases, e-Government services can also be orchestrated by different basic services to assemble larger services implementing more sophisticated business processes. Examples of such basic services are electronic signature (e-Signature) services or electronic identification (eID) services. Higher sophisticated or more complex services, which involve different basic services, are e.g., e-Voting or e-Procurement. In the following, the author briefly enumerates e-Government basic services as well as possible application domains. Details on existing e-Government services and application domains can be found e.g., in Heindl [2003] or Gronau et al. [2010].

2.1.5.1 Basic Services

In this subsection, important e-Government basic services, which are frequently re-used to assemble larger and more complex services, are briefly elaborated.

e-Services: In the context of this thesis, e-Services is referred to as the generic term for electronic services provided by public authorities or bodies. Usually, governments or public authorities provide some kind of e-Catalogue, where e-Services can be registered, discovered, or linked.

¹The European Commission is currently working on a new data protection regulation [European Commission, 2012a], which will supersede the existing data protection directive probably in 2016.

e-Documents: Within e-Government processes, electronic documents (e-Documents) frequently need to be exchanged in transactions between stakeholders and the government. Depending on specific requirements, e-Documents in the context of e-Government might have a special format or support specific functionality such as electronic signatures or encryption.

e-Signature: Electronic signatures are a valuable means to ensure integrity, authenticity, and non-repudiation of e-Documents. Because of their properties, e-Signatures are applied in nearly every e-Government transaction, which requires authentic data by ensuring integrity at the same time.

eID: Like traditional paper-based IDs, electronic IDs (eIDs) allow for unique identification and secure authentication in electronic processes. Especially in e-Government, unique identification is essential as sensitive data are processed in many cases.

2.1.5.2 Application Domains

This subsection briefly discusses application domains where e-Government basic services are applied. The discussed application domains have neither hierarchical character nor can they fully be treated isolated. Furthermore, the list is not intended to be exhaustive and should just provide the reader some insights into possible application domains of e-Government.

e-Participation: E-Participation (electronic participation) includes all electronic procedures, which enables citizen involvement into political decision making processes. Software applications enabling e-Participation are e.g., wikis, social networks, web forums, or reputation and online petition systems.

e-Voting: In e-Voting (electronic voting), electronic means are used to place votes or to count votes. Thereby, the term e-Voting includes both voting machines used in polling stations or elections carried out over the Internet (i-Voting).²

e-Delivery: E-Delivery (electronic delivery) focuses on the reliable and secure transfer of electronic data (or e-Documents) between entities or stakeholders respectively (in the context of e-Government). E-Delivery mechanisms e.g., provide public authorities possibilities to receive approval that a certain e-Document was successfully delivered to and was received by the intended recipient.

e-Procurement: E-Procurement (electronic procurement) is the procurement of goods and services using ICT. The process of e-Procurement is usually divided into two phases, the e-Tendering (electronic tendering) and the e-Purchasing (electronic purchasing) phase. In e-Procurement, all involving phases are modeled electronically.

e-Justice: e-Justice (electronic justice) has the goal to facilitate administrative procedures of judicial systems by using ICT. E-Justice includes the communication between courts and public authorities as well as professional representatives (lawyers, notaries, etc.), citizens, and businesses.

e-Health: E-Health (electronic health) refers to electronic processes that support healthcare. E-Health can actually be seen as a different domain to e-Government. However, both domains use similar concepts and thus several e-Government concepts such as eID can also be applied in the e-Health domain.

²The terms e-Participation and e-Voting can also be subsumed under the term e-Democracy.

2.2 E-Government in Austria

Austria has been working on appropriate e-Government solutions for a couple of years and has invested significant efforts in their development. The main aim of these efforts is to support Austrian citizens and businesses in online procedures and thereby facilitating access to public authorities or public administrations with the help of ICT. In addition, also internal governmental processes should be facilitated and unnecessary burdens or media-breaks should be reduced. Thus, Austria is one of the leading countries in e-Government adoption since many years. This leading position has been manifested by several e-Government benchmarks [Wauters et al., 2007; Lörincz et al., 2010; Tinholt et al., 2012]. In this section, the author describes e-Government in Austria on organizational, legal, and technical level. However, the focus of this section lies on technical core concepts, which basically lead to this upfront position [Posch et al., 2010].

2.2.1 Basic Objectives

Austria follows a well-defined and sustainable e-Government strategy, which is aligned along several initiatives and regulations of the European Union. The main strategy dates back to the year 2000 and is based on agreements achieved in the EU summits in Feira [European Council, 2000b] and Lisbon [European Council, 2000a]. In these summits, common objectives such as online availability of main governmental services by the year 2005 had been agreed. These agreements have been anchored in the Austrian government program to join forces and to stimulate e-Government in Austria. Several EU initiatives dealing with e-Government agreements to strengthen the European internal market have followed. Several European initiatives will be discussed in Section 4.1.

All these initiatives have yielded according amendments of the Austrian e-Government strategy and implementations based on well-established information and communication technologies. However, the main vision for successful and sustainable e-Government in Austria, which has been elaborated in the year 2000, is still valid. This vision envisages that all Austrian citizens and businesses must be able to conduct all governmental processes and transactions electronically, fast and in a simply manner, and without any special or detailed knowledge on technology [Schüssel and Morak, 2005].

From this overall vision and from the general Austrian e-Government strategy, the following basic objectives of e-Government solutions in Austria can be derived [Plattform Digital Austria, 2008]:

- Assure trust in provided services by appropriately informing citizen on the security-, privacy-, and transparency-preserving features of provided solutions.
- Include all relevant authorities to avoid silo solutions, i.e. separated solutions of different authorities, which hinder interoperability between them.
- Iteratively transform services to achieve complete transactional and integrated services without media breaks (cf. Section 2.1.3).

One major aim of the Austrian e-Government strategy is to inform citizens about the availability and the maturity of electronic governmental services. This way, citizens should be able to recognize the added value such as higher comfort and flexibility, and should also gain an appropriate level of trust in these services. Therefore, it is important that e-Government applications are easily accessible and follow common and approved approaches to assure an adequate degree of usability. Moreover, e-Government applications should be easily locatable by citizens and any existing barriers that threaten access to services should be removed. The use of existing and well-established standards helps to decrease such barriers. Another important criterion with respect to citizen information is security. Security and privacy are essential to assure trust in governmental online services that usually transfer or process sensitive data.

Citizens must believe and give credit to the same level of trust for online services as they do for traditional paper-based procedures. Citizens must be appropriately informed about the strengths and security features of used technologies.

Another main pillar of the Austrian e-Government strategy constitutes the inclusion of all relevant authorities. This requirement involves the implementation of e-Government on different public administrative levels. This means that e-Government should be implemented on national, regional, and local level involving federal states, municipalities, and cities. All levels must cooperate with each other to guarantee consistency and to avoid silo solutions. Existing infrastructures should be conjointly re-used to benefit as much as possible from the advantages offered by e-Government.

Existing e-Government infrastructures and solutions should not be abandoned, but moreover integrated into new and emerging services. The aim is to develop fully-fledged transactional and integrated solutions and services without media breaks. This means that citizens should be able to electronically apply for governmental procedures and at the same time receive the results without the need for paper-based post mail. To achieve this goal, governmental services should be transformed iteratively to electronic pendants. This means to set up simple and pure informational services at the beginning and to steadily increase the complexity and sophistication of these services. The final goal is to roll out complete transactional and integrated services in the end (cf. Section 2.1.3).

2.2.2 Main Pillars

The step-wise transformation and implementation of transactional services necessitates continuous amendments that are facilitated by fast technological improvements. The fulfillment of this requirement can be facilitated by a modular design of services and by the definition of appropriate interfaces. Besides the definition of technological concepts and solutions, the realization of a comprehensive e-Government strategy requires the implementation of long-term and fundamental structures in several areas. By the help of an e-Government strategy, concepts and guidelines are worked out, which need to be further implemented step-wise. To implement those concepts, a general framework, not only on technical but also on organizational and legal level, has to be implemented. This guarantees the necessary basis for a successful and sustainable e-Government infrastructure.

The following subsections briefly describe the main pillars of the Austrian e-Government strategy (organizational, legal, and technical frameworks) that have been defined to guarantee successful e-Government solutions in Austria.

2.2.2.1 Organizational Framework

To achieve the ambitious objectives defined by the Austrian e-Government strategy, efficient and collaborative organizational structures are required. Therefore, Austria relies on a dynamic and flexible organizational model. The most important entities of this organizational model according to Plattform Digital Austria [2008] are the:

- E-Government Platform
- E-Cooperation Board
- Plattform Digital Austria
- E-Government Innovation Center

The *E-Government Platform* consists of the Austrian vice chancellor, several ministries, the president of the Austrian Federal Economic Chamber, the presidents of social insurance carriers, and governing actors of e-Government working groups, which have strong relations to the federal states in Austria. The

major objective of this platform is the organization of e-Government initiatives and activities in Austria on political level.

The *E-Cooperation Board* is a collaboration of ministries, federal states, associations of Austrian cities and towns, and advocacy groups. The E-Cooperation Board coordinates ongoing work in the field of e-Government and determines the responsibility for carrying out e-Government implementation plans.

The *Platform Digital Austria* constitutes the coordination and strategy council of the federal government for e-Government in Austria. All e-Government projects converge in this council. Hence, this council represents one of the central entities of the Austrian e-Government strategy.

The *E-Government Innovation Center* has been founded in parallel to the Platform Digital Austria. It is responsible for technology observation and technical innovations with respect to e-Government. Furthermore, federal states, cities, or municipalities are supported in their e-Government activities. In addition, the E-Government Innovation Center has been a partner in several European-wide e-Government projects such as the EU large scale pilot projects (cf. Section 4.3).

2.2.2.2 Legal Framework

Besides a mature organizational structure, a consistent legal framework represents a relevant factor for successful and sustainable e-Government in Austria. The main pillar of the Austrian legal framework for e-Government constitutes the Austrian E-Government Act [Federal Chancellery, 2008], which has been especially stipulated according to the Austrian e-Government strategy. However, the legal framework is not based on the Austrian E-Government Act only, but includes several additional relevant laws and regulations. Basically, the main legal framework components of the Austrian e-Government are the:

- E-Government Act ("E-Government Gesetz")
- Signature Act ("Signaturgesetz")
- General Administrative Procedures Act ("Allgemeines Verwaltungsverfahrensgesetz")
- Service of Documents Act ("Zustellgesetz")

Within the European Union, Austria was one of the first Member States that has adopted a comprehensive e-Government law [IDABC eGovernment Observatory, 2006]. The *Austrian E-Government Act* [Federal Chancellery, 2008] had come into force on March 1, 2004 and was amended on January 1, 2008. The three main principles of the Austrian E-Government Act are freedom of choice regarding citizens' interaction with the government and public authorities, guaranteeing security and data protection, and assurance of barrier-free access to e-Government services for all citizens.

The *Austrian Signature Act* [Federal Chancellery, 2010c] constitutes the implementation of the EU Signature Directive [European Parliament and Council, 1999b], which was published by the European Commission in 1999. This directive specifies a common legal framework for electronic signatures in the European Union. In general, the Austrian Signature Act distinguishes between *simple*, *advanced*, and *qualified* electronic signatures. Qualified electronic signatures are legally equivalent to hand-written signatures according to the EU Signature Directive. Qualified electronic signatures play a major role in the Austrian eID concept, as they are also used for secure electronic authentication of citizens in online procedures (cf. Section 2.2.3.1 and Section 2.2.3.3).

The *General Administrative Procedures Act* [Federal Chancellery, 2010b] regulates procedures of nearly all public administrations and authorities in Austria. For instance, this act regulates how citizens can contact public authorities. In electronic processes, this can be done e.g., via e-mail or web forms.

The *Service of Documents Act* [Federal Chancellery, 2013] defines the postal and electronic delivery of authoritative documents to citizens. Similar to the paper-based world, in electronic delivery a differentiation between verifiable and non-verifiable delivery exists. In a verifiable delivery scenario the

recipient confirms the receipt of a document by her signature. In Austria, verifiable deliveries can also be carried out using electronic means. Some more details on electronic delivery in Austria will be given in Section 2.2.3.4.

2.2.2.3 Technical Framework

The technical framework to be applied for e-Government in Austria is based on modern and approved information and communication technologies. By the help of these technologies, data and message exchange between citizens, businesses, and public authorities can be organized in a secure and transparent way. The technical core component within the Austrian e-Government strategy constitutes the Austrian citizen card concept (cf. Section 3.6.2). The Austrian citizen card [Leitold et al., 2002] is an electronic ID (eID), which allows for secure and reliable authentication of citizens in online procedures and enables citizens to create qualified electronic signatures.

Smart cards are currently a popular technology that can be used to practically implement the Austrian citizen card concept. National health insurance cards (e-card)³, which are applicable as citizen card, have been rolled out nation-wide in 2005 [Federal Ministry of Health, 2013]. However, the Austrian citizen card concept is technology agnostic, hence alternative implementations are also possible. An increasing number of citizens use the Austrian mobile phone signature [Orthacker et al., 2010]. In this solution, citizen card functionality is not implemented by a smart card but by a central server with attached hardware security module (HSM). Citizens authorize access to personal data stored and processed in the central HSM by means of a two-factor authentication with the help of their mobile phones.

In general, Austria tries to guarantee technology neutrality in its e-Government solutions. This neutrality is guaranteed by open interfaces and easy ex-changeability of single modules. One major aspect thereby is the use of international standards. On the one hand, such standards ensure interoperability between cross-domain applications of public authorities. On the other hand, well-established and proven standards ascertain a high level of security and privacy for citizens.

2.2.3 Technical Core Concepts

One reason for Austria's leading position in e-Government are several open source components, which can be re-used by public authorities to support their services. One example of such a core component is the citizen card software (CCS), which facilitates the use of the Austrian citizen card for online applications. In this section, several technical concepts facilitating e-Government adoption in Austria will be described according to Posch et al. [2010].

2.2.3.1 Electronic Signatures

In traditional, paper-based governmental processes signing a document by hand usually expresses a declaration of intent. Of course, declarations of intent also play an important role in e-Government scenarios and processes. In online processes, such declarations are modeled by the use of electronic signatures. This subsection gives a brief overview on electronic signature concepts and implementations adopted within the Austrian e-Government strategy.

Citizen Signature To ensure authenticity of an electronic document, electronic signatures must be linked to the data to be signed in such a way that manipulations on the signed document can be recognized. Several cryptographic signature methods (e.g., RSA [Denning, 1984] or ECDSA [Johnson and Menezes, 1998]) are able to fulfill this requirement and thus are basic building blocks for reliable and authentic message exchange between different entities or e-Government stakeholders respectively.

³<http://www.chipkarte.at>

Electronic signatures play an important role in Austria but also in the European e-Government context. Thereby, the EU signature directive [European Parliament and Council, 1999b] defines the legal framework for electronic signatures in the EU. According to this directive, *advanced electronic signatures* require the following properties. First, they require the identification of the signatory and, second, the recognition of any alteration on electronically signed data. Cryptographic material for signature creation must be kept under sole control of the signatory (citizen). Moreover, the EU signature directive defines so-called *qualified electronic signatures*. In fact, qualified electronic signatures are advanced electronic signatures, which are created by the help of a *secure signature creation device* (SSCD) and are based on a qualified certificate. Such qualified electronic signatures are legally equivalent⁴ to handwritten signatures according to this directive and thus can be used as evidence in court procedures. Thereby, the SSCD ensures technologically that the signature creation data are appropriately protected from misuse.

On legal level, the implementation of the EU signature directive constitutes the Austrian Signature Act [Federal Chancellery, 2010c]. On technological level, the Austrian citizen card is the means for allowing citizens to create qualified electronic signatures. Currently, implementations of the Austrian citizen card based on smart cards and mobile phones exist. Software components facilitating the creation of electronic signatures using the Austrian citizen card are called *citizen card software* (CCS). The author skips a detailed discussion of the Austrian citizen card and the citizen card software at this passage and refers to Section 3.6.2 for details.

Official Signature In traditional governmental procedures public authorities usually have to sign authoritative documents and additionally put an official seal on them. As an electronic pendant, the Austrian e-Government initiative introduced the so-called *official signature*. The official signature has been especially designed for public authorities and ensures non-alterations and authenticity of electronically signed documents of public authorities. Furthermore, the official signature should clearly show that the electronic document comes from and has been signed by an official public authority.

The rules for applying an official signature are regulated in the Austrian E-Government Act [Federal Chancellery, 2008]. Actually, the law is that strong that even print-outs of officially-signed electronic documents have the same probative force as their electronic copies.

Basically, the official signature constitutes an advanced electronic signature, whereby the corresponding signature certificate includes a special attribute that marks the affiliation to a public authority. This attribute is used to recognize official signatures in electronic verification processes. However, official electronic documents should also be easily recognizable by citizens or businesses, hence particular information must be provided on the official document. Therefore, every officially signed document should include a visualization of the official signature. The visualization – for instance – includes an emblem of the federal state or municipality that issued the document, and additionally must contain supplementary information that the signature has been created by an official authority. Finally, the visualization must contain information where and how the signature can be verified.

To facilitate recognition of official signatures by citizens, as part of the Austrian e-Government strategy a convention for a uniform appearance of official signatures has been created. This convention [Tauber and Karning, 2013] recommends to illustrate an official signature as table. Figure 2.2 shows an example of an official signature. Besides the emblem of the public authority, the table contains the textual information that the signature has been created by an official authority. Additionally, the table contains details on the electronic signature and information for a signature verification.

To facilitate the creation of official signatures for public authorities, several open source modules are available. For instance, the module MOA-SP/SS (Module für Online Applikationen – Signaturprüfung und Server-Signatur)⁵ enables the creation and verification of XML signatures [Bartel et al., 2008] and

⁴Exceptions in Austria are however family matters, for instance, drawing up a will still requires personal communication with a notary.

⁵<https://joinup.ec.europa.eu/software/moa-idspss/>

Signaturwert	U3AB1Q+4VFO4L/TWuyrt1HIN27mMPa4D618yBAJ3xXpJHhVmo7ynEslAzc36DVIrYAKByADHa6/fub1Rty1o oi/DGOI3p93T+B1r0tGnVc4AQIh+JSoo3VbqGK/eygtQgU4gOJzzVys6qMkEBTnhV1EJbqX11eKk1N3xR8qh Pjghuv/KXJZxp/61XStHfb9ym/W6DpVg6Pwy9s2NTLsIqQ6UKk26t9VOXbaP1Hr5Uhh1K1NIMUt+Up7UGnos yOG6Nx81vFTBveWSAVYWZj1+IFe2OCXt4JrvnrE19leBP7IY4M6BPdRnpXpcS1YmaqAOJH+tkMCX+Y63PD K36jpw--	
	Datum/Zeit-UTC	2013-09-27T13:49:35+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C-AT
	Serien-Nr.	465297
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	ets1-bka-moa-1.0
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at . Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

Figure 2.2: Sample Layout of an Official Signature

CMS (Cryptographic Message Syntax) [Housley, 1999] signatures. For creation, either software- or hardware-based certificates (e.g., from an HSM) can be used. MOA-SP/SS can be accessed via a well-defined Java-API or via web service (WS).

Another software module for official signatures is PDF-AS (PDF Amtssignatur)⁶. PDF-AS constitutes an open source Java library that can either use MOA-SS or the Austrian citizen card for creating official signatures on PDF documents. The visualization layout can be individually configured by the public authority in the library but is, however, aligned to the standard layout described before.

Signature Verification One specific advantage of electronic signatures compared to traditional handwritten signatures is the non-ambitiously technical verifiability. This can be achieved by applying appropriate cryptographic mechanisms on the signed document, if in addition the signing certificate – which is usually public – is available. Thereby, signature verification allows to check the document's integrity, authenticity, and guarantees non-repudiation. Non-repudiation means that the signatory cannot deny having signed the document.

To allow citizens and businesses the possibility to verify signed electronic documents, several open source components have been developed within the Austrian e-Government initiative. In addition, a central signature verification service⁷ is operated by the *Austrian Regulatory Authority for Broadcasting and Telecommunications*⁸. This service allows verification of signed documents of arbitrary signature formats such as XML signatures [Bartel et al., 2008] or PDF signatures [E-Government Innovation Center (EGIZ), 2013]. Details on the architecture and the implementation of this service can be found in Zefferer et al. [2011].

2.2.3.2 Encryption

Besides signature capabilities, the Austrian e-Government technical framework includes functionality for the protection of confidentiality of data. Again, this functionality can be used through the Austrian citizen card. Besides key pairs for signature creation, an additional key pair is stored on the card, which can be used for the secure encryption and decryption of data. Thereby, the public encryption keys of every Austrian citizen are available through a central LDAP directory. Hence, data can be encrypted for each Austrian citizen and stored confidentially. [Zwattendorfer et al., 2013d]

The software that facilitates the use of encryption and decryption functionality of the Austrian citizen card is CCE (Citizen Card Encrypted)⁹. CCE is a platform-independent and open source software developed by A-SIT (Secure Information Technology Center - Austria)¹⁰. Basically, CCE allows for the

⁶<https://joinup.ec.europa.eu/software/pdf-as/>

⁷<https://pruefung.signatur.rtr.at>

⁸<https://www.rtr.at>

⁹<https://joinup.ec.europa.eu/software/cce/description>

¹⁰<http://www.a-sit.at>

encryption and decryption of arbitrary data and the management of files or directories both for single and multiple users.

For file and directory encryption and decryption, CCE relies on hardware-based keys, which are stored on the Austrian citizen card. However, also software-based keys can be used within CCE. Particularly, the use of the Austrian citizen card enables a highly secure and confidential data exchange since the required keys are stored in hardware and thus cannot be read out by an application. CCE currently supports the smart card-based implementation of the Austrian citizen card only, as no encryption and decryption functionality is provided by the mobile phone signature variant at the moment. However, other smart card implementations can be easily integrated by implementing an API provided by CCE.

CCE relies on the well-known and established S/MIME [Ramsdell and Turner, 2010] standard as container format for storing data. S/MIME is also widely integrated in several e-mail clients for encrypting e-mails. In the following, the main features of the CCE software are briefly explained [Zwattendorfer et al., 2013d]:

- *Smart card as secure decryption unit*
The CCE software supports the use of smart cards to decrypt the S/MIME containers. The process of decryption is directly carried out on the smart card, initiated by the user entering a PIN.¹¹
- *Support of group encryption*
Files and directories can be encrypted for multiple users, which can be organized in a group-like hierarchy. The management of groups is handled manually by the users on their own. However, the support of multiple users also allows for the inclusion of appropriate backup keys.
- *Support of the Austrian PKI infrastructure*
Asymmetric public key encryption facilitates encryption procedures of users and groups. The public keys of recipients are hence publicly available through the Austrian PKI infrastructure by querying the central LDAP directory. Nevertheless, CCE also enables the integration of arbitrary PKI infrastructures (e.g., from an enterprise context), which can be done by extending its open source application interface to support the new infrastructure.

2.2.3.3 Identification and Authentication

Unique identification and secure authentication are essential processes within e-Government. In Austria, the Austrian citizen card is the means of choice for citizen identification and authentication at online services. To facilitate the integration of citizen card functionality – and hence identification and authentication – at online applications, the Austrian e-Government initiative supported the implementation of an open-source module, which is called MOA-ID (Module für Online Applikationen - Identifikation)¹². This module takes over the identification and authentication process using the Austrian citizen card for a online applications and service providers respectively. However, a detailed discussion on identification and authentication in Austria is postponed thus to Section 3.6 is referred.

Nevertheless, to keep this subsection self-contained, the three main use cases for identification and authentication of citizens in Austria are listed. The Austrian e-Government strategy foresees the following three identification and authentication use cases [Lenz et al., 2014]:

- Secure identification and authentication of Austrian citizens by the use of the Austrian citizen card
- Secure identification and authentication on behalf of a natural or legal person
- Secure identification and authentication of foreign citizens of other EU member states

¹¹ Actually, a hybrid encryption approach is used in CCE, i.e. only a symmetric encryption key needs to be decrypted directly on the smart card and not the whole S/MIME container. The container is afterwards decrypted on the user's PC.

¹²<https://joinup.ec.europa.eu/software/moa-idspss>

2.2.3.4 Electronic Delivery

In Austria, official and jurisdictional documents are delivered according to the *Service of Documents Act* [Federal Chancellery, 2013]. To enable fully transactional and integrated e-Government services without media breaks, an electronic delivery framework has been introduced in Austria. Electronic delivery offers the possibility to send and receive certified mail electronically 24/7. Location-independence and time-savings are the main advantages on citizen-side, whereas public authorities mainly benefit from cost savings. In other words, electronic delivery constitutes the pendant to traditional certified-mail (RSa, RSb), which guarantees delivery to the intended addressee and provides the sender a proof of delivery at the same time. Details on this e-Delivery framework can be found in Tauber et al. [2011b,c].

Currently, e-Delivery in Austria is free of charge for the recipient. The recipient just needs to be registered by one authorized e-Delivery service provider¹³. Log-in at an e-Delivery service is only possible via the Austrian citizen card. During log-in, the recipient signs the confirmation of receipt, which is delivered as electronic return receipt to the sender. Due to that, this certified e-Delivery approach is legally equivalent to traditional paper-based certified mail.

Before e-Delivery service providers can be authorized to operate, they must run through a supervised accreditation process of the federal chancellery to ensure compliance with technical and organizational policies. Unless otherwise agreed, the e-Delivery service provider keeps the delivered document stored for 14 days for the recipient. In addition, recipients have the possibility to declare absences such as vacation or illness. In this time, documents with a time limit for reception must not be delivered to the recipient.

To facilitate the integration of e-Delivery services into applications for public authorities, within the Austrian e-Government initiative the open source module MOA-ZS (Module für Online Applikationen – Zustellung)¹⁴ was designed and developed. MOA-ZS incorporates a web interface that can easily be queried by an application. Main tasks of this module are locating the recipient via the central Austrian document delivery system (DDS), computing diverse cryptographic operations such as signature creation and verification operations, and delivering documents to authorized e-Delivery service providers.

2.2.3.5 E-Payment

Equally to traditional paper-based procedures, also for electronic procedures fees may apply. For achieving e-Government procedures without media breaks, it is therefore necessary to model and integrate also the payment process electronically into electronic procedures.

On the Internet, various payment systems have already evolved. The most popular examples are credit card payment systems, automatic debit transfer systems, or online payment systems such as *Pay-Pal*¹⁵. All these systems normally use their own proprietary interfaces, which leads to the situation that online shops or public authorities must implement all available interfaces if they want to support a particular payment system.

Therefore, in cooperation with the private sector, the so-called *eps*¹⁶ (e-Payment standard) has been developed. The eps standard provides a uniform and standardized interface between online shops or public authorities and credit institutions or other payment service providers. Main advantage of this standard is that the result of the payment process can be directly returned to the payment requesting application. Online shops or public authorities need not to wait for the receipt of payment but can further continue the procedure without any break or interrupt. Hence, several online banking or credit card payment systems can also be used for immediate and irrevocable payments.

¹³A list of authorized e-Delivery service providers can be found on <http://www.bka.gv.at/site/7889/default.aspx>

¹⁴<https://joinup.ec.europa.eu/software/moa-zs>

¹⁵<https://www.paypal.com>

¹⁶http://www.stuzza.at/12363_DE.htm

Customers benefit from this standard because no explicit registration process at a new payment system is required. Existing and trusted systems and mechanisms such as online banking or credit card payment systems can be integrated into the application. Contrary, online shops or public authorities benefit from immediate confirmation of payment and thus are able to directly continue the processing of the ongoing procedure. Furthermore, on technical level only one uniform interface needs to be implemented.

To facilitate the integration of the *eps* interface into public authority applications, the open source middleware EPS-2 handler has been developed within the Austrian e-Government initiative. This middleware implements the complete and complex *eps* interface for the communication between public authority and actual payment service provider. In particular, complicated processes such as XML signature creation and verification are encapsulated by the handler for the actual application. The application provider just needs to implement a simplified web service interface connecting to the EPS-2 handler to integrate different payment systems into its applications.

2.2.4 Sample E-Government Procedure

In this subsection, according to Posch et al. [2011] a common e-Government procedure (the application and issuance of a criminal record certificate) is described. First, the generic (traditional) process flow of a public administration procedure is explained. After that, the sample e-Government process flow of issuing of a criminal record certificate is illustrated aligned to the phases of the generic process flow.

2.2.4.1 Generic Process Flow

Traditional paper-based administrative procedures can be usually split into three phases (application, back-office processing, delivery) [Posch et al., 2011]. First, an applicant (e.g., a citizen in a C2G, or a business in a C2B communication scenario) has to fill out an application form at a public authority's office. In most cases, the citizen (in a C2B scenario as a representative of a business) has to show her ID for proving her claimed identity. Subsequently, the citizen has to sign the filled application form. By doing so, the public authority can launch the according administrative procedure. However, fees might apply which have to be charged before the final start of procedure processing. All these processes can be seen as the *application* phase.

After that, the public servant responsible for this procedure carries out all things that are necessary for processing the application. For instance, this might involve additional communication with the applicant if supplementary documents are missing, or querying appropriate registers to find additional information from the applicant to continue the procedure's processing. If the public servant comes to a result and is able to notify the applicant, the decision usually must have an official character and thus must be officially signed by the public authority. In paper-based procedures, this is carried out through signing the decision document by the processing public servant and putting a seal on it. These steps, where the public servant processes the application, are seen as the *back-office processing* phase.

Finally, the official document needs to be delivered to the applicant, hence this last phase is called *delivery* phase. In traditional procedures, the official document is either handed out personally to the applicant during offices hours or sent via registered mail to the applicant's home address. Figure 2.3 illustrates the individual phases.

Traditional paper-based procedures may be cumbersome for both the applicant and the procedure processing public servant. Therefore, in the following the author describes how the same procedure steps are handled as an e-Government process. Thereby, any media breaks are avoided and thus the described example can be seen as fully transactional and integrated service. To give a concrete example, the author describes the complete process of issuing a criminal record certificate electronically. For better illustration, we also refer to individual technical components involved that have been discussed in Section 2.2.3.

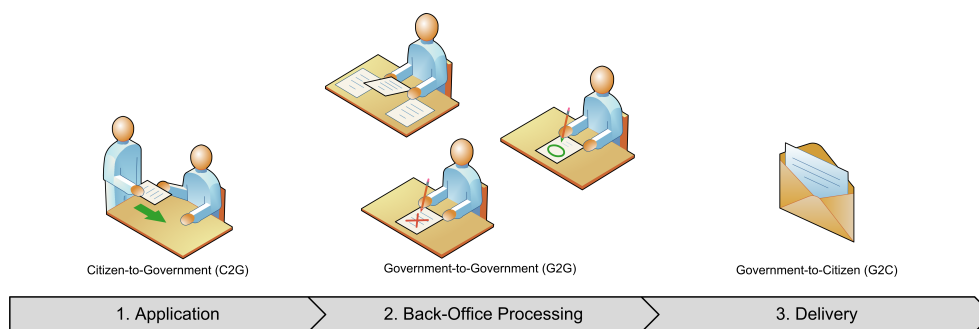


Figure 2.3: Generic Public Administration Process Flow [Posch et al., 2011]

2.2.4.2 Electronic Process Flow

The procedure for issuing a criminal record certificate electronically exists since the very first e-Government initiatives in Austria. This procedure also consists of the three phases: *application*, *back-office processing*, and *delivery*. However, all these steps are carried out fully electronically. In this example, it is assumed that the criminal record certificate can be issued electronically through a proper web application.

Before being able to file an electronic application, the requesting citizen has to find the relevant online application. To ease this process, Austria follows the one-stop shop principle [Wimmer, 2002]. Thereby, the Austrian government offers the e-Government portal *Help*¹⁷, which acts as single entry point for any kind of application. In the *Help* portal, all available procedures are modeled as life events e.g., birth, marriage, or passport renewal. Citizens just need to follow the information and description provided by *Help* and then are directed to the correct application. In this concrete example, depending on her home address the citizen is forwarded to a web application of her federal police station.

In a first step, the citizen needs to authenticate at this local web application before being able to file an application for receiving an electronic criminal record certificate. Unique identification and secure authentication is carried out by using her Austrian citizen card. The module MOA-ID is involved handling these processes for the web application. After that, the citizen is now allowed to file the desired application. This is done by filling out an appropriate web form. Based on the entered data, an application document is created, which needs to be signed by the citizen to give her willingness to start the electronic procedure in the back-office. Again, signature creation is carried out by using the Austrian citizen card. Thereby, access to this citizen card functionality is managed by the citizen card software. After that, the applicant is forwarded to a payment service provider, where application fees can be paid either via credit card or bank account transfer. The complete communication between the web application and the payment service provider is conducted through the EPS-2 handler and the corresponding *eps* protocol. Finally, the citizen gets a confirmation e-mail that the application has been successfully filed. All these steps belong to the first *application* phase.

In the *back-office* phase, the criminal record register is automatically queried for the applying citizen. The retrieved data are structured in XML. To provide the requesting citizen an easy readable and authentic document, the XML structure is first transformed into a PDF document and then officially signed by the federal police station using MOA-SS and PDF-AS. The electronic document is now ready to be delivered to the applicant.

In the last *delivery* phase, the document is sent electronically to the citizen via certified electronic mail. Thereby, the document is electronically transferred to an e-Delivery service provider. The technical component MOA-ZS facilitates this process for the web application. The delivered document can be fetched by the citizen from the e-Delivery service provider through successful citizen card login. By logging in via citizen card, the citizen electronically signs the return receipt for the sender.

¹⁷<http://help.gv.at>

2.3 Chapter Conclusions

This chapter gave an introduction to e-Government in general and to e-Government in Austria in particular. The aim of this chapter was to give the reader a basic understanding on the range and facets of e-Government in general as well as on the basic concepts and technical core of e-Government in Austria. Identification and authentication plays an important role in the remainder of this thesis. Hence, the reader should be aware on how the following chapters fit into the overall e-Government concept.

Chapter 3

Electronic Identity

Uniquely identifying a citizen is crucial in most cases when communicating with governments. In traditional public authority processes, citizens have to prove their identity showing an ID (e.g., passport, driving license, etc.) in the public authority's office. Unique identification is not less important in e-Government processes, hence the same requirement also holds for electronic procedures, i.e., when a user files an application electronically. Thereby, unique identification is particularly essential when sensitive or personal data are involved and need to be processed. However, electronic identification is not a new topic, thus different possibilities and approaches exist. This chapter defines various terms related to electronic identity and discusses the electronic identity management concept in Austria to give the reader a basic understanding on the fundamental ideas and concepts to be enhanced and amended in the subsequent chapters.

The chapter is structured as follows. In Section 3.1, identity related terms such as identification, authentication, identity management, etc. are introduced and discussed. Section 3.2 continues by discussing challenges, which need to be coped with, when dealing with electronic identity. In Section 3.3, different existing identity models and their advantages and disadvantages are elaborated. Section 3.4 briefly overviews the terms single sign-on (SSO) and single logout (SLO). Afterwards, different protocols for exchanging identity and authentication information between entities are evaluated. Finally, in Section 3.6 electronic identity concepts applied on national level in Austria are discussed. This includes the description of the Austrian citizen card and eID concept as well as the explanation of the technical eID architecture to be adopted for citizen identification and authentication.

3.1 Electronic Identity in General

This section aims on providing the reader a basic level of knowledge for the further concepts discussed in this thesis. Starting with the definition of several terms such as *electronic identity* or the corresponding processes of *identification* and *authentication*, the author also digs into detail on the management of identities. Since electronic identity and relating concepts are not new, several definitions have already evolved over time. Previous work include the identity management glossaries of Modinis [2005], the National Science and Technology Council (NSTC) [2008], Gutierrez and Piñuela [2009], Next-generation Networks [2009] or of ISO/IEC JTC 1 [2011]. A good overview on different identity management terminology glossaries is given in Bruegger and Müller [2013]. In the following – when giving definitions – the author refers to these glossaries but also takes additional scientific literature into account.

3.1.1 Identity and Digital Identity

A person's identity can have several facets, being a simple identifying number or a collection of personal attributes. In this subsection, the author defines the very basic terms on identity.

3.1.1.1 Identity

The term *identity* plays an important role both in real life and in the online world. It is used in every situation where the proof of being a particular person or having specific attributes or properties are required. In real life, the proof of identity is – for instance – required when traveling to another country. Thereby, usually showing a passport or a personal ID is necessary to prove that one is a specific person and possess a specific citizenship to enter the country. In this context, the natural person herself constitutes the *identity* possessing different attributes (e.g., name or citizenship).

According to Abelson and Lessig [1998], it is difficult to give a formal definition of identity. Identity can have different meanings in different disciplines [Arora, 2008b]. However, the Oxford Dictionaries [2014] define the term *identity* as "the fact of being who or what a person or thing is" [Oxford Dictionaries, 2014]. In relation to that, the Oxford Dictionaries [2014] stipulate an additional synonymous definition, where identity constitutes "the characteristics determining who or what a person or thing is" [Oxford Dictionaries, 2014].

In other words, the term *identity* describes distinct and non-ambiguous properties and characteristics of a person. By these properties and characteristics the person can be distinguished from others. For instance, such characteristics are name, gender, or the color of hair and eyes. An identity in real life is often also referred to as *principal*, within a digital context as *subject* [Andersson et al., 2011]. Additional information on the term *identity* can also be found in Bohm and Mason [2010].

3.1.1.2 Digital Identity

Basically, a digital identity has the same properties and characteristics as an identity in the real world. The only exception is that the properties are available in digital format and can be used as identity claims in distributed networks. There is no common agreement on a definition of digital identity, thus the author briefly overviews different definitions in this subsection. The author starts with the following definition of Bertino and Takahashi [2011]:

"Digital identity can be defined as the digital representation of the information known about a specific individual or organization."

Thereby, it can be seen that a digital identity more or less refers to a digital representation of personal characteristics or attributes.

A similar definition of digital identity to the one of Bertino and Takahashi [2011] is given by the Digital ID World Magazine [2002]. The Digital ID World Magazine [2002] defines a digital identity as "the representation of a human identity that is used in a distributed network interaction with other machines or people" [Digital ID World Magazine, 2002].

By this definition, digital identity is put into a technical context. Also Pfitzmann and Hansen [2010] state that. According to them, a "digital identity denotes attribution of attribute values to an individual person, which are immediately operationally accessible by technical means" [Pfitzmann and Hansen, 2010]. Hence, technical processing plays an important role when defining a digital identity.

Furthermore, according to the Digital ID World Magazine [2002], a digital identity consists of two parts:

1. Personal identity (who someone is)
2. Proofs of the identity (attributes someone possesses to prove the personal identity)

A personal identity consists of a set of characteristics of a person within a specific context, whereas these characteristics cannot or can only hardly be altered during a particular time period. Examples for such characteristics are the date of birth or genetic patterns such as eye color or height. Of course, date of birth – for instance – can be denied but it cannot be altered. [Camp, 2004]

Proofs of the identity are in fact attributes that define and characterize the personal identity. These proofs can be diversified, can have various values, and can be applied in miscellaneous cases. [Digital ID World Magazine, 2002]

In contrast to that, the Next-generation Networks [2009] stipulate that a digital identity consists of three parts, namely *identifiers*, *credentials*, and *attributes*. Bertino and Takahashi [2011] explain these parts in detail: Identifiers are usually strings consisting of various characters, digits, or symbols. Identifiers can be general or scoped within a specific context. Furthermore, they can be persistent or only valid within a certain time frame. Finally, they can be unique or ambiguous. Examples of identifiers are usernames, phone numbers, or URIs. Referring to Bertino and Takahashi [2011], credentials are “a set of data providing evidence for claims about parts of or entire identities”. Credentials can be e.g., passwords or digital certificates. Attributes are a set of characteristics or properties being a part of an identity. Attributes of an identity can be the name, date of birth, or eye color (cf. Section 3.1.1.1). Figure 3.1 shows the composition of a digital identity.

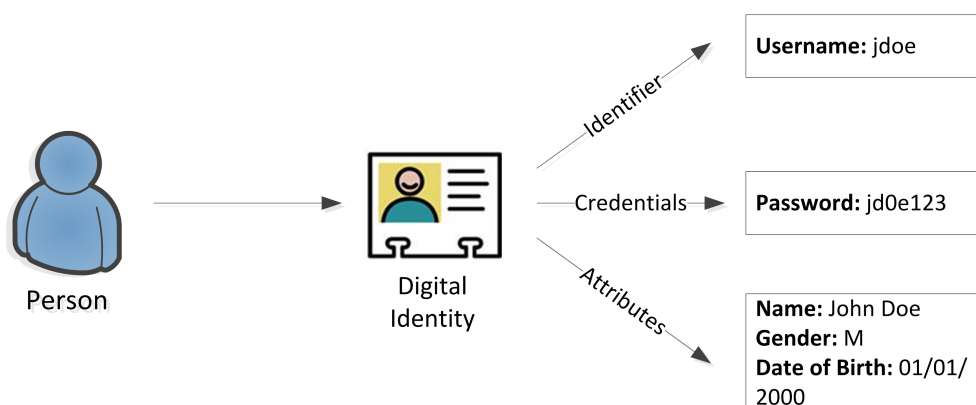


Figure 3.1: Digital Identity [Bertino and Takahashi, 2011]

A summary of definitions on digital identity can be found e.g., in [Cameron, 2005b]. For further reading, a complete book elaborating on digital identity has been written by Windley [2005].

3.1.2 Identification, Authentication, and Authorization

Identification, *authentication*, and *authorization* are all processes involving an identity. Furthermore, they more or less can be seen hierarchical in most cases. Authentication usually requires an identification process before. The same argument holds for authorization, which usually requires prior authentication. However, counterexamples exist. Two of them are discussed in Section 3.1.2.4.

During an identification process, a person or principal just claims that she is a specific identity. In real life – for instance – this is done by claiming “I am John Doe”, in the online world e.g., by showing an identifier or a username. Such a claim is usually not enough in terms of security, hence a proper proof of the *identification* process (proving that I am John Doe) is required in most cases. The process of proving an identity is called *authentication*. Assigning certain rights, roles, or permissions to an identity and further proving them is called *authorization* (proving that I, John Doe, am a doctor). [Camp, 2004].

In the following more detailed description of the terms *identification*, *authentication*, and *authorization* the author mainly refers on their use in the online world. A graphical illustration of these three processes is shown in Figure 3.2.

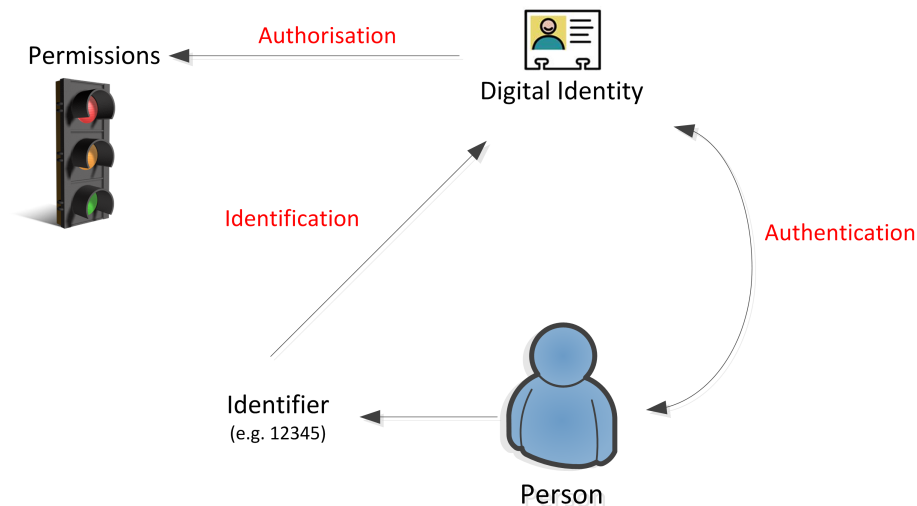


Figure 3.2: Identification, Authentication, and Authorization [Andersson et al., 2011]

3.1.2.1 Identification

According to Clarke [1994], "*human identification is the association of data with a particular human being*". In fact, identification can be seen as process of linking data to a particular person or principal respectively. The definition of Camp [2004] is similar but is more concrete on the term "data". Camp [2004] defines identification as "*the association of a personal identifier with an individual presenting attributes*". Making this definition a bit more general, then identification can be seen as the association between a personal characteristic and a subject representing various attributes. Such a personal characteristic could be the name of the person or the date of birth.

Taking an example, identification can be described as the association between a person (subject) and the full name (attribute). In this case the name "John Doe" identifies the person "John Doe". An identification process defines the presentation of an attribute a person can be uniquely identified with (in a given context). According to the example above, the person "John Doe" can be uniquely identified by presenting her name in a closed context. However, unique identification is only possible as long as no other person with the name "John Doe" in the closed context exists. If this is the case, additional attributes for unique identification would be required. I.e, the name and additionally the date of birth are usually sufficient for identification within small groups. However, if a large amount of users comes into play – such as the population of a whole country – identification based on name and date of birth might not be sufficient to guarantee uniqueness. Thus, in such a huge population, identification of citizens based on name and date of birth may be ambitious. To still being able to ensure unambiguous identification, each citizen of the country gets a unique identifier assigned. As an example, how unique identification has been realized in Austria will be explained in Section 3.6 in detail.

In general, identification can be based on different means. Clarke [1994] lists a couple of means by which a person can be identified. According to Clarke [1994]; Arora [2008b] the variety of means for identification is listed in Table 3.1.

Clarke [1994] sees *appearance* as something how a person looks e.g., the color of eyes or skin. A person can be identified by comparing these characteristics to a picture of an ID for instance. *Social behavior* refers to how a person interacts with others. To identify persons, mobile phone records to reveal whom the person communicated with can be used. *Names* are identifiers how a person is called by others. These can be either nicknames or official names as printed on a passport. Within an organization, usually *codes* are used for identification. Examples are social security numbers or the numbers of an ID card. Persons can also be identified on something the person knows (*knowledge*) e.g., a password or a personal PIN. *Tokens* are used for identification of persons if they have something e.g., they hold a

Table 3.1: Means of Identification according to [Clarke, 1994; Arora, 2008b]

Means of Identification	Definition	Example
<i>Appearance</i>	How the person looks	Pictures on ID documents
<i>Social behavior</i>	How the person interacts with others	Mobile phone records, video surveillance data, credit card transactions, etc.
<i>Names</i>	What the person is called by other people	Name listed in national registry or on passports, nicknames
<i>Codes</i>	What the person is called by an organization	ID card numbers, social security numbers
<i>Knowledge</i>	What the person knows	Passwords, PINs
<i>Tokens</i>	What the person has	Smart card, mobile phone
<i>Bio-dynamics</i>	What the person does	Pattern of the handwritten signature
<i>Natural physiography</i>	What the person is	Fingerprint, retina, etc.
<i>Imposed physical characteristics</i>	What the person is now	Height, weight

smart card or mobile phone. Pattern of handwritten signatures are identification means for what a person does and thus relate to *bio-dynamics*. *Natural physiography* or biometrics [Jain et al., 2011] use for identification things a person is. For instance, this can be fingerprints. Finally, height or weight can be used as identification as currently *imposed physical characteristics*.

3.1.2.2 Authentication

The term *authentication* defines the process of verifying a subject's identity or corresponding attributes. Just presenting subject's characteristics or attributes depicts only a claim. A claim without proper proof is not sufficient. The proof of a claim is called authentication. Camp [2004] defines authentication as a "*proof of an attribute*". According to Section 3.1.1.2, credentials (e.g., passwords, digital certificates, etc.) are used for proofing a claim.

During an authentication process a person proves her identity she claims to be. By checking the proof (credential), the authenticity and trustworthiness of the presented identity can be verified. Hence, the purpose of an authentication process is to verify that an identity can be trusted under certain circumstances and for specific operations. In real life, an example for authentication would be the identity check by verifying the photo of a person's passport. Having a look at the username/password authentication mechanism as example for online authentication, the username represents the identity and the password depicts the evidence for proofing the identity.

Camp [2004] distinguishes in his publication between *identity authentication* and *attribute authentication*. For Camp [2004], identity authentication refers to proving the association between a person (or entity in general) and an identifier. Attribute authentication is similar, i.e. proving the association between a person (or entity) and an attribute.

Credentials are used for proving authentication. For creating credentials in authentication systems different approaches exist [Windley, 2005]:

- Something a person knows
- Something a person has
- Something a person is

Referring to Windley [2005], in the first approach (*something a person knows*) authentication is based on a credential a person knows. The most popular example are passwords, where a user authenticates at a system or application by presenting a secret password. By comparing the presented password with a stored one¹ the validity of the password can be checked and the presented identity verified.

In the second approach (*something a person has*), authentication takes place using a credential a person has or holds. In most situations, such credentials are issued by a trusted third party. A practical example would be a digital certificate issued to a person by an organization.

Finally, in the last approach (*something a person is*) authentication is based on natural physiography characteristics such as biometric data. Practical examples are using fingerprints or retina scans for authentication.

The described approaches are also known as authentication factors [Windley, 2005]. To increase the level of security and authentication strength, sometimes these approaches or factors are combined. In general, combinations are called *multi-factor authentication*. Usually, if two factors are combined, authentication approaches are called as *two-factor authentication*, whereas *single-factor authentication* refers to the usage of just one approach. In general, the more authentication factors are combined the more secure the authentication mechanisms is [Windley, 2005].

3.1.2.3 Authorization

Mostly, the term authorization is used in conjunction with identification and authentication, whereas an authorization processes usually succeeds an authentication process [Andersson et al., 2011; Curphey et al., 2002]. Referring to Camp [2004], "*authorization is a decision to allow a particular action based on an identifier or attribute*". In other words, authorization defines granting or denying access to protected resources or services for a certain identity. Thereby, identities are assigned particular rights or permissions [Andersson et al., 2011]. Authorization is often used in connection with groups and roles. Usually, identities are assigned to groups or roles. Each individual role or group has defined access rights, thus identities can only get access to intended resources or services based on the rights defined in the assigned role or group.

The terms *authorization* and *access control* are often not properly distinguished [Curphey et al., 2002]. According to Curphey et al. [2002], "*authorization is the act of checking to see if a user has the proper permission to access a particular file or perform a particular action*". In comparison to that, Curphey et al. [2002] define access control as a "*much more general way of controlling access to [...] resources*". Curphey et al. [2002] see the focus of authorization on the use of credentials and specific rules whereas access control has broader facets e.g., including time or location restrictions or constraints. Further details on access control can be found in Sandhu and Samarati [1994]; Windley [2005].

3.1.2.4 Special Cases

Identification, authentication, and authorization are not strictly tightened together or hierarchical. The following examples according to Andersson et al. [2011] illustrate this statement.

Identification without authentication In some scenarios it might be necessary that only one person or principal needs to authenticate, whereas for others identification is sufficient. As an example, the author assumes registering the results of an exam in the university's online information system. In this scenario, the lecturer, who held the exam, needs to authenticate at the online system. However, for archiving the grades the students awarded for this exam just identification of the students in the online system is necessary. The students do not need to authenticate for this process, hence they are *identified without authentication*. [Andersson et al., 2011]

¹In practical applications usually not the password itself but a hash value of the password is stored for comparison.

Authentication without identification To illustrate this special case, the author again refers to an example, assuming that a person wants to play online casino. For proving that the person is allowed to play online casino, she must be older than 18. However, most identity management systems reveal the full date of birth or the complete identity of the person to the online casino application although only her age would be required. Just proving the age is sufficient for authentication in this case. Hence, a person can be *authenticated without identification*. So-called anonymous credential systems such as *U-Prove* [Brands, 2000] or *Idemix* (Identity Mixer) [Camenisch and Lysyanskaya, 2001] are specific technologies that support these special use case. [Andersson et al., 2011]

3.1.3 Electronic Identity (eID)

Identification (cf. Section 3.1.2.1) is particularly essential if sensitive and personal data are processed. Especially in e-Government processes unique and secure identification is vital. Whereas in traditional public administration processes citizens are requested to provide a conventional ID (e.g., passport, driving license, etc.) for identification, in contrast to that, in e-Government processes citizens are requested to provide an *electronic identity* (eID) for accessing e-Government services. According to the CEN/ISSS Workshop on eAuthentication [2004], "*electronic identity solutions have the aim to guarantee the identity of a person (or a legal entity, e.g. a company) during the access to e-services and in order to provide the trust to the parties involved in the electronic transaction*". The usage of electronic identification is not required for all electronic services e.g., when opening an e-mail account just self-identification and self-registration is sufficient. However, eIDs are needed when sensitive data are processed and thus secure identification of persons is crucial [CEN/ISSS Workshop on eAuthentication, 2004].

Electronic identities are mainly used in a governmental and national context. When talking about eIDs, many publications tighten this term to eID cards only [Arora, 2008b,a; Myhr, 2005; CEN/ISSS Workshop on eAuthentication, 2004]. However, eIDs can be stored on various media [Graux et al., 2009d] and many other solutions than smart cards exist to model electronic identities in national scenarios (cf. Section 5.1). In the context of this thesis, electronic identity (eID) refers to any technological approach that fulfills the requirements of securely and uniquely identifying a person electronically in a specific – particularly national – context. Such requirements can be based on existing national law, which is applicable in both traditional paper-based and electronic processes [Myhr, 2005].

Referring to Arora [2008a], an electronic identity offers the following three so-called I-S-A functions: Identification, Signature, and Authentication. All these functions can also be carried out by physical IDs. However, applying these functionality electronically refers to an electronic identity (eID) [Arora, 2008a]. The signature functionality of an eID – in particular on European level – was mainly driven by the EU signature directive [European Parliament and Council, 1999b]. The signature directive defines *advanced electronic signatures* and *qualified electronic signatures*. According to this directive, advanced electronic signatures are uniquely linked to and can identify the signatory, can be created under full control of the signatory, and ensure full integrity of signed data [European Parliament and Council, 1999b]. Qualified electronic signatures are in fact advanced electronic signatures but are created within a secure signature creation device (SSCD) and are based on a qualified certificate (cf. Section 2.2.3.1). In particular, this directive stipulates that qualified electronic signatures are legally equivalent to handwritten signatures. In sensitive areas of applications such as e-Government, secure and unique identification is essential. According to Myhr [2005], it is crucial to ensure the link between a person possessing an eID and the data of the eID. The link must be so strong that a third party is able to accept the eID as a valid eID [Myhr, 2005]. Furthermore, electronic identity data must be unambiguous and must enable unique identification. Finally, eIDs must allow for strong authentication such as multi-factor mechanisms [Myhr, 2005] (cf. Section 3.1.2.2).

To achieve this strict objectives, Myhr [2005] lists the following features an electronic identity (eID) needs to support:

- universality of coverage
- uniqueness
- permanence
- exclusivity
- precision

Following these features of Myhr [2005], every person, who needs to get identified within a specific context, should have an identifier (*universality of coverage*). Furthermore, the identifier should be unique to avoid unambiguity and every person should have one identifier only (*uniqueness*). In addition, the identifier should not change and thus should stay persistent for this person (*permanence*). The identifier should also be exclusive, hence not other method of identification should be used (*exclusivity*). Finally, identifiers should be sufficiently different to avoid any mistakes (*precision*). [Myhr, 2005]

These features are actually fulfilled by most national eID solutions. The author discusses the Austrian eID solution in Section 3.6 and some other European eID solutions in Section 5.1. At the moment, most of these national eID solutions are legally based on the EU signature directive [European Parliament and Council, 1999b]². However, the European Commission is currently working on a new legal framework where a first draft version was published in 2012 [European Commission, 2012b].

3.1.4 Identity Management

Identity management is basically used to manage digital identities and to control and regulate access to various protected resources. Alpár et al. [2011] refer to identity management as *"the processes and all underlying technologies for the creation, management, and usage of digital identities"*. In more detail, according to Alpár et al. [2011] it *"covers the process of establishing the identity of a remote user (or system), managing access to services by that user and maintaining identity profiles concerning that user"*. As this definition of Alpár et al. [2011] already indicates, identity management is actually not tailored to the organization of users or persons only. In fact, identity management can also relate to systems or services, as the following definition of Clercq and Rouault [2004] suggests:

"Identity Management can be defined as the set of processes, tools and social contracts surrounding the creation, maintenance, utilization and termination of a digital identity for people or, more generally, for systems and services to enable secure access to an expanding set of systems and applications. Identity"

While the previous definitions refer to digital identities in general, the definitions of Clauß and Köhn-topp [2001] and Pfitzmann and Hansen [2010] explicitly contain the management of partial identities. The term partial identity will be explained in Section 3.1.4.3.

Identity management is a complex topic because different stakeholders are involved, different processes need to be carried out for successfully managing identities, and different types of identities can exist. In the following subsections the author elaborates in more detail on these aspects.

3.1.4.1 Stakeholders

An identity management system usually involves four entities or stakeholders [Bertino and Takahashi, 2011]. Referring to Bertino and Takahashi [2011], a *service provider* (SP) provides different online services to so-called *subjects* or *users*. Before being allowed to consume such services, a user has to

²In Austria the E-Government Act [Federal Chancellery, 2008], which refers to the EU signature directive [European Parliament and Council, 1999b], constitutes the legal basis for electronic identity.

successfully identify and authenticate. Therefore, the user usually identifies and authenticates at a so-called *identity provider* (IdP). The identity provider is then in charge of providing the user's identity data and supplementary authentication results to the service provider in a secure way. Finally, a *control party* (CP) might be involved, which is usually a law or regulation enforcing body that needs to investigate identity data transactions e.g., for data protection reasons. Hence, main purpose of such a control party is auditing. Figure 3.3 illustrates the communication process in an identity management system including all four entities.

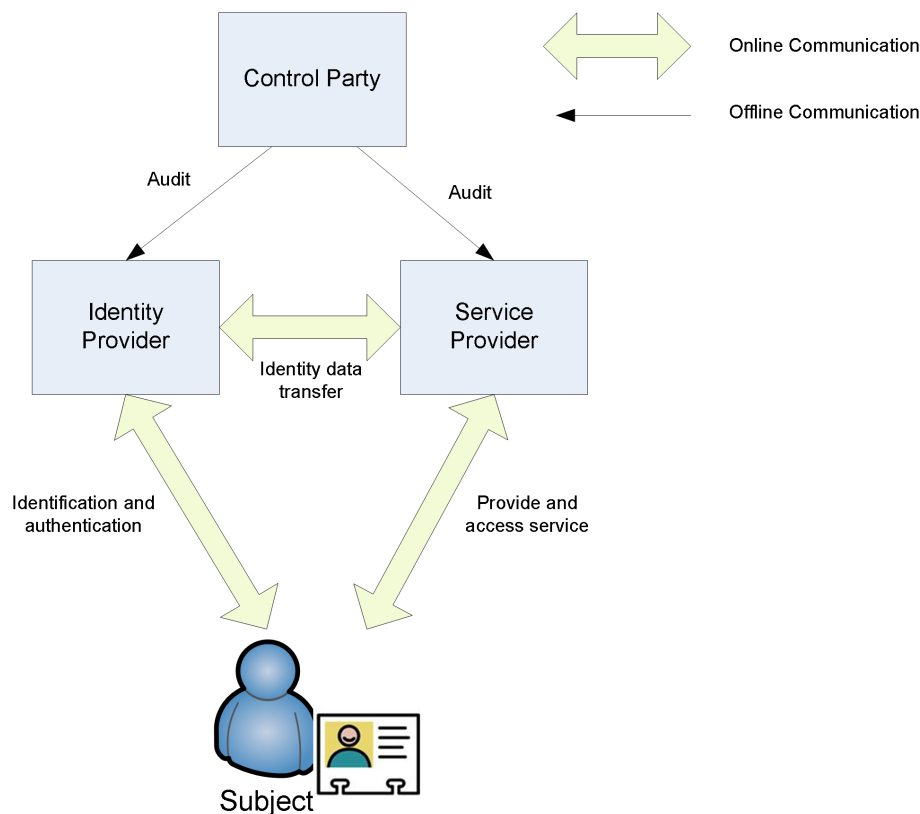


Figure 3.3: Stakeholders in an identity management system [Bertino and Takahashi, 2011]

All these stakeholders have different interests and requirements [Alpár et al., 2011]. In the following, details on the individual stakeholders according to [Bertino and Takahashi, 2011] are given.

Subject/User: Subjects or users are persons or entities that own one or more digital identities. These identities consist of different attributes. Bertino and Takahashi [2011] classify them into legal documents-based attributes, demographic attributes, financial attributes, biometric attributes, and transactional attributes. Legal documents-based attributes are attributes asserted from government-issued documents such as passports, driving licenses, or national IDs. Examples for demographic attributes are age, gender, or address. Financial attributes are issued e.g., by banks and are – for instance – credit card or bank account information. Biometric attributes have already been discussed in Section 3.1.2.1 and are natural physiography characteristics such as fingerprints. Transactional attributes are dynamic and are mostly created during interactions or transactions on the Internet. Examples for transactional attributes are session cookies.

All these attributes are valuable assets which require special protection against threats. Identity threats will be discussed in Section 3.1.5.

Identity provider (IdP): Main functionality of identity providers is the provision of digital identities to users and the transfer of identification and authentication data to a service provider during an

identification and authentication process. According to Bertino and Takahashi [2011], an IdP has four main tasks: (1) Assignment of an identifier to a user, (2) Linkage of the identifier with attributes of the user, (3) Provision of appropriate credentials for proving identity data, and (4) Creating assertions on identification and authentication data.

Service provider (SP): Service providers are entities that provide protected services or resources to users. For providing these protected services, user identification and authentication is required, which is usually taken over by the IdP for the SP. Hence, the SP usually needs to trust the IdP that the credentials provided by the user for authentication are sufficiently strong for granting access to the requested protected resources.

Control party (CP): Control parties are usually regulatory bodies, which enforce appropriate law or regulations. Based on that, control parties have the right to inspect and audit transactional data in case any fraudulent activity has been detected. Its main task is auditing.

3.1.4.2 Identity Lifecycle

In general, digital identities are not persistent over time. For instance, users may move to another place and thus the address attribute of a digital identity changes. Hence, digital identities run through a lifecycle which consists of four different phases. Figure 3.4 illustrates these four lifecycle phases according to Bertino and Takahashi [2011].

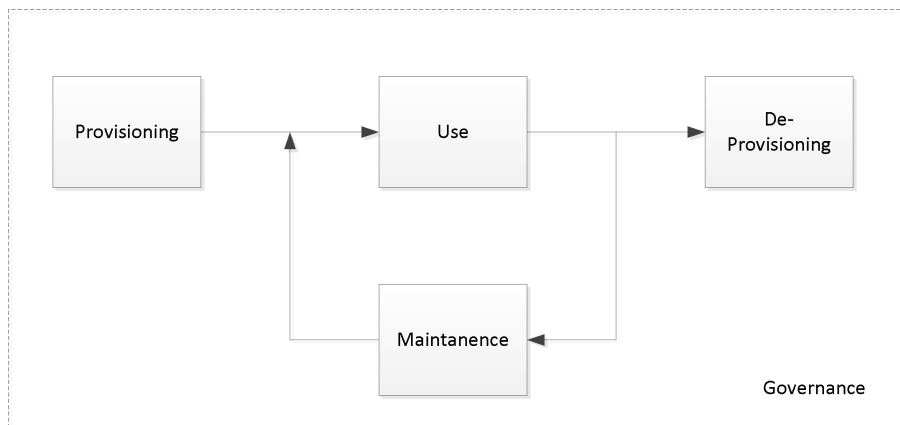


Figure 3.4: Identity Lifecycle [Bertino and Takahashi, 2011; Andersson et al., 2011]

First, a digital identity needs to be provisioned, i.e. the digital identity is created (*provisioning*). After that, the identity is used during various processes or transactions (*use*). Over time, identity attributes may change or attributes need to be added or removed, hence the identity must be maintained (*maintenance*). Finally, the identity may expire or is not used anymore, thus it must be revoked or de-provisioned (*de-provisioning*). In the following, details on the individual phases are given [Bertino and Takahashi, 2011; Andersson et al., 2011; Windley, 2005].

Provisioning: The provisioning phase is merely the phase where an identity is created. Creation can be carried out automatically online or manually during an offline process. Before being able to create an identity, attribute data to be linked to the identity are required. These data can be either self-asserted (e.g., entering personal data on a web page) or attested by a trusted third party. In both scenarios, provided attribute data needs to be somehow verified before identity creation. In addition, credentials corresponding to the attributes need to be created and issued to the user. Such credentials can be e.g., passwords or digital certificates. Finally, the complete identity can be formed by linking the attributes and the credentials to an identifier.

Use: This phase is the most visible phase for users because identity data are used and consumed by service providers. The most frequent application processes are identification, authentication, and authorization for granting access to protected resources. Further application use cases are single sign-on (cf. Section 3.4.1) or attribute sharing and distribution into other systems or databases [Bertino and Takahashi, 2011].

Maintenance: Identities are usually not static and may change over time. Reasons are attribute updates such as permission changes, adding or removal of attributes, or expiring credentials (e.g., digital certificates), which require maintenance efforts on the identity. If the identity was successfully updated, it can be used again. Updates can be triggered automatically (e.g., by expired access permissions) or manually (e.g., lost password functionality). Assigned identifiers should not be changed.

De-Provisioning: De-provisioning can be seen as the opposite process to identity provisioning. In this phase, identity data can be either revoked or deleted. Revocation of credentials is of particular importance if credentials get stolen or compromised. Failing to revoke or delete – for instance – expired identity data can easily lead to unauthorized access or open the door for other attack vectors. Any revocation or deletion should be properly documented and involved systems should be informed.

Governance: Governance is an important part to ensure integrity of the whole identity lifecycle phases. During the lifecycle, transactions on identity data should follow well-defined identity policies. These policies should ensure compliance with specific regulations or even law. Such policies can e.g., define how identities should be created, used, maintained, or deleted, describe the required strength of an authentication process, or regulate conditions for access control. In addition, all transactions should be logged for future auditing purposes in case any inspection or forensic analysis is required. All transactions involving identity data should be replicable and provable.

Windley [2005] describes an additional phase in his identity lifecycle, which is *propagation*. Propagation describes the phase of propagating or distributing created identities to appropriate systems, i.e. storing identity information in directories or databases. This phase would be situated between the *provisioning* and the *use* phase.

3.1.4.3 Types of Identities

Digital identities can have different characteristics. For instance, they can be differentiated based on the location of creation or storage, or on the context of use [Andersson et al., 2011]. In the following, according to Pfitzmann and Hansen [2010]; Hansen et al. [2008]; Andersson et al. [2011] different types of digital identities are briefly elaborated. However, the list does not claim for completeness.

Complete identity: For Pfitzmann and Hansen [2010] a complete identity *”is the union of all attribute values of all identities of this person”*. This statement further implies that a principal can have multiple digital identities.

Partial identity: Referring to Pfitzmann and Hansen [2010], a partial identity *”is a subset of attribute values of a complete identity”*. Hansen et al. [2008] go a bit more into detail. For them, an identity contains a set of attributes and this set *”contains subsets representing partial identities in different areas of life the individual wants or must take part in”* [Hansen et al., 2008]. Each of these partial identities *”represents the person in a specific context or role”* [Pfitzmann and Hansen, 2010]. Hence, different parts of life are also separated in the digital world by building partial identities [Borcea-Pfitzmann et al., 2006]. In real applications, partial identities are usually called an account [Andersson et al., 2011]. According to Andersson et al. [2011], an account is a *”a self-contained*

set of identity information that is used for a specific purpose only and that is maintained for serving this purpose only”.

Pseudonymous identity: A pseudonymous identity usually includes a pseudonym as an identifier [Pfitzmann and Köhntopp, 2001]. A pseudonym *”decouples a digital identity from the real-world entity but preserves the univocal linkage to a unique entity”* [Andersson et al., 2011]. The difference to a normal digital identity is that an identity consumer (e.g., service provider) can still interact with a person as usual but does not get revealed the real identity of the person. For decoupling the digital identity from the person a trusted third party – which acts as mediator – is required. The trusted third party is responsible for linking the pseudonymous identity to the person. If required, the trusted third party is also the only entity that can reveal this linkage and could disclose the person’s real identity. [Andersson et al., 2011]

Anonymous identity: Anonymous identities provide unlinkability between a digital identity and the real-world person. For Andersson et al. [2011] an anonymous identity *”can be considered as a partial identity whereby the available identity claims are not sufficient to derive an identifier or otherwise link to any real-world entity”*. Hence, the real-world identity of a person cannot be revealed by disclosing an anonymous identity. Anonymous identities are usually just temporary and not persistent. Technologies modeling anonymous identities are e.g., *U-Prove* [Brands, 2000] or *Idemix* [Camenisch and Lysyanskaya, 2001].

Further information on partial identities can be found in the results of the FIDIS³ project and on pseudonymity and anonymity in Pfitzmann and Köhntopp [2001]; Roth and Schmidt [2011].

According to Andersson et al. [2011], *”a digital identity is usually bound to a certain domain of applicability”*. Hence, an identity may only have specific meaning in a specific context or domain. In the following, different identities with respect to the underlying domain are described [Andersson et al., 2011]:

Local identity: Referring to Andersson et al. [2011], *”a local identity can be seen as a digital identity that is created and used only in a closed environment or domain”*. Mostly, such identities are self-created. A typical example would be a local password store within the user’s domain or the account of the operating system of the user’s PC. [Andersson et al., 2011]

Global identity: In contrast to a local identity, a global identity can be used *”across local domains or within one global computing ICT infrastructure”* [Andersson et al., 2011]. Advantage of a global identity is that it can be used in a broader context, however, disadvantages are privacy concerns.

Federated identity: According to Andersson et al. [2011], a federated identity *”denotes the portability of identity information across multiple systems or organizations”*. Thereby, identities and identity information are not stored within a single and central domain but distributed. Linking the stored identities across domains is referred to as federation. According to Poetzsch et al. [2009], identity federation *”lets entities use the same sets of identification data, to get access (and authorisation) to the several different (otherwise autonomous) services offered by all the organisations associated with the system of federation”*. The model of identity federation will be discussed in more detail in Section 3.3.4. Federated identity is also a key enabler for single sign-on (SSO), which will be discussed in Section 3.4.1. Further information on federating identities can also be found in Windley [2005]; Chadwick [2009]; Shim et al. [2005].

Brokered identity: According to Alamäki et al. [2003], an identity broker is responsible for translating an identity. The resulting identity can be denoted as brokered identity. In such scenarios, the

³<http://www.fidis.net>

identity broker acts as trusted intermediary on behalf of the user the identity belongs to [Andersson et al., 2011]. An identity broker can – for instance – be used for preserving user’s privacy e.g., hiding user’s real identity from a service provider through pseudonymization [Alamäki et al., 2003].

3.1.5 Identity Threats

Digital identities can contain sensitive personal information and thus are a valuable asset that needs particular protection against various threats. In this subsection, a couple of threats regarding identity according to Andersson et al. [2011]; Tsolkas and Schmidt [2010] are briefly listed.

Identity theft: Identity theft means stealing the identity of another person and moreover acting instead of her in a non-intended manner. Such a scenario can have several severe implications e.g., unauthorized persons can get access to protected resources or can buy things when being able to use the credit card linked with the thieved identity.

Identity linking: In this threat scenario, as much information of a specific identity as possible is collected. For instance, information of partial identities can be bundled and a more comprehensive identity profile derived based on this information. Data can be collected e.g., through the use of persistent identifiers, through requesting more information than necessary for service provisioning, or even through personal information disclosed on social networks.

Identity manipulation: In such a threat, attackers try to manipulate and change individual identity attributes. Access control permissions can – for instance – be manipulated by changing role or group data of an identity. Identities could get access to sensitive data which they actually had not been authorized before.

Identity disclosure: Identity data or individual attributes can also be unwillingly be disclosed. This is particularly fatal e.g., if information of a terrible disease or any other health information gets disclosed.

3.1.6 Trust Management

“Trust is the characteristic whereby one entity is willing to rely upon a second entity to execute a set of actions and/or to make a set of assertions about a set of principals and/or digital identities. In the general sense, trust derives from some relationship (typically a business or organizational relationship) between the entities” [Goodner and Nadalin, 2009]. Trust plays an important role in the identity management context as different entities and stakeholders interact with each other. For instance, service providers outsourcing the identity management to an identity provider have to trust the identity provider that the asserted and received information about a user is correct and valid.

Since trust effects several entities, their realization can be different. Different trust models have already emerged over time. In the following typical trust models referring to Andersson et al. [2011]; Linn et al. [2004] are introduced.

Direct trust: *“In a direct trust relationship, one party usually fully trusts the other party without the use of any intermediaries or other third parties”* [Andersson et al., 2011]. In other words, presented claims are only accepted if the entities directly and without any intermediary communicate with each other.

Indirect trust: *“In an indirect trust relationship, the affected parties solely rely on claims asserted by a common third party with which a pre-existing trust relationship is already established”* [Andersson et al., 2011]. There is no direct trust path between the individual entities but they rather rely on a trusted third party.

Pairwise trust: *"Pairwise Trust describes the case where two entities have direct business agreements with each other"* [Linn et al., 2004]. In fact, this is a special case of direct trust as only two entities are involved. In pure direct trust relationships several entities can have a direct trust path e.g., to one single trusted third party.

Brokered trust: *"Brokered Trust describes the case where two entities do not have direct business agreements with each other, but do have agreements with one or more intermediaries so as to enable a business trust path to be constructed between the entities"* [Linn et al., 2004]. In other words, the two entities have no direct trust relationship with each other but the intermediaries have. Due to that, a trust relationship between the two entities through the intermediaries can be established. According to Andersson et al. [2011], the intermediaries *"construct the trust path and feature a trust relationship that is at least as stable as the resulting trust relationship between the two service parties shall be"*. In fact, this is a special case of indirect trust, as a couple of indirect trust relationships are involved.

Community trust: *"Community Trust applies when the business trust between a pair of entities is derived from their enrollment in a common authentication infrastructure and acceptance of its practices, without reliance on other business agreement paths"* [Linn et al., 2004]. In other words, trust is established through the membership in a community [Linn et al., 2004].

3.2 Challenges for Electronic Identity

Electronic identity and identity management plays an important role in our daily lives. In many G2C, C2B, or G2B scenarios it is crucial that the involved parties can be sure whom they are communicating with. To ensure trustworthy identities and to make electronic communication involving electronic identities reliable, electronic identities and identity management systems must deal with several challenges. In the following, a couple of high-level challenges based on the work of Cameron [2005a]; Dhamija and Dusseault [2008]; Górnjak et al. [2011]; Fumy and Paeschke [2011] are listed.

Security: Security is essential in particular for eID implementations to encounter any identity threat (cf. Section 3.1.5) or an identity compromise during online transactions. Thereby, cryptographic technologies play an important role. [Fumy and Paeschke, 2011]

Privacy: Although unique identification is required in some situations, users still must not be forced to disclose more information than necessary [Cameron, 2005a]. Furthermore, in some situations users still want to stay anonymous [Fumy and Paeschke, 2011] or want to avoid any profiling or tracking through persistent identifiers (unlinkability) [Naumann and Hogben, 2008; de Andrade et al., 2013]. Hence, privacy is an important challenge that must be overcome when designing or implementing an identity management system. Further information on eIDs and privacy features can be found in Naumann and Hogben [2009].

Trust: Appropriate trust relationships between all involved entities are key [Fumy and Paeschke, 2011]. According to Fumy and Paeschke [2011], users must be able to trust and understand the security and privacy principles of identity management systems. Suitable and reasonable policy statements must exist to provide information on the identity data usage [Cameron, 2005a].

Data control: According to Fumy and Paeschke [2011], *"in any eID scheme, end users should be entitled to maximum control over their own personal data. This implies that it must be left up to the data owner to grant access to her or his personal data to a service provider [...]"* [Fumy and Paeschke, 2011]. de Andrade et al. [2013]; Górnjak et al. [2011] define this challenge as *user-centricity*, thus users and not the service or identity provider should be in full control about

identity data. Furthermore, referring to Cameron [2005a]; Dhamija and Dusseault [2008] user consent plays an important role to encounter this challenge.

Usability: According to Dhamija and Dusseault [2008]; Fumy and Paeschke [2011], usability is important for users to accept identity management systems or authentication mechanisms. For instance, multiple identities must be easily manageable or the authentication processes must be easy to understand and follow [Dhamija and Dusseault, 2008; Fumy and Paeschke, 2011].

Interoperability: Referring to Fumy and Paeschke [2011], "*interoperability facilitates the portability of identities and enables service providers to accept a variety of credential and identification media types*". In addition, interoperability is essential that different systems dealing with identity are able to interact with each other [Górniak et al., 2011]. The use of open standards, interfaces, and specifications can help to increase interoperability between different systems.

3.3 Identity Models

Identification and authentication are by far no new issues, thus several different identity management systems have evolved [Bauer et al., 2005]. In most identity management systems, interactions between the four stakeholders user, identity provider, service provider, and control party (cf. Section 3.1.4.1) takes place. Not all systems follow the same methodological approach. For instance, some systems store identity data centrally, whereas other systems follow a federated approach.

In the following subsections the most important models based on the work of Alpár et al. [2011]; Cao and Yang [2010]; Dabrowski and Pacyna [2008a,b]; Jø sang et al. [2005]; Jø sang and Pope [2005]; Jø sang et al. [2007]; Palfrey and Gasser [2007] are briefly described. Distinction criteria are the storage location of identity data (i.e. central database, user domain, or distributed storage). Each of these models has its specific characteristics. One may have advantages on privacy and user control, another one on scalability. For simplicity, a discussion of the control party in all subsequent models is skipped because its functionality remains the same in all models.

3.3.1 Isolated Model

The *isolated model* [Cao and Yang, 2010; Jø sang et al., 2005] is basically the simplest traditional identity model. Alpár et al. [2011] denote it as silo model. In this model, the service provider and identity provider merge, hence identification and authentication are directly carried out at the service provider (cf. Figure 3.5). In addition, the functionality of the identity management system (creating, maintaining, or deleting identities) can only be used by this specific service provider. If a user wants to access services of another service provider, she needs to register at the other service provider's identity management system again. This further means that each individual service provider has to store and maintain the identity data and credentials of the user separately. While this still may not be a huge burden for service providers, the diversity of credentials for accessing various service providers may become unmanageable for users [Jø sang and Pope, 2005]. This model can still be found by many service providers on the Internet.

3.3.2 Central Model

The *central model* [Alpár et al., 2011; Jø sang et al., 2005; Cao and Yang, 2010; Palfrey and Gasser, 2007] avoids diverse isolated identity management systems, where the user has to register separately. Instead, the identity management system is outsourced by several service providers to a central identity provider. The identity provider takes over all identity-related functionality for the service provider, including credential issuance, identification and authentication, and the management of the identity life-cycle in general (cf. Section 3.1.4) [Bertino and Takahashi, 2011]. Furthermore, in this model users'

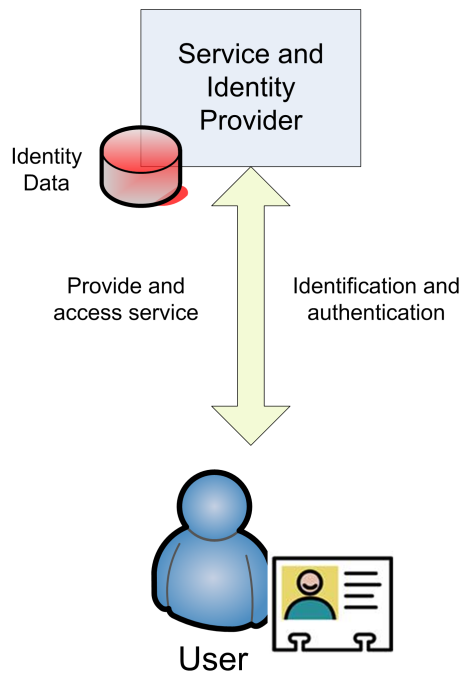


Figure 3.5: Isolated Model

identity data are stored in a central repository at the identity provider and service providers do not need to maintain identity data in their own repositories [Cao and Yang, 2010]. For authentication at a service provider, the user has to identify and authenticate at the identity provider before. The identity provider then assembles a token including all necessary identity and authentication information of the user and transmits it to the service provider⁴. Figure 3.6 illustrates the central model.

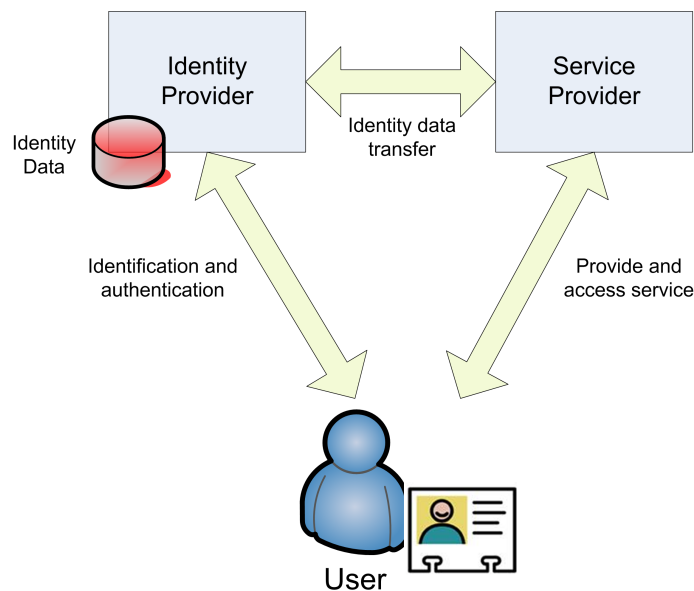


Figure 3.6: Central Model

Jø sang et al. [2005] further distinguish the domain model for the identifier used. In the *common identifier model* one and the same identifier is used for identification at all service providers. In contrast to that, in the *meta identifier domain model* separate identifiers are used for identification at the individ-

⁴Different approaches exist; hence identity data can be either pushed to or pulled from the service provider.

ual service providers. However, all separate identifiers map to a common meta identifier at the identity provider to uniquely identify the user. Typical examples implementing this approach are *Kerberos* [Neuman et al., 2005] or the *Central Authentication Service* (CAS – cf. Section 3.5.7).

3.3.3 User-Centric Model

While in the central model all identity data of the user are stored in the domain of the identity provider, in the *user-centric model* [Alpár et al., 2011; Jø sang et al., 2005; Palfrey and Gasser, 2007] all identity data are stored directly in the user’s domain e.g., on a secure token such as a smart card (cf. Figure 3.7). The main advantage of this model is that the user always remains the owner of her identity data and stays under their full control [Dabrowski and Pacyna, 2008b]. Identity data can only be transferred by an identity provider to a service provider if the user explicitly gives her consent to do so. Compared to the central model, this tremendously increases users’ privacy. Jø sang and Pope [2005] discuss in detail this user-centric approach. Typical examples implementing this model are *Windows CardSpace*⁵ or various national eID solutions such as the *Austrian citizen card* [Leitold et al., 2002] or the *German eID* [Fromm and Hoepner, 2011].

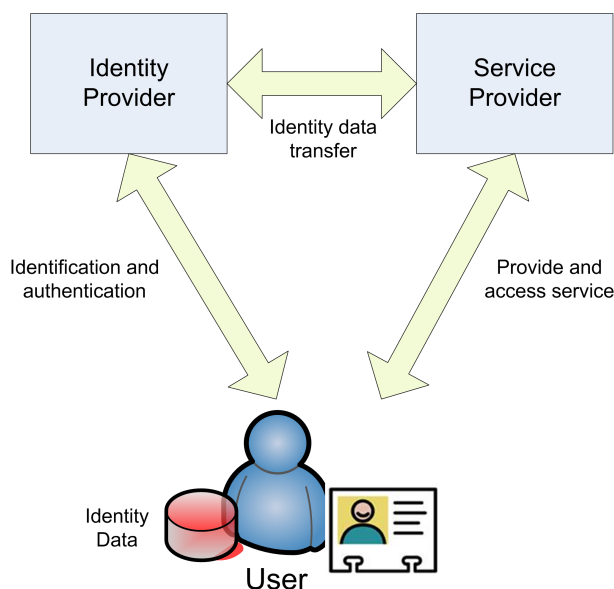


Figure 3.7: User-Centric Model

3.3.4 Federated Model

In the *federated model* [Cao and Yang, 2010; Palfrey and Gasser, 2007; Windley, 2005], identity data are not stored in a central repository but are rather stored distributed across different identity and/or service providers. No single entity is fully controlling the identity information [Palfrey and Gasser, 2007]. The distributed identity data of a particular user are linked usually by the help of a common identifier⁶. All identity providers and service providers, which take part in such a federation, share a common trust relationship amongst each other. The trust relationship is usually established on organizational level whereas enforcement is carried out on technical level. This federated model particularly supports identification and authentication across different domains, which paves the way for cross-domain single sign-on [Cao and Yang, 2010]. Popular examples of this approach are the *Security Assertion Markup Language*

⁵[http://msdn.microsoft.com/en-us/library/vstudio/ms733090\(v=vs.90\).aspx](http://msdn.microsoft.com/en-us/library/vstudio/ms733090(v=vs.90).aspx)

⁶It is not necessary that the common identifier is shared. Different identifiers mapping to the same user are also possible [Cao and Yang, 2010].

(SAML – cf. Section 3.5.2), *Shibboleth*⁷, or *WS-Federation* (cf. Section 3.5.6). Figure 3.8 illustrates the federated model.

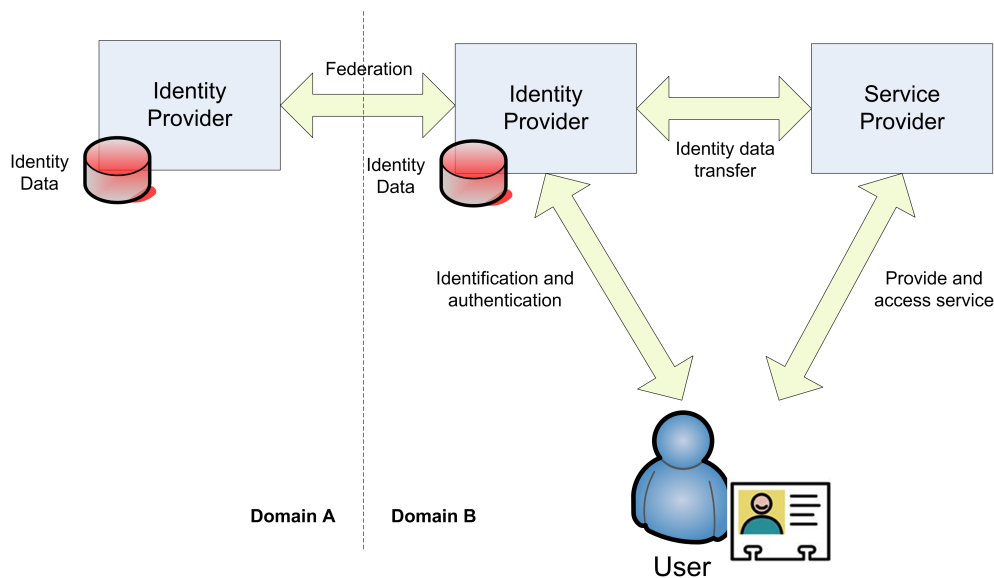


Figure 3.8: Federated Model

3.4 Single Sign-On and Single Logout

Single Sign-On (SSO) and *Single Logout* (SLO) are frequent processes in authentication scenarios to increase usability and to provide users a more comfortable authentication and logout process. In this section, the processes of single sign-on and single logout are briefly elaborated.

3.4.1 Single Sign-On

An increasing number of service providers rely on user authentication before their services can be accessed. The reason can be either just securing their services or personalization. Since these services or applications are generally offered by different service providers, a user usually needs to authenticate at each provider separately. Taking the username/password authentication scheme as an example, a user needs to remember a single password for each service provider. Over time, this can lead to an increasing number of passwords a user has to remember. Due to that, most users tend to choose easy-to-remember passwords or to re-use one password for different service providers. This tremendously leads in a lack of security.

To overcome this issue, the concept of *single sign-on* (SSO) was developed. Clercq [2002] defines single sign-on as: "the ability for a user to authenticate once to a single authentication authority and then access other protected resources without reauthenticating". In other words, with the help of single sign-on users get the ability to authenticate in a distributed network or system just once but still get access granted to other different protected resources. The access to other resources happens automatically, seamlessly, and more or less transparent (depending on the SSO implementation) to the user. Going back to the example of username/password authentication, a user needs to remember only one password with high strength instead of multiple easy to remember passwords. This heavily increases security.

In the following, advantages and disadvantages of SSO according to Clercq [2002]; Anchan and Pegah [2003]; Linden and Vilpola [2005] are discussed. On the one side, single sign-on saves time

⁷<http://shibboleth.net>

and costs because users just need to run through one authentication process only. Security is usually increased because authentication takes place on a single place which should be particularly protected. Users do not need to remember several different passwords anymore but can just use a strong one only. However, on the other side this leads to one main disadvantage of single sign-on systems: if an attacker figures out the identity and authentication data of the SSO system, the attacker will be able to gain access to all services protected by the SSO system. Table 3.2 lists some advantages and disadvantages of SSO systems referring to Clercq [2002]; Tsoikas and Schmidt [2010].

Table 3.2: Advantages and Disadvantages of SSO [Clercq, 2002; Tsoikas and Schmidt, 2010]

Advantages	Disadvantages
<ul style="list-style-type: none"> • Only one credential required for multiple authentications • Higher security since stronger credentials can be used • Greater user comfort and higher productivity because only one authentication process must be run through • Less time consuming authentication processes 	<ul style="list-style-type: none"> • Identity provider is central point of failure or attack • If an attacker can steal the SSO credentials, the attacker gets access to multiple protected resources • Merging systems to achieve SSO can be complex due to interoperability constraints

3.4.1.1 Systems

By this time, several SSO architectures have already evolved. All have different characteristics and different underlying architectures. Clercq [2002] gives a good overview on different architectures. In this section, a differentiation of architectures and systems, respectively, is given based on the work of Pashalidis and Mitchell [2003]. Principally, Pashalidis and Mitchell [2003] distinguish between *pseudo-SSO* systems and *true-SSO* systems.

Pseudo-SSO system: A pseudo-SSO system merely is some kind of middleware between a user and one or more service providers. If a user wants to access an application of a service provider, the user has to authenticate at the pseudo-SSO system first. According to Pashalidis and Mitchell [2003], this first authentication process is called *primary authentication*. All other authentication processes are *secondary*, as they are carried out by the pseudo-SSO system. The pseudo-SSO system manages and maintains the respective user credentials for the individual service providers and presents them to the service provider on demand. Depending on the authentication mechanism, these can be username/password pairs, X.509 certificates, etc. Locally installed password managers are a typical example implementing this approach.

True-SSO system: A true-SSO system also acts as intermediary between a user and one and more service providers. In this system, primary authentication is carried out at an identity provider. The identity provider thereby has a trust relationship with all those service providers that want to enable SSO authentication. In most cases, establishment of such trust relationships is done on organizational level without technical means. Main difference between a pseudo-SSO system and a true-SSO system is that in the true-SSO system primary authentication takes place at the identity provider. No further "real" authentication is carried out at subsequent service providers. In a true-SSO system, service providers authenticate users based on assertions issued from the identity

provider, which contain user's identity and authentication information [Pashalidis and Mitchell, 2003]. These assertions are transferred from the identity provider to the service provider through a secure channel. Current implementations of this type of system are *SAML*, *CAS*, or *OpenID* (cf. Sections 3.5.2, 3.5.7, and 3.5.3).

3.4.2 Single Logout

Single logout (SLO) or *global logout* can be seen as the contrary process to single sign-on. The logout process is called single logout if the user wants to logout from all service providers she is currently logged in [Suoranta et al., 2013].

Although this process seems natural, many SSO protocols still neglect this functionality. Currently, only SAML, CAS, and WS-Federation (cf. Section 3.5.8) support this functionality. If single logout is not supported, users can only logout at the individual service providers separately. Hence, still multiple logout processes would be required even if the user had been logged in via single sign-on.

Having no single logout mechanism can have severe security implications. Users usually do not know that – if they press a logout button – that they are only logged out at one application and not at all they have been logged in. For instance, if a user uses multiple single-sign on authenticated services at a public workstation and she just logs out at one service, a subsequent user can easily get access to the other authenticated services of the previous user [Linden and Vilpola, 2005]. The only possibility to avoid such a situation would be closing all web browser windows [Linden and Vilpola, 2005]. Hence, this is one reason why SLO should not be neglected when designing a SSO system.

3.5 Identity Protocols

Basically, identity protocols facilitate the secure exchange of identity and authentication data of a user between a service provider and an identity provider. Depending on the authentication process, these data can become considerably complex. It is thus reasonable to have a common understanding and an appropriate structure of the data to be exchanged according to a well-defined and standardized identity protocol. Figure 3.9 illustrates the communication path where identity protocols are applied in typical identity management scenarios. For simplicity, identity data transfer are illustrated as direct communication channel between identity provider (IdP) and service provider (SP). However, identity data can also be transferred between these entities through the user as intermediary.

Currently, the most dominant identity protocol applied in the field is the *Security Assertion Markup Language* (SAML)⁸. Its dominance and prevalence across Europe has been proven by an empirical study carried out by Zwattendorfer et al. [2012d]; Ivkovic and Zwattendorfer [2009]. Besides SAML, various other approaches for the secure exchange of identity and authentication data exist. *OpenID*⁹, *OAuth*¹⁰, *OpenID Connect*¹¹, *WS-Federation*¹², or *CAS*¹³ are further popular examples. Most of these protocols find use also in the cloud domain, for details on the cloud adoption the author refers to Section 7. In the following subsection, basics of the individual protocols are described and finally the protocols are compared amongst each other according to different selected criteria.

⁸<http://saml.xml.org>

⁹<http://openid.net>

¹⁰<http://oauth.net>

¹¹<http://openid.net/connect>

¹²<http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html>

¹³<http://www.jasig.org/cas>

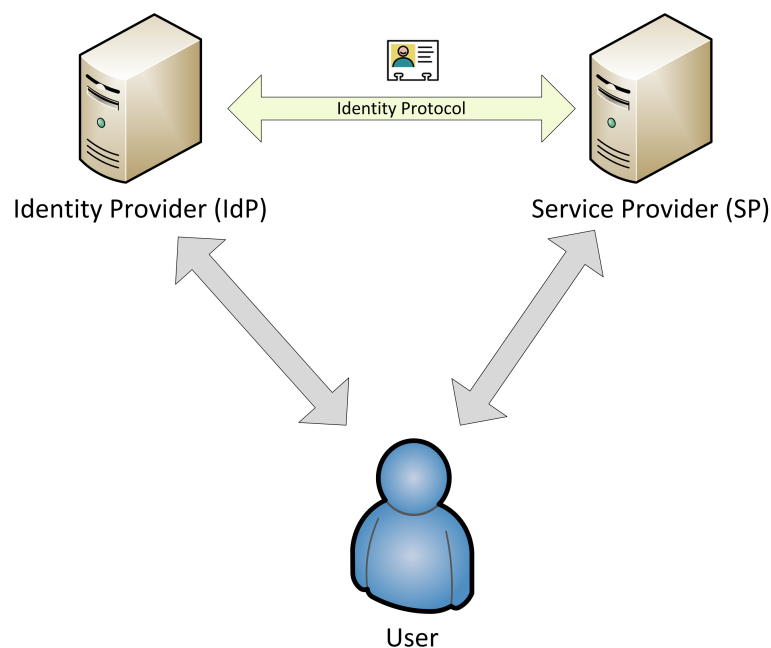


Figure 3.9: Identity Protocols Application

3.5.1 Terminology

Although all mentioned protocols aim on secure identification and authentication of users and the corresponding data transfer, they usually make use of different terminology for individual involved entities or stakeholders respectively. To get a common understanding of the heterogeneous terminology, the following Table 3.3 overviews the different, but in fact semantically equivalent terms used in all protocols. As a reference, the terms that have been described in Section 3.1.4 are used.

Table 3.3: Terminology of different identity protocols

Component	SAML	OpenID	OAuth	OpenID Connect	WS-Federation	CAS
Service Provider (SP)	Service Provider	Relying Party	Client	Client	Resource Provider (Relying Party)	Web Service
Subject	Subject	End User	Resource Owner	Resource Owner	Requestor (User)	User
Identity Provider (IdP)	Identity Provider	OpenID Provider	Authorization Server AND Resource Server	Authorization Server AND Resource Server	Security Token Service (Identity Provider)	Central Authentication Server

In contrast to all other identity protocols, OAuth focuses on authorization and not on pure authentication. Because of that, OAuth distinguishes in its architecture between an entity (authorization server), which enforces an authorization decision, and an entity (resource server), which stores protected resources or identity data respectively. In contrast to that, SAML encapsulates both functionality in one entity (identity provider). Hence, both OAuth entities together (authorization server and resource server) can be seen as identity provider. This way of looking on OAuth will also be used in the following sections.

3.5.2 SAML

SAML (Security Assertion Markup Language) [Cantor et al., 2009b] constitutes an XML-based standard that has been developed by OASIS¹⁴ and that has been especially designed for the secure exchange of authentication and authorization data of a given *subject*. A subject in SAML terminology defines the main actor for whom identity and authentication data needs to be exchanged. Usually this term concerns a natural person but it can also be a web service or a system in general [Madsen et al., 2005].

Historically, SAML originates out of two markup languages, which had been specified already before the development of SAML, namely S2ML (Security Services Markup Language) [Mishra et al., 2001] and AuthXML [Prodromou et al., 2000]. Both aimed for the realization of secure business transactions in the e-Commerce sector using XML. The first version of SAML (version 1.0) [Hallam-Baker and Maler, 2002] was published in 2002. An amended version (version 1.1) [Maler et al., 2003] was introduced in 2003. The current version, which is widely used at the moment, is version 2.0. This version was published in March 2005 and focus has been laid on federated identity (cf. Sections 3.1.4.3 and 3.3.4). Version 2.0 was influenced by experiences of other specifications and projects, namely by the *Shibboleth*¹⁵ project and the *Liberty Alliance* project¹⁶. In the meantime, the SAML specifications have continuously improved and several errata documents exist [Hardjono et al., 2012].

According to the general identity protocol application (cf. Figure 3.9), authentication or authorization data are typically exchanged between one *identity provider* and one or more *service providers*. The identity provider is usually responsible for the subject's authentication and the issuance of so-called SAML assertions for authentication requesting service providers. A SAML assertion [Cantor et al., 2009b] is an XML-based security token, which assures that a certain subject has been successfully authenticated using specific means at a certain point in time. Furthermore, the subject can own specific attributes e.g., if authorization is required. Service providers that receive such assertions verify it and grant or deny access to the resources that have been requested by the subject. In SAML terminology, identity providers are also called *asserting party* or *SAML authority*, service providers can also be named *relying party*.

Summarizing, the most important features of SAML are [Lockhart et al., 2008]:

- *Single sign-on (SSO)*
Single sign-on (cf. Section 3.4.1) defines the ability to authenticate in a distributed system or network only once by still gaining access to multiple services without re-authentication. In web-based systems SSO is usually achieved by storing browser cookies. However, this approach is limited to single DNS domains only as cookies cannot be shared across domains. SAML solves this issue by applying standardized protocols for the exchange of authentication information independent of DNS domains.
- *Identity federation*
The term identity federation constitutes the federation of user information between entities across security domains (cf. Section 3.3.4). In that case, user information is shared and exchanged between those entities, but necessarily not the same amount of data and identity information are stored at the individual entity. Hence, not every entity needs to save and maintain user data on its own. Usually, entities agree on such an exchange based on a common identifier.
- *Web services and other industry standards*
The SAML specification has been designed in such a flexible and modular way that SAML message exchange is not strongly limited to SAML protocols but can also be used within other frameworks. A typical example is securing web service messages within WS-Security [Lawrence et al., 2006] tokens.

¹⁴Organization for the Advancement of Structured Information Standards, <http://www.oasis-open.org>

¹⁵<http://shibboleth.internet2.edu>

¹⁶<http://www.projectliberty.org>

All Liberty Alliance work has now been transferred to the Kantara Initiative, <http://kantarainitiative.org>

3.5.2.1 SAML Architecture

SAML highly profits from its modular architecture. Due to this modularity, various components can be put together and appropriate solutions for different use cases can be modeled. Figure 3.10 illustrates this nested architectural model, where statements specify the most detailed and profiles the highest abstract level. The following enumeration gives a brief introduction into the individual SAML components according to Lockhart et al. [2008].

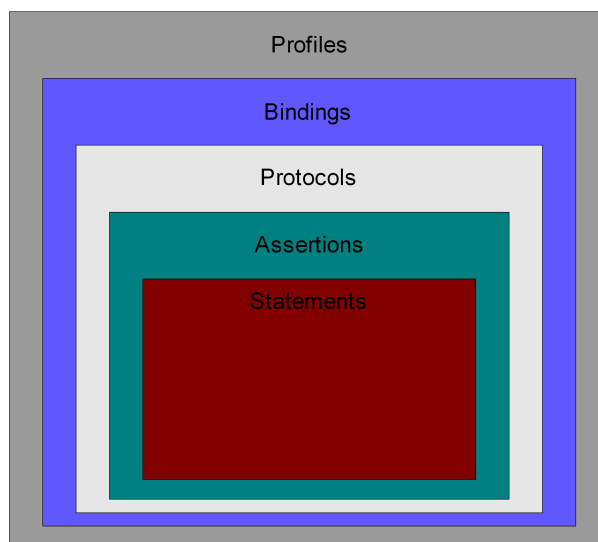


Figure 3.10: SAML Architecture [Ivkovic and Zwattendorfer, 2009; Lockhart et al., 2008]

Assertions: So-called SAML assertions [Cantor et al., 2009b] constitute the core component of SAML. SAML assertions contain specific information about a subject e.g., subject-related special attributes or information indicating that the subject has been successfully authenticated. In typical scenarios, assertions are issued by an identity provider and consumed by a service provider, which uses the included information for access control decisions of the subject.

Basically, three different types of SAML assertions can be distinguished although the wrapping XML-fragment is common to all of them. A differentiation on the assertion is made based on the statements (see Figure 3.10) included. The SAML specification distinguishes between the following three statements:

- Authentication Statement
- Attribute Statement
- Authorization Decision Statement

Authentication statements are usually created by an identity provider if a subject has been authenticated successfully. The statement contains information at what point in time and by which means the subject has authenticated and specifies the validity period of the assertion. *Attribute statements* wrap specific attributes belonging to the authenticated subject. Additionally, *authorization statements* can give information whether the subject is permitted to gain access to a certain resource or not. Although authorization statements have especially been designed for access control, in practice mainly attribute statements are used for authorization. There is also no strict regulation to use only one statement per assertion. Hence, different statements can be mixed. However, there is a limitation to one authentication statement only.

Listing 3.1 illustrates the structure of an assertion including an authentication statement. In fact, this assertion issued by `http://www.idp.com` assures that the user identified by the e-mail

address *john.doe@test.com* was successfully authenticated on April 3, 2014 at 11:00 using a password-based authentication mechanism. The assertion's validity is 30min.

List of Listings 3.1: Sample SAML Assertion

```

1 <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
2   Version="2.0" IssueInstant="2014-04-03T11:00:00Z">
3   <saml:Issuer Format=urn:oasis:names:SAML:2.0:nameid-format:entity>
4     http://www.idp.com
5   </saml:Issuer>
6   <saml:Subject>
7     <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:
8       emailAddress">
9       john.doe@test.com
10    </saml:NameID>
11  </saml:Subject>
12  <saml:Conditions>
13    <saml:ConditionsNotBefore="2014-04-03T11:00:00Z" NotOnOrAfter="
14      2014-04-03T11:30:00Z">
15    </saml:ConditionsNotBefore>
16  </saml:Conditions>
17  <saml:AuthnStatement AuthnInstant="2014-04-03T11:00:00Z"
18    SessionIndex="77777777">
19    <saml:AuthnContext>
20      <saml:AuthnContextClassRef>
21        urn:oasis:names:tc:SAML:2.0:ac:classes:
22        PasswordProtectedTransport
23      </saml:AuthnContextClassRef>
24    </saml:AuthnContext>
25  </saml:AuthnStatement>
26 </saml:Assertion>

```

Protocols: SAML Protocols [Cantor et al., 2009b] define the next layer in this modular architecture.

They specify which assertion is transmitted between two providers or entities and also define how this transmission takes place. SAML assertions can be either pulled from or pushed by an identity provider. If pulled, the service provider requests an assertion from the identity provider. If using the push method, the identity provider sends unsolicited assertions to the service provider without any further request.

Bindings: SAML Bindings [Cantor et al., 2009a] depict the transport protocol used for carrying the SAML protocol messages. These protocols remain untouched by the SAML specification and are just used for transportation. Typical examples for such transport protocols are HTTP or SOAP web services.

Profiles: SAML Profiles [Hughes et al., 2009] combine all inner parts (statements, assertions, protocols, bindings) of the modeling architecture to model certain use cases. The most popular use case or profile, respectively, depicts the so-called *Web Single Sign-On Profile* [Hughes et al., 2009], which enables users single sign-on across multiple applications and domains by using web browsers.

The main advantages of SAML are its wide and broad adoption (several implementations exist since years) and high modularity for being able to model and profile individual use cases. Furthermore, its extensive specifications include definitions for metadata, identity provider discovery, or single logout support. However, this can also be seen as one disadvantage because a huge set of specifications is not easy to understand and to implement. Moreover, extending SAML requires detailed profiling to tailor the existing specifications to model the required use case. Finally, because of the use of XML, SAML is more heavy-weight and thus is less adoptable for mobile clients.

3.5.3 OpenID

OpenID [OpenID Foundation, 2007] defines a decentralized authentication system for web-based and OpenID enabled services. Currently, OpenID is specified in version 2.0. Version 2.0 was finalized in 2007. Again, OpenID enables single sign-on. Users just need to authenticate once at so-called OpenID providers, which are in fact identity providers according to Table 3.3, for accessing multiple protected resources or services. OpenID relies on URL-based or XRI-based identities and identifiers. In fact, an OpenID username or identifier, respectively, follows the syntax of an URL or XRI (Extensible Resource Identifier) [Reed et al., 2005].

The fundamental principle in an OpenID authentication scenario is the OpenID identifier. The OpenID identifier is issued to users by an OpenID provider during registration. For authentication, users need to provide this identifier to a relying party (service provider) if they want to access a protected resource. The identifier is usually simply entered into an OpenID login form provided by the relying party. Based on the OpenID identifier, the relying party is able to forward the user to the corresponding OpenID provider for authentication. The location and endpoint of the OpenID provider is determined and extracted out of the OpenID identifier. Afterwards, the user authenticates at the OpenID provider using appropriate credentials. No particular authentication mechanism is specified, however, most OpenID providers rely on username/password schemes. Nevertheless, also stronger authentication mechanisms such as national eIDs could be supported. After successful authentication, user's identification and authentication information is returned from the OpenID provider to the relying party. If the user wants to authenticate at another relying party using the same OpenID provider, the user just needs to provide her OpenID identifier again at the other relying party. Authentication is then carried out seamlessly and without further user interaction, which corresponds to single sign-on.

One advantage of OpenID is that users do not need to rely on a specific OpenID provider but can use the particular provider of their choice. More precisely, due to the decentralized architecture and the open specification, users are able to simply setup their own OpenID provider and use it for authentication. The OpenID specification is also flexible, hence the specifications can easily be extended and amended. OpenID is already widely deployed in the field. According to Kissel [2009], 9 million web sites that have incorporated OpenID login and approximately 1 billion OpenID user accounts existed by 2009. However, although OpenID has been widely adopted in the field user acceptance is still lacking. In addition, security features are specified as optional only. Furthermore, OpenID does not specify explicit application registration and application authentication with respect to the OpenID provider. Finally, single logout functionality is neither specified nor supported.

3.5.4 OAuth

The first draft version of *OAuth* was published in 2007, whereas the final version 1.0 was released as RFC 5849 [Hammer-Lahav, 2010] in 2010. The current version 2.0 was published as RFC 6749 [Hardt, 2012] two years later in 2012. Version 2.0 is not backwards compatible to version 1.0. The main idea of OAuth is enabling various client applications (e.g., web, desktop, or mobile applications) easy access to protected resources and data of end users. Hence, OAuth actually focuses more on authorization than authentication because a user can authorize a client application to access and retrieve user data from a resource server. However, in this section the author still briefly mentions OAuth since the next protocol – OpenID Connect – focuses on authentication instead of authorization and uses OAuth as underlying framework.

The OAuth core specification is RFC 6749 [Hardt, 2012]. Similar to the specifications of the other identity protocols, several supplementary documentation and specifications exist, which extend and amend the functionality of OAuth in different areas. In contrast to the general architecture shown in Figure 3.9, the OAuth framework actually involves four entities. According to Hardt [2012], these are the *resource owner* (subject/user), the *client* (service provider), an *authorization server*, and a *resource*

server. Equally to the other protocols, the authorization server and the resource server form together the identity provider. The resource server stores protected resources whereas the authorization server is responsible for managing access to the protected resources of the resource server. In the following, a typical authorization process using OAuth and these four components are briefly described according to Hardt [2012].

In a typical authorization process, a client application (web, desktop, or mobile application) wants to access protected resources which belong to a resource owner (user) and which are stored on a resource server. In a first step, the client application requests authorization from the resource owner. Thereby, the user is forwarded to the authorization server. At the authorization server the user has to authenticate and has to decide either granting or denying authorization for the client application to access data on the resource server. If the user grants access and the client could be authenticated by the authorization server, the authorization server generates a so-called *access token*. The access token is further transmitted to the client. The client can use this access token for accessing protected resources on the resource server. The resource server validates the token and – if valid – is able to provide the requested data.

One advantage of OAuth is its broad adoption, thus many implementations exist. Furthermore, due to the use of HTTP and JSON (JavaScript Object Notation) the integration into mobile clients is easier than with XML-based protocols. The openness and flexibility of the specification can be seen as one disadvantage because the specifications allow for room of interpretation and thus additional profiling is required. Finally, security features are usually not required to implement when using OAuth out of the box.

3.5.5 OpenID Connect

OpenID Connect [Sakimura et al., 2014] is a very new specification since the final version 1.0 was adopted in February 2014. Although its name may mistakenly lead to the assumption that OpenID Connect is an extension to OpenID, the OpenID Connect specifications rather build upon the OAuth 2.0 protocol. OpenID Connect constitutes a lightweight protocol and framework for the secure exchange of identification and authentication data via a REST-API. The functionality of OAuth 2.0 is completely included in the specifications but also OpenID 2.0 functions can be integrated by applying appropriate extensions.

OpenID Connect supports different clients for the exchange of identity information e.g., browser-based, mobile, or JavaScript clients. Principally, equally to OAuth also OpenID Connect relies on SSL/TLS as underlying secure transport protocol for secure message exchange. The current specifications are extensible, i.e. OpenID Connect can be extended and amended to support message encryption, identity provider discovery, or logout.

A sample authentication process flow is as follows [Sakimura et al., 2014]: A service provider (relying party, client) wants to access information stored at an identity provider¹⁷. Therefore, an appropriate authorization request is sent from the service provider to the identity provider. The identity provider asks the user for authentication and authorization. The identity provider responses to the authorization request of the service provider with an ID token and an access token. The ID token already includes user information such as a personal identifier or the user's name. The access token can be used in subsequent process steps to request further user information from the identity provider (as done in pure OAuth).

The advantages and disadvantages of OpenID Connect are similar to the ones of OAuth. OpenID Connect allows easy adoption for mobile clients due to the use of lightweight protocols such as HTTP and JSON instead of XML. However, since the specifications are rather new only a few implementations are available and thus experience must still be gained before broad adoptions. Finally, single logout features are excluded within its specifications.

¹⁷For simplicity, under the term identity provider the combination of authorization server and resource server is subsumed.

3.5.6 WS-Federation

The current version of *WS-Federation* [Goodner and Nadalin, 2009] is 1.2, which was published in 2009. WS-Federation is part of the WS-* specifications (WS-Trust, WS-Security, WS-Policy, etc.) and extends WS-Trust by the possibility of a flexible federated identity management architecture. According to Goodner and Nadalin [2009], WS-Federation “*defines mechanisms to allow different security realms to federate, such that authorized access to resources managed in one realm can be provided to security principals whose identities are managed in other realms*” [Goodner and Nadalin, 2009]. In other words, principals belonging to one security realm are allowed to access protected resources in another security realm or domain if a trust relationship between those realms exists.

To achieve that, for authentication and authorization WS-Federation also relies on the model of a *Security Token Service* (STS), which is used as trusted service throughout the overall WS-* specifications. Thereby, WS-Federation extends the model of an STS by identity management requirements in such a way that the specifications can be used by web services as well as web browsers. The WS-Federation specification explains appropriate trust relationships, the format of exchanged security tokens, and applicable transport protocols. Regarding the architecture, WS-Federation is similar to SAML. On the one hand, WS-Federation also uses XML and SOAP, and, on the other hand, profiles supporting appropriate use cases are defined.

In general, WS-* or WS-Federation aim on the secure exchange of web service messages across different security domains or realms. The use of a web browser (passive requestor) as client is a special use case in the specifications. The secure exchange of messages across trust boundaries using a web browser is specified in the *Passive Requestor Profile* [Goodner and Nadalin, 2009].

In a sample authentication scenario, a user (resource requestor) belonging to security realm A wants to access a protected resource in security realm B. Between both security realms an appropriate trust relationship has been established before. According to the *Passive Requestor Profile* [Goodner and Nadalin, 2009], three entities are involved in an authentication process. The identity provider (including an STS) and the user belong to security realm A, whereas the resource provider that hosts the protected resource belongs to security realm B. The user of realm A, who wants to access a protected resource in realm B, is redirected to the STS of the identity provider in realm A. The user authenticates at the identity provider and the STS issues a security token for realm B and thus for the resource provider. The resource provider verifies the security token and either grants or denies access to the protected resource based on the information in the token.

WS-Federation has a comprehensive specification and thus supports numerous use cases. Compared to the other protocols – except SAML – it includes a specification document for metadata. However, the comprehensive specifications can also be disadvantageous because they may be hard to implement. Another disadvantage is that WS-Federation is heavyweight because – equally to SAML – XML is used for modeling messages. The use of XML also lowers the applicability for mobile clients. Finally, WS-Federation has not reached broad adoption and acceptance over the past years, hence also only a few implementations exist.

3.5.7 CAS

The *Central Authentication Service* (CAS) [Mazure et al., 2005] has been originally developed by the University of Yale and is now maintained by Jasig (Java Architectures Special Interest Group)¹⁸. CAS depicts a SSO solution based on web technologies. The functionality with respect to SSO is mainly defined in version 1.0 of the protocol. Version 2.0 aims on proxy authentication on various levels and can be seen as an extension to version 1.0. Version 2.0 is fully backwards compatible to version 1.0.

¹⁸<http://www.jasig.org>

Users just need to authenticate once at a so-called CAS server (identity provider), usually by providing username/password. To permit access to multiple applications the CAS server issues security tickets that can be verified by the respective application. In detail, a CAS authentication flow is as follows [Mazure et al., 2005]: A user wants to access a protected resource at a service provider. Since no authentication context exists between the user and the service provider, by clicking on a URL the user is redirected to the CAS server. The CAS server authenticates the user using appropriate means. After successful authentication, the CAS server generates a security ticket and forwards the user back to the service provider including the security ticket. The service provider transmits the received security ticket directly to the CAS server. The CAS server verifies the ticket and returns appropriate user information to the service provider.

Main advantage of CAS is probably its easy to implement specification and protocol. Furthermore, because CAS relies on HTTP parameters only, data packets transferred between entities are small. Finally, single logout functionality is specified. Nevertheless, also some disadvantages can be found. CAS supports security features only optionally and the transferred identity data are limited to usernames. Finally, no explicit application registration at the CAS server is supported.

3.5.8 Comparison of Identity Protocols

In this section, the described identity protocols are compared and evaluated amongst each other according to selected criteria (functional, organizational, and technical criteria). In the following subsections, first the evaluation criteria are defined and explained, and subsequently the evaluation is presented. For comparison and evaluation, always the default specification of the individual protocols has been taken as a basis. Some properties or features can still be fulfilled or improved if optional parts of the specification are implemented or the specifications are extended and amended according to specific needs.

3.5.8.1 Evaluation Criteria

In the following, the evaluation criteria are defined and explained. The following general notations are applied for the evaluation:

- X ... Criterion, feature, or functionality is supported
- L, M, H ... Low, Medium, High

Table 3.4 gives details on functional, Table 3.5 on organizational, and Table 3.6 on technical evaluation criteria.

Table 3.4: Functional evaluation criteria

Functional Criterion	Description
<i>Security</i>	Security features (e.g., use of SSL/TLS, digital signatures, etc.) in the specification are <ul style="list-style-type: none"> • L ... not included. • M ... optionally included. • H ... mandatory included.
<i>Extensibility</i>	Extensibility of the specifications is <ul style="list-style-type: none"> • L ... foreseen. • M ... optional. • H ... necessary.
<i>Single sign-on (SSO)</i>	X ... Single sign-on is supported.
<i>Single logout (SLO)</i>	X ... Single logout is supported.
<i>User consent</i>	Giving user consent is <ul style="list-style-type: none"> • L ... not possible. • M ... optional. • H ... mandatory.

Table 3.5: Organizational evaluation criteria

Organizational Criterion	Description
<i>Format of the identifier</i>	The format of the identifier is <ul style="list-style-type: none"> • L ... not specified. • M ... partially specified. • H ... completely specified.
<i>Format or names of additional user attributes</i>	The format or names of additional user attributes are <ul style="list-style-type: none"> • L ... not specified. • M ... partially specified. • H ... completely specified.
<i>Level of adoption/distribution</i>	The protocol/specification has <ul style="list-style-type: none"> • L ... little adoption. • M ... medium adoption. • H ... wide adoption.
<i>Open source libraries</i>	Open source libraries are <ul style="list-style-type: none"> • L ... not available. • M ... occasional available. • H ... available in different programming languages.
<i>Interoperability</i>	X ... Interoperability between implementations is tested.
<i>Metadata</i>	X ... Metadata are specified.
<i>Registration of applications</i>	Registration of applications is <ul style="list-style-type: none"> • L ... not required. • M ... not exactly specified. • H ... specified.

Table 3.6: Technical evaluation criteria

Technical Criterion	Description
<i>Data exchange format</i>	The data exchange format will be declared quantitatively.
<i>Bindings</i>	Possible bindings are declared qualitatively.
<i>Transfer protocol</i>	Possible transfer protocols are declared qualitatively.
<i>Token size</i>	Approximate token sizes are stated quantitatively.
<i>Identity provider (IdP) discovery</i>	X ... IdP discovery is supported.
<i>Authentication of the application</i>	Authentication of the application is <ul style="list-style-type: none"> • L ... not required. • M ... not exactly specified. • H ... specified.
<i>SP-initiated/IdP-initiated</i>	The protocol supports the initiation of an authentication process by an <ul style="list-style-type: none"> • SP • IdP

3.5.8.2 Evaluation

The following Tables 3.7, 3.8, and 3.9 evaluate and compare the different identity protocols with respect to the prior defined criteria.

Table 3.7: Comparison with respect to functional criteria

Protocol / Functional Criterion	SAML 2.0	OpenID 2.0	OAuth 2.0	OpenID Connect 1.0	WS-Federation 1.2	CAS 1.0
<i>Security</i>	H	M	M	H	H	L
<i>Extensibility</i>	H	H	H	H	H	M
<i>Single sign-on (SSO)</i>	X	X	X	X	X	X
<i>Single logout (SLO)</i>	X				X	X
<i>User consent</i>	M	M	M	M	M	M

Discussing Table 3.7, basically all of the evaluated protocols can be used for the transfer of identification and authentication data between service provider and identity provider. High security based on the default specifications deliver SAML, OpenID Connect, and WS-Federation. By appropriate extensions and profiling also other protocols can reach a high security level. All protocols are easily extendable, except CAS, where extensions are actually not foreseen. Single sign-on is supported by all protocols. However, the pendant single logout is supported by SAML, WS-Federation, and CAS only. Giving user consent is optionally possible in all protocols.

Referring to Table 3.8, the format of the identifier is partially specified in all protocols, except in OAuth. OAuth focuses on authorization, hence data transferred must not necessarily be related to identification and authentication processes. The format or names of additional user attributes are mostly not specified. However, OpenID, OpenID Connect, and WS-Federation specify additional user attributes and names in more detail. The level of adoption is high for SAML, OpenID, and OAuth. The adoption of OpenID Connect and WS-Federation is low. The final specification of OpenID Connect is rather new, and WS-Federation did not get generally accepted. In addition, CAS can mostly be found in university

Table 3.8: Comparison with respect to organizational criteria

Protocol / Organizational Criterion	SAML 2.0	OpenID 2.0	OAuth 2.0	OpenID Connect 1.0	WS-Federation 1.2	CAS 1.0
<i>Format of the identifier</i>	M	M	L	M	M	M
<i>Format or names of additional user attributes</i>	L	H	L	M	M	L
<i>Level of adoption/distribution</i>	H	H	H	L	L	M
<i>Open source libraries</i>	H	H	H	L	M	H
<i>Interoperability</i>	X	X			X	
<i>Metadata</i>	X				X	
<i>Registration of applications</i>	H	L	M	H	H	M

environments only. The level of distribution also reflects the availability of open source libraries. Thus, for widely adopted protocols also several open source libraries in different programming languages exist. Explicit interoperability tests are made only occasionally, i.e. for SAML, OpenID, and WS-Federation. Metadata are specified in two protocols only, namely in the two XML-based ones SAML and WS-Federation. Application registration is also specified in these two protocols and in addition in OpenID Connect. In the other protocols registration of applications is either not necessary (OpenID) or not specified (OAuth, CAS).

Table 3.9: Comparison with respect to technical criteria

Protocol / Technical Criterion	SAML 2.0	OpenID 2.0	OAuth 2.0	OpenID Connect 1.0	WS-Federation 1.2	CAS 1.0
<i>Data exchange format</i>	XML	URL-Parameter	URL-Parameter, JSON	URL-Parameter, JSON	XML	URL-Parameter
<i>Bindings</i>	SOAP, HTTP-Redirect, HTTP-POST, etc.	URL-Parameter	URL-Parameter (GET and POST)	URL-Parameter (GET and POST)	URL-Parameter (GET and POST)	URL-Parameter
<i>Transfer protocol</i>	HTTP, SOAP	HTTP	HTTP	HTTP	HTTP	HTTP
<i>Token size</i>	> 1 KB	> 500 Bytes	> 50 Bytes	> 100 Bytes	> 1 KB	> 10 Bytes
<i>Identity provider (IdP) discovery</i>	X	X		X	X	
<i>Authentication of the application</i>	H	L	M	M	H	H
<i>SP-initiated/IdP-initiated</i>	SP, IdP	SP	SP	SP	SP	IdP

According to Table 3.9, the data exchange format is XML for SAML and WS-Federation, whereas the other protocols rely on HTTP parameters and URL parameters only. In addition to these parameters, OAuth and OpenID Connect support the exchange of JSON tokens. The format also influences the size

of a transmitted token, varying between a few bytes and several kilobytes. As transfer protocol, mainly HTTP is used. Only SAML supports the transfer of SAML messages over SOAP too. The different protocols rely on both front-channel and back-channel bindings. Front-channel bindings are only applied in OpenID and WS-Federation. IdP discovery is supported by SAML, OpenID, OpenID Connect, and WS-Federation. In OpenID, IdP discovery is part of the default protocol. Authentication of applications is specified in most protocols. However, in OAuth and OpenID Connect this is not explicitly regulated and OpenID does not necessarily require application authentication.

Further comparisons and evaluation of identity protocols and identity management systems – also including PRIME (cf. Section 5.4.4) or Windows CardSpace – can be found in Ferdous and Poet [2012].

3.6 Electronic Identity in Austria

Unique identification and secure authentication plays an important role within the Austrian e-Government concept. In particular, since sensitive citizen data are processed, unambiguous citizen identification is essential in G2C scenarios and corresponding e-Government procedures. The Austrian e-Government concept foresees a thorough eID concept based on the Austrian citizen card, the official eID in Austria [Leitold et al., 2002], enabling secure identification and authentication of citizens in Austrian e-Government applications. Moreover, the Austrian eID concept also contains representative authentications and authentications of foreign EU citizens, which are treated equally to Austrian citizens in e-Government scenarios. This section overviews the Austrian eID and citizen card concept and gives details on the individual identification and authentication scenarios.

3.6.1 The Austrian eID Concept

Secure and privacy-preserving identification and authentication are key features of the Austrian citizen card. The citizen card representing the Austrian national eID relies on existing unique identifiers that are further used to derive sector-specific identifiers. Unique identifiers are essential as identification based on first name, last name, and date of birth may be ambiguous, especially when the number of users increases. Therefore, in Austria all citizens are registered in the *Central Register of Residence* (CRR) and have a 12-character (40-bit) unique number assigned (*CRR-Number*). The CRR-Number acts as unique identifier for these citizens.

Due to data protection restrictions, the CRR-Number must not be directly used in e-Government processes. Therefore, the CRR-Number is encrypted to derive a new unique identifier. In detail, it is a 168-bit Triple-DES (3DES) encryption [Barker and Barker, 2012] of the concatenation of the *CRR-Number* and a 8-bit *seed* value. The encryption function looks as follows [Hollosi and Hörbe, 2007]:

$$sourcePIN = 3DES(CRR - Number || seed || CRR - Number || CRR - Number)$$

The use of the CRR-Number three times is just for enlarging the calculation basis to 128-bit. This new identifier is created by the *SourcePIN Register Authority* (SRA)¹⁹, a subdivision of the *Austrian Data Protection Authority*²⁰. The resulting 128-bit derived identifier is named *sourcePIN* and is also unique for all citizens. The sourcePIN is stored on the citizen card together with other identity related data such as first name, last name, and date of birth. Those identification data and the corresponding citizen's qualified signature keys are wrapped within a special XML-based data structure. This data structure is called *Identity Link* and is electronically signed by the SourcePIN Register Authority. This signature establishes and certifies a link between the identity data and the qualified certificate stored on the citizen card. The Identity Link can be further used for unique identification at online applications.

¹⁹<http://www.stammzahlenregister.gv.at>

²⁰<http://www.dsb.gv.at>

According to the Austrian E-Government Act [Federal Chancellery, 2008], the unique identifying sourcePIN requires special protection to preserve citizen's privacy. A permanent storage of this identifier is only allowed within the Identity Link stored on the citizen card. Hence, for identification at online applications it is forbidden by law to store the sourcePIN permanently. Because of this restriction – due to data protection reasons – the Austrian e-Government strategy foresees a sector-specific model for identification at online applications. Instead of using the sourcePIN directly, a sector-specific identifier is derived from the sourcePIN. This so-called *sector-specific PIN* (ssPIN) is derived from the combination of the *sourcePIN* and a governmental *sector* identifier (e.g. finance, tax, etc.) by using the SHA-1 cryptographic one-way hash function [Gallagher, 2012]. In detail, the resulting 160-bit ssPIN value for sector A is calculated as follows [Hollosi and Hörbe, 2007]:

$$ssPIN_{(A)} = SHA - 1(sourcePIN || sector A)$$

The use of cryptographic hash functions allows for special privacy protection, as the sourcePIN cannot be calculated out of a given ssPIN. In addition, an authority belonging to a specific governmental sector is not able to calculate the ssPIN of another sector, i.e. the ssPIN of the finance sector differs from the ssPIN of the tax sector. Hence, within the Austrian eID concept the ssPIN constitutes the identifier to be finally used for identification at online applications. In some cases, public authorities belonging to different sectors still may need to exchange data of the same user. For this purpose, the Austrian e-Government Act defines the notion of an *encrypted ssPIN* [Federal Chancellery, 2008], i.e. a public authority may use an ssPIN of a different administrative sector only in encrypted form. Details on the algorithms for the calculation of the individual identifiers are described in Hollosi and Hörbe [2007].

The entire Austrian eID concept for natural persons relies on the unique identifier stored in Austria's Central Register of Residence. Austrian citizens living in Austria, and hence being registered in the CRR, are usually the typical use case and were the basic assumption when developing e-Government strategies and concepts in Austria. However, the Austrian eID concept also foresees e-Government applications for persons not listed in the CRR (e.g., foreign citizens or Austrian citizens currently residing in a foreign country). Such persons are not registered in the CRR but can be registered in the so-called *Supplementary Register for Natural Persons* (SR) and get a so-called *SR-Number* assigned. The Supplementary Register for Natural Persons constitutes an additional register for foreign citizens or Austrian citizens living abroad. Through the Supplementary Register for Natural Persons, these persons become part of the Austrian eID infrastructure and thus get the possibility to use e-Government applications in Austria. In more detail, by registering in the Supplementary Register for Natural Persons, they also get a unique sourcePIN by deriving the SR-Number assigned. This way, foreign citizens can be treated equivalently to domestic Austrian citizens in online e-Government applications. In fact, foreign citizens can use online applications and e-Government processes equally to Austrian citizens. The legal basis for that is the so-called E-Government Equivalence Decree [Federal Chancellery, 2010a], which was published and became law in 2010. This decree specifies which foreign electronic IDs can be treated equally to the Austrian eID, i.e. the Austrian citizen card. Figure 3.11 illustrates the privacy-preserving sectoral identifier model in Austria for Austrian citizens and foreign citizens.

Another main pillar of the Austrian eID ecosystem is the usage of electronic mandates. Electronic mandates can be used as electronic representations for natural and legal persons, or for professional representatives. In case of representation of natural persons, the sourcePIN of both the representative and the represented person are taken for modeling the mandate process electronically. However, also legal persons such as companies get a unique number (also called sourcePIN) for governmental processes in Austria. This unique number of a legal person and the sourcePIN of the representative (natural person) are used for mandate generation.

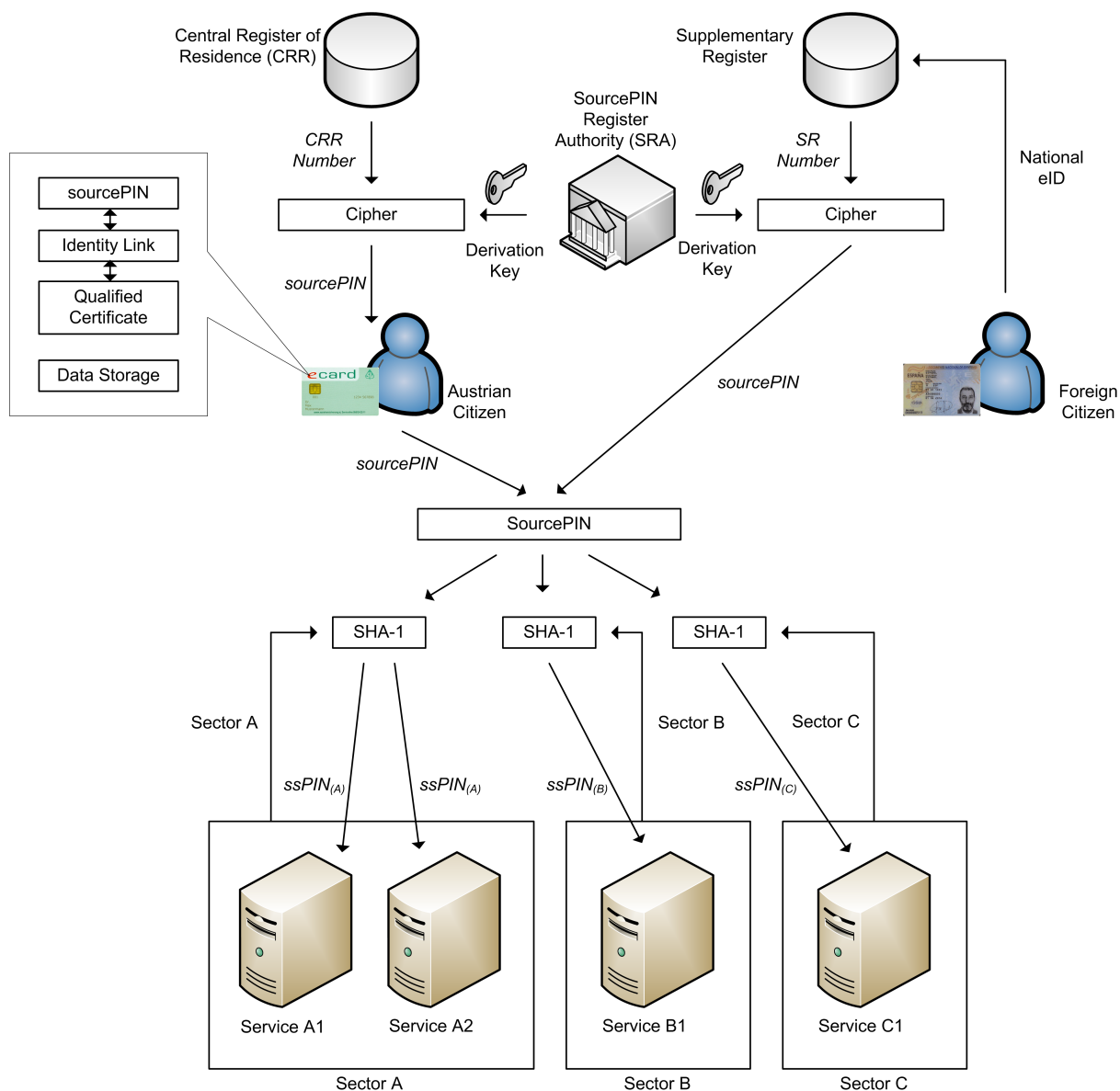


Figure 3.11: The Austrian eID Concept [Tauber et al., 2012]

3.6.2 The Austrian Citizen Card Concept

The Austrian eID concept constitutes one of the key concepts of the Austrian e-Government strategy. The Austrian citizen card [Hollosi et al., 2014], in turn, defines the key concept of the Austrian eID concept. Representing the official eID in Austria, the citizen card is basically an abstract definition of a secure eID token that is in possession of the citizen. Its main capabilities are secure identification and authentication of citizens as well as the creation of qualified electronic signatures according to the EU signature directive [European Parliament and Council, 1999b].

As mentioned above, the citizen card concept is a technology-neutral concept that allows for several different implementations. Currently, smart cards and mobile phones [Orthacker et al., 2010] can be used as citizen card. However, the technology-neutral approach guarantees that also alternative approaches and implementations can be developed and deployed in the future. In the following, citizen card functions and the citizen card model based on the work of Stranacher et al. [2013c] are briefly elaborated. Further details on the citizen card architecture can be found in Leitold et al. [2002].

3.6.2.1 Citizen Card Functions

Irrespective of the actual implementation of the citizen card concept, the Austrian citizen card provides a well-defined set of functionality. In the following, the supported features of the Austrian citizen card are briefly elaborated according to Hollosi et al. [2014]; Stranacher et al. [2013c].

Identification and Authentication of Citizens Unique identification and secure authentication are essential components of governmental processes. In e-Government processes, the citizen card provides technical means for carrying out identification and authentication electronically. By using the citizen card in online applications, user identification is based on the Identity Link. The Identity Link is a special data structure including the citizen's first name, last name, date of birth, and the sourcePIN as unique identifier. The sourcePIN allows for unique identification of users in online procedures. Although the sourcePIN is unique, it must not be used directly for identification at online applications due to legal privacy restrictions (cf. Section 3.6.1).

Security sensitive applications usually require users not only to identify but also to authenticate. Identification and authentication are actually related processes. The claim to be a person is typically referred to as identification (cf. Section 3.1.2.1), while the proof of this claim is referred to as authentication (cf. Section 3.1.2.2). In Austria, the citizen card is not only used for identification but also for electronic authentication. In online processes, authentication is carried out by creating an electronic signature by applying citizen card functionality. The functionality to create electronic signatures using the Austrian citizen card is described in the following.

Secure and Qualified Electronic Signatures Besides proofing a claimed identity, citizens often need to express a written declaration of intent in governmental processes or transactions. This requirement can occur, for instance, when applying for a governmental procedure at the beginning or at the end of such a procedure, when confirming the receipt of results. In traditional paper-based procedures and processes, a written expression of declaration of intent is carried out through hand-written signatures. In electronic processes, the hand-written signature needs some equivalent.

According to the Austrian signature act [Federal Chancellery, 2010c], which constitutes the Austrian implementation of the EU signature directive [European Parliament and Council, 1999b], the electronic pendants to hand-written signatures are qualified electronic signatures. Qualified electronic signatures are equivalent to hand-written signatures by law in most cases, exceptions are, however, procedures targeting family law or inheritance law. In general, electronic signatures are cryptographic mechanisms to express a declaration of intent electronically. According to the EU signature directive, qualified electronic signatures are advanced electronic signatures (cf. Section 2.2.3.1) but are created by using a qualified digital certificate and by invoking a secure signature creation device (SSCD). A qualified digital certificate needs to include some specific information with respect to the EU signature directive. All requirements for qualified digital certificates are defined in this directive. An SSCD is usually a cryptographic hardware token that needs to fulfill several requirements also defined in the EU Signature Directive. Qualified electronic signatures have also already been discussed in Section 2.2.3.1.

Encryption and Decryption Besides the signature key pair and certificate, a further key pair is stored on the citizen card. This additional key pair can be used for encryption and decryption of data. The public keys of every citizen, which are used for encryption purposes, can be queried from a national and central LDAP (Lightweight Directory Access Protocol) directory. These keys can then be further used for encrypting data for arbitrary citizens. Through encryption, data can be either stored or exchanged securely and confidentially.

The private key – corresponding to the public key published in the LDAP directory – is only stored

on the citizen card of the citizen²¹. This means, the private key is stored in secure hardware and hence cannot be read out. This private key is used for decrypting data. Since the private key is only stored in the citizen card, decryption is only possible within the card.

Data Storage The last functionality of the Austrian citizen card constitutes simple data storage. The citizen card provides a readable and writable data storage. The data storage is divided into logical entities, which are irrespective of the physical storage location. Possible physical storage locations are the citizen card itself, the citizen card software (see next section), the citizen's hard drive, or data storage accessible over the Internet e.g., cloud storage solutions. Data to be stored can be of arbitrary format, such as other digital certificates, XML data, or similar data formats. [Hollosi et al., 2014]

3.6.2.2 Citizen Card Model

Figure 3.12 illustrates the general citizen card model according to Hollosi et al. [2014] and shows all participating parties and components in citizen card-based transactions. The central component of the citizen card model is the so-called citizen card software (CCS), which constitutes a middleware residing between the citizen and the online application (OA). All involved entities are briefly described below based on the work of Hollosi et al. [2014]; Stranacher et al. [2013c].

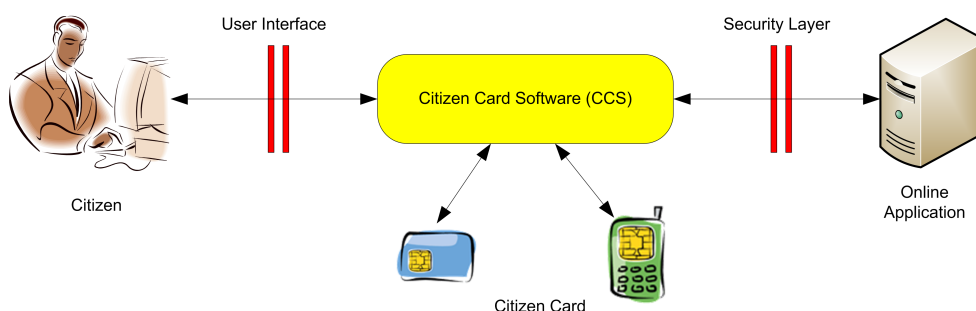


Figure 3.12: The Austrian Citizen Card Model [Stranacher et al., 2013c; Hollosi et al., 2014]

Citizen: A *citizen* is a natural person who wants to access a governmental application by using citizen card functionality. The citizen card functionality is invoked through the citizen card software.

Online Application: An *online application* (OA) is a governmental or business application offering specific services to citizens, which may require citizen card functionality. For instance, restricted access to services is protected through citizen card authentication.

Citizen Card Software: The *citizen card software* (CCS) constitutes a software, which is either locally installed on the citizen's computer or provided remotely on a server. This software provides citizen card functionality to the citizen. Amongst others, citizen card functionality mainly includes identification, authentication, or the creation of electronic signatures (cf. Section 3.6.2). The citizen card software is the core component of this model, implementing the *security layer* and *user interface* and thus facilitating access to citizen card functions and operations. Details on available CCS implementations can be found in [Centner et al., 2010; Orthacker et al., 2010].

User Interface: The *user interface* is the interface between the user and the citizen card software. Required credentials (e.g., smart card PIN, mobile phone number and password, etc.) to authorize access to citizen card functionality are collected from the user through this interface.

²¹Encryption and decryption is currently only supported by smart card-based citizen card implementations.

Security Layer: The *security layer* [Hollosi et al., 2014] is a well-defined interface between the online application and the citizen card software. Via this interface, applications are able to easily access citizen card functionality irrespective of knowing any citizen card specifics. Thus, this interface can be used without paying attention to the underlying citizen card implementation. Implementation specifics are encapsulated by the citizen card software.

3.6.3 The Austrian eID Architecture

The Austrian identity ecosystem allows unique identification and secure authentication for both natural and legal persons. To ease an integration of the rather complex Austrian eID ecosystem into security sensitive applications, a set of software modules has been developed, which cover most functionality and hide complex details. Figure 3.13 illustrates main components and entities of the the Austrian eID architecture separated into operational domains. Their interactions and individual process flows supporting different use cases will be described in the subsequent sections. The operational domains are described next according to Stranacher et al. [2013c].

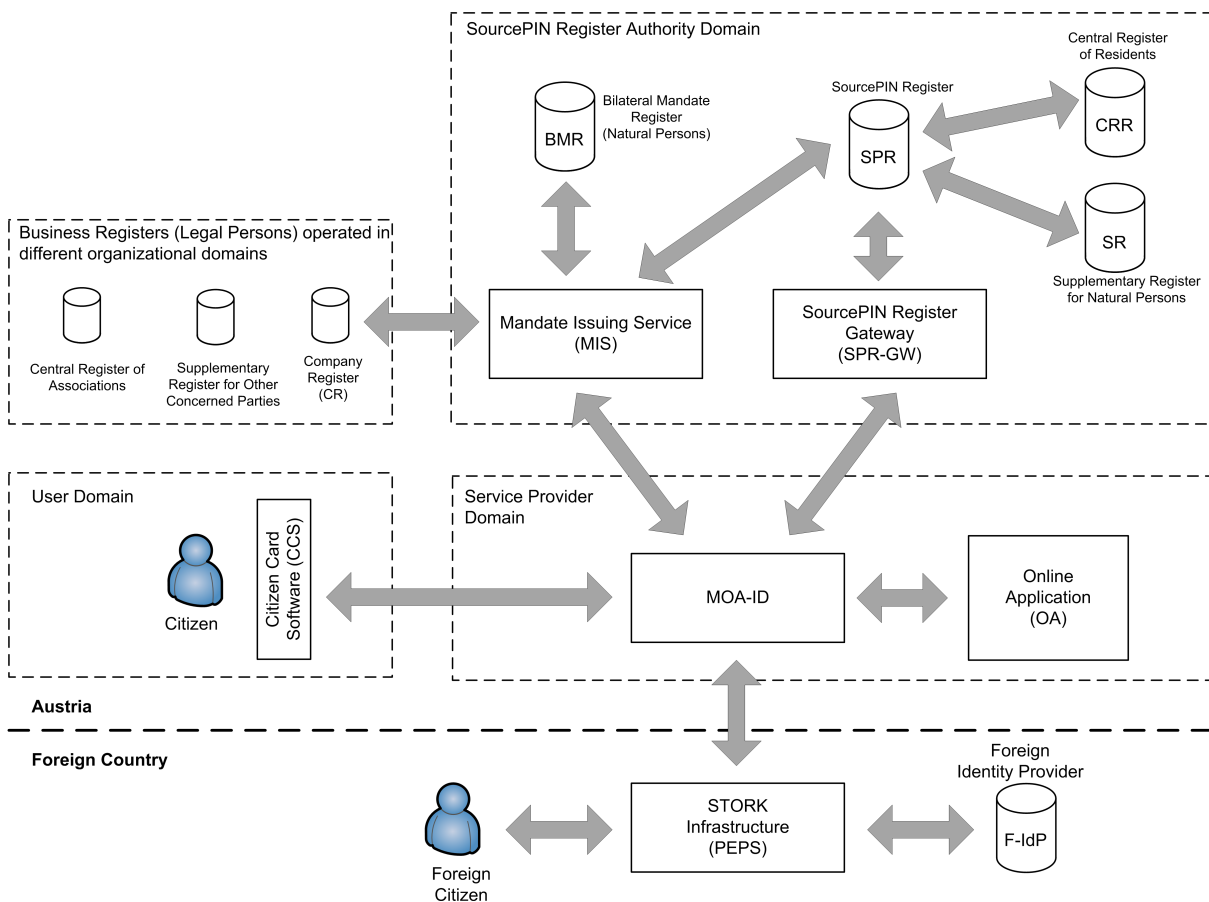


Figure 3.13: The Austrian eID Architecture

User Domain: A *citizen* wants to access a public or private sector service using her Austrian citizen card. The citizen card software, which enables easy access to citizen card functionality, usually runs in the citizen's domain.

Service Provider Domain: A service provider hosts one or more public or private sector *online applications* providing web-based services to citizens. These services require qualified and secure identification and authentication of the Austrian citizen card (or equivalent foreign eIDs), which is

handled and managed by *MOA-ID*. On the one hand, *MOA-ID* accesses citizen card functionality for identification and authentication, and, on the other hand, provides specific and authentic citizen data to the online application for further processing.

SourcePIN Register Authority Domain: The *Mandate Issuing Service* (MIS) is only invoked if citizen wants to authenticate as a representative for a natural or legal person. The MIS issues electronic mandates on the fly. For querying appropriate mandate information for natural person representation, the MIS has to query the *Bilateral Mandate Register* (BMR). For fetching appropriate mandate information for representing legal persons, an according *Business Register* - depending on the type of the legal person - needs to be queried. To finish an authentication process using representation between natural persons, the *SourcePIN Register* (SPR) needs to be queried. The SourcePIN Register is more or less a virtual register, which bundles the information of the *Central Register of Residents* (CRR) and the *Supplementary Register for Natural Persons* (SR). The *SourcePIN Register Gateway* (SPR-GW), which is also operated within the SourcePIN Register Authority Domain, is only invoked in the case of foreign citizen authentication. Thereby, the SPR-GW facilitates the registration of foreign citizens in the SR for *MOA-ID*.

Business Registers: In Figure 3.13 the individual business registers (*Company Register*, *Central Register of Associations*, *Supplementary Register for Other Concerned Parties*) are subsumed under one block for simplicity. However, the individual registers are actually operated in different organizational domains. Operators are for instance the *Austrian Ministry of Justice* or the *Austrian Ministry of the Interior*. These business registers contain information of legal persons and hence also mandate information for their representation in electronic processes.

Foreign Country: Foreign citizens usually authenticate via the *STORK infrastructure* (cf. Section 5.5). The STORK infrastructure (aka PEPS – Pan-European Proxy Service) operated in the foreign country queries an appropriate *Foreign Identity Provider* (F-IdP) for citizen identification and authentication. Authenticated citizen data is transferred via the STORK infrastructure (PEPS) into the Austrian eID system (in detail to *MOA-ID*).

The individual components work all together to support different use cases. In the following subsections, three identification and authentication use cases by detailing the interaction and communication between these components are described.

3.6.4 Identification and Authentication of Austrian Citizens

For identification and authentication of Austrian citizens at online applications mainly the component *MOA-ID* is responsible. *MOA-ID* handles the identification process by reading and verifying the citizen's Identity Link and by deriving the sector-specific PIN from the citizen's sourcePIN. Authentication is carried out by qualified signature creation, stating the willingness of authenticating at the online application. The citizen's signature is verified by *MOA-ID*.

Figure 3.14 illustrates the middleware architecture applied in Austria and the involved components required for Austrian citizen identification and authentication only. The aim of this architecture is to decouple the actual identification and authentication process from the online application. The middleware actually consists of two parts, a client middleware (citizen card software) and a server-side middleware (*MOA-ID*). The client middleware handles the smart card communication for smart card-based citizen card implementations or the communication with the Mobile Phone Signature server²² for the implementation using citizens' mobile phones. In contrast, the server-side middleware manages the actual authentication process and the communication with applications of a service provider. The server-side

²²<http://www.handy-signatur.at>

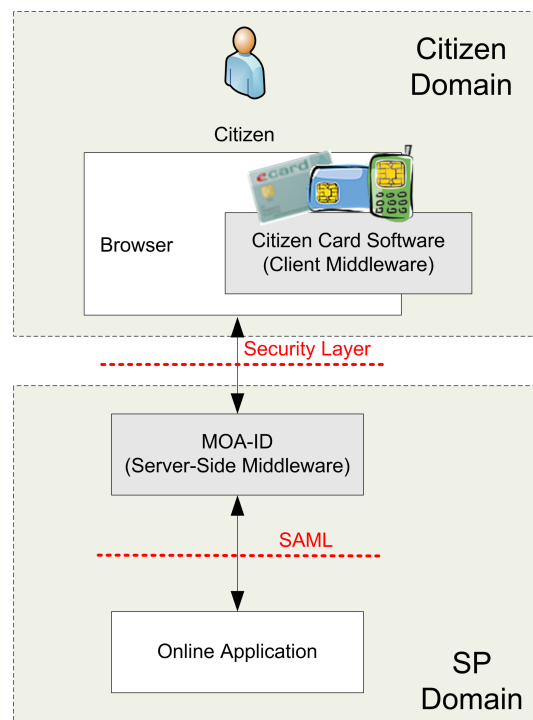


Figure 3.14: Austrian eID architecture for Austrian citizen identification and authentication only [Sumelong et al., 2011]

middleware MOA-ID has been developed to decouple a service provider from specifics of a citizen card implementation.

The client middleware allows the server-side middleware to access an Austrian eID card via a web browser. The client middleware can either be a piece of software running on the user's PC, a Java Applet running in the user's browser, or a server-side implementation such as the Austrian Mobile Phone Signature. In case of adopting the alternative using the Java Applet, this client middleware (called MOCCA²³) is also divided into two parts. The Java Applet running on the citizen's client is responsible for the card-based communication with the Austrian eID cards. The client middleware running on a remote server executes computationally intensive operations (such as XML processing) needed for the communication between the server-side middleware MOA-ID and the eID cards.

In general, to enable citizens secure access to online services using the Austrian national eID, the service provider, e.g., a municipality, must at least run a server-side middleware MOA-ID and a server-based client middleware MOCCA if desired. In contrast, server-based client middleware installations in the SP domain are only necessary if the Java Applet variant of the Austrian client middleware is deployed. Other card-based middleware implementations are usually installed locally in the user's domain. In addition, the Mobile Phone Signature server acting as server-based client middleware is operated by a trusted third party (A-Trust²⁴).

According to Figure 3.14, within the authentication architecture the following two important interfaces can be identified.

MOA-ID - Client Middleware: Between the citizen's client middleware and MOA-ID a national protocol is used. This national interface (security layer [Hollosi et al., 2014]) defines functions on an abstract level for the citizen card (e.g., creating digital signatures) which can be accessed by MOA-ID. The protocol used for communication between these two modules is based on XML.

²³<https://joinup.ec.europa.eu/software/mocca/home>

²⁴<http://www.a-trust.at/>

The XML-commands for the security layer can be bound to an arbitrary transport protocol such as TCP/IP or HTTP. In case of MOA-ID, HTTP over SSL/TLS is used.

MOA-ID - Online Application: MOA-ID provides a common and well-defined interface based on SAML (cf. Section 3.5.2) or OpenID Connect (cf. Section 3.5.5) for the exchange of authentication and identity information between MOA-ID and SAML-aware online applications of a service provider. For simplicity, in the remainder of this thesis identification and authentication processes are described based on the use of SAML only.

The complete identification and authentication process for Austrian citizens is illustrated in Figure 3.15. The individual process steps are described in detail in the following [Stranacher et al., 2013c]:

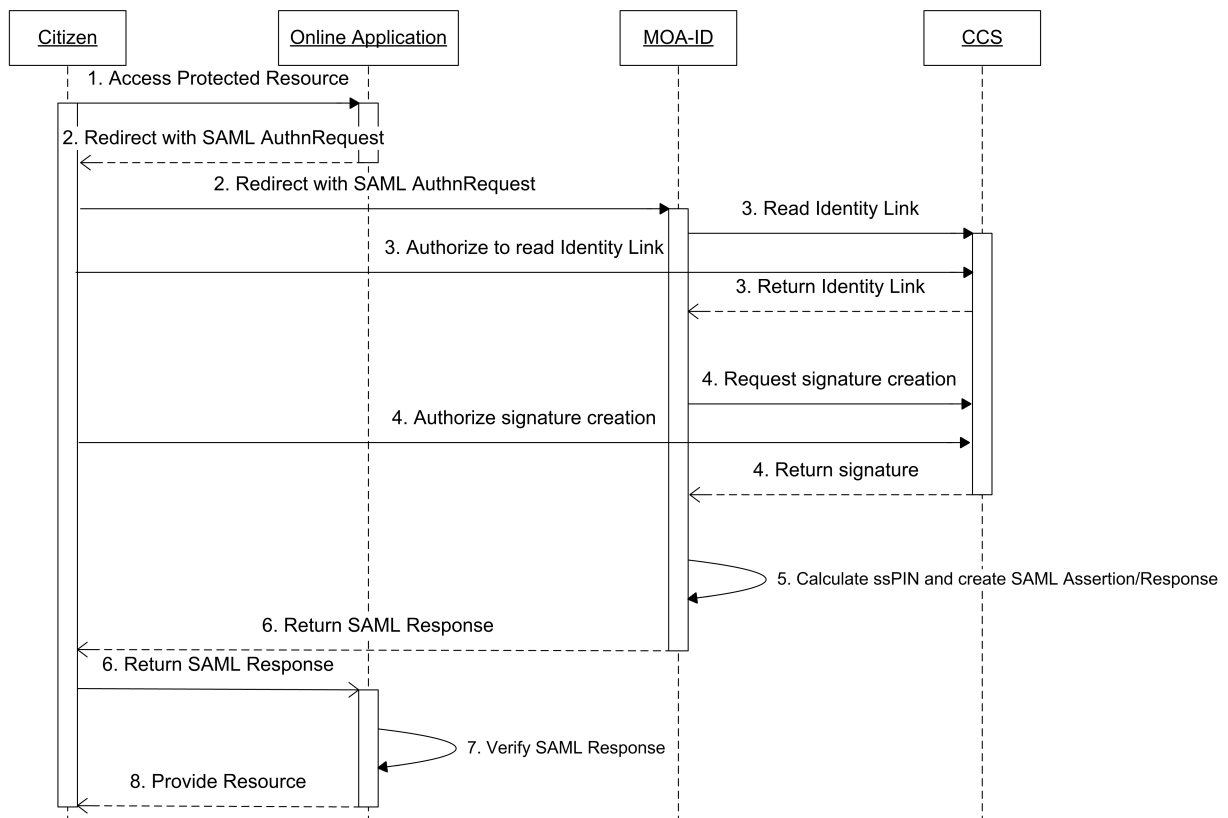


Figure 3.15: Process flow of Austrian citizen identification and authentication

1. The citizen wants to access a protected resource at the online application, which requires proper authentication.
2. The online application assembles a SAML authentication request (cf. Section 3.5.2), which is transmitted via HTTP-Redirect to MOA-ID.
3. In this step, MOA-ID sends an appropriate XML request to the CCS for retrieving the Identity Link from the citizen card. The citizen authorizes this request appropriately depending on the CCS implementation. The Identity Link is returned to MOA-ID and verified.
4. MOA-ID requests the creation of a qualified electronic signature indicating the willingness of the citizen for online application authentication. The citizen creates a signature, which is sent back to MOA-ID and verified. The citizen authorizes this request appropriately depending on the CCS implementation.

5. MOA-ID derives the appropriate ssPIN for the sector the online application belongs to and assembles a SAML assertion/response, which includes the ssPIN and additional citizen data out of the Identity Link.
6. MOA-ID returns the SAML response to the online application via HTTP-POST.
7. The online application verifies the SAML response and extracts the citizen attributes.
8. After successful verification, the online application grants access to the resource.

3.6.5 Legal Persons and Electronic Mandates

Besides MOA-ID, in this scenario also the Mandate Issuing Service (MIS) [Tauber et al., 2011a] plays an important role. Figure 3.16 illustrates the identification and authentication scenario when representing a legal person. For simplicity, the author limits this use case to legal person representation only, as the representation of natural persons is similar. The following steps need to be carried out in this process [Tauber et al., 2011a; Stranacher et al., 2013c]:

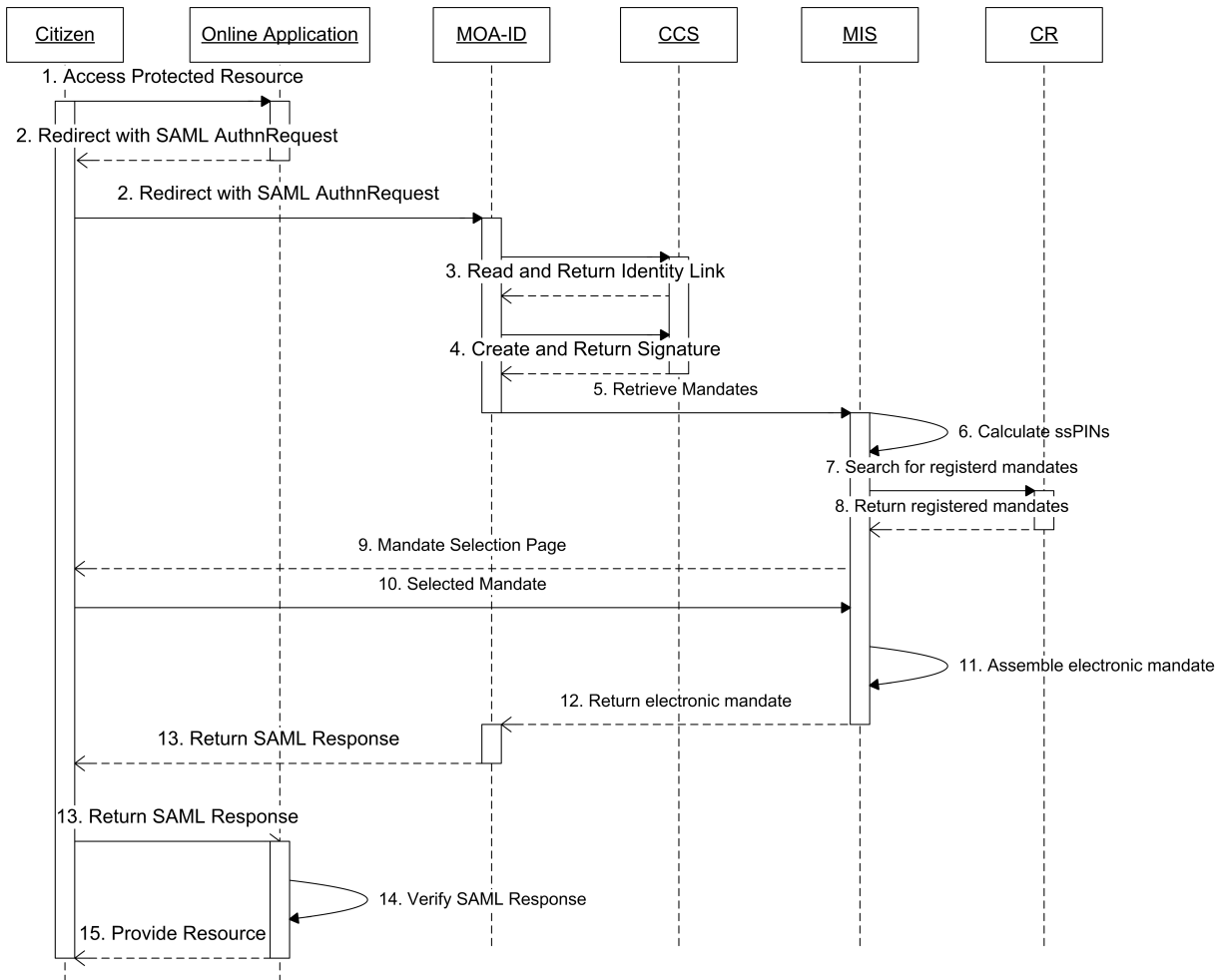


Figure 3.16: Process flow representing a legal person electronically

1. This process step is equal to normal Austrian citizen authentication (cf. Section 3.6.4). The citizen wants to access a protected resource at the online application, which requires proper authentication. However, the citizen indicates that she wants to authenticate on behalf of somebody (e.g., by activating a checkbox).

2. This process step is equal to normal Austrian citizen authentication (cf. Section 3.6.4). The online application assembles a SAML authentication request, which is transmitted via HTTP-Redirect to MOA-ID.
3. This process step is equal to normal Austrian citizen authentication (cf. Section 3.6.4). In this step, MOA-ID sends an appropriate XML request to the CCS for retrieving the Identity Link from the citizen card. The citizen authorizes this request appropriately depending on the CCS implementation. The Identity Link is returned to MOA-ID and verified. The authorization process step for authorizing the Identity Link read request is not explicitly shown.
4. This process step is equal to normal Austrian citizen authentication (cf. Section 3.6.4). MOA-ID requests the creation of a qualified electronic signature indicating the willingness of the citizen for online application authentication. The citizen creates a signature, which is sent back to MOA-ID and verified. The citizen authorizes this request appropriately depending on the CCS implementation. The authorization process step for authorizing signature creation is not explicitly shown.
5. Since the citizen wants to authenticate on behalf of somebody, the MIS is queried by MOA-ID for accessing all mandates the citizen is empowered. For that, MOA-ID sends the citizen's Identity Link to the MIS.
6. Out of the sourcePIN from the Identity Link, the MIS calculates all appropriate ssPINs for querying the individual registers. For simplicity, in this scenario the author illustrates the query process at the company register (CR) only.
7. The MIS searches the CR for registered mandates using the corresponding $ssPIN_{CR}$ of the citizen.
8. The CR returns all registered mandate information for this citizen.
9. The MIS presents the citizen a selection page of all available mandates for her (mandates from the CR, BMR, etc.).
10. The citizen selects the mandate she wants to use for authentication at this online application. In this illustrated scenario the author assumes that the citizen wants to act on behalf of a company.
11. The MIS assembles all necessary mandate information and signs these data to generate an electronic mandate according to the specification defined by Rössler et al. [2006]. Amongst others, this electronic mandate contains information of the citizen, who represents the company, the company, and the type of empowerment the citizen is allowed to act on behalf.
12. The MIS returns the electronic mandate to MOA-ID.
13. MOA-ID assembles an appropriate SAML assertion/response including the electronic mandate and transmits it to the online application.
14. The online application verifies the response.
15. If verification is successful the online application grants access. The citizen is now able to do online procedures on behalf of the selected company.

Details on the Austrian electronic mandate concept can be also found in Tauber et al. [2013].

3.6.6 Identification and Authentication of Foreign Citizens

In this scenario, the author illustrates how foreign citizens are able to use Austrian e-Government services. In this scenario, the STORK infrastructure – and especially the PEPS model – is involved. For details on the STORK framework and the PEPS model the author refers to Section 5.5.

The process flow for authenticating foreign citizens at Austrian online applications is illustrated in Figure 3.17. The required steps are the following [Stranacher et al., 2013c; Tauber et al., 2012]:

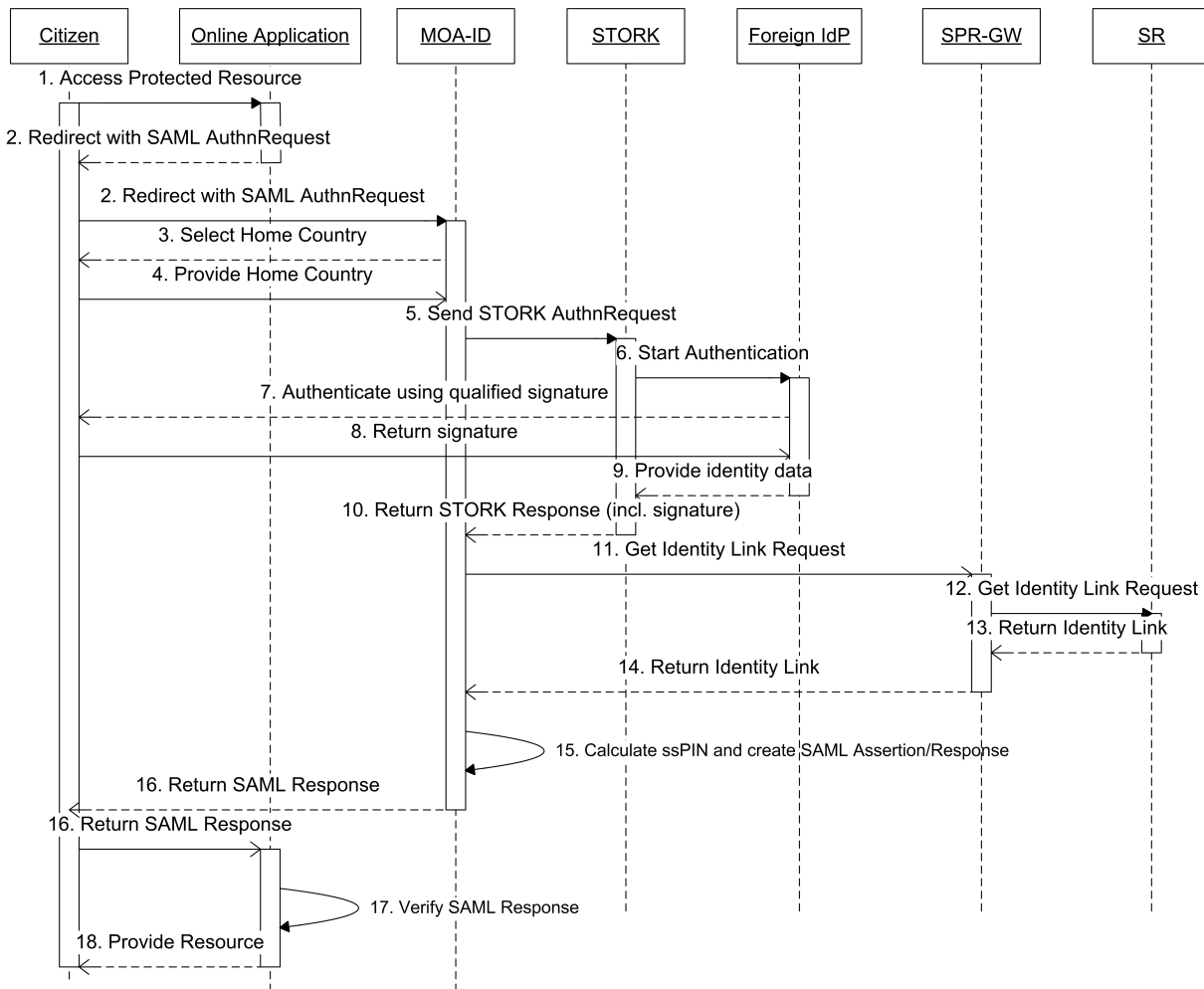


Figure 3.17: Process flow of foreign citizen identification and authentication

1. A foreign EU citizen wants to access a service of an Austrian online application.
2. The online application assembles an appropriate SAML authentication request and sends it to MOA-ID.
3. MOA-ID presents the foreign citizen a page where the citizen can select her country of origin.
4. The citizen provides her home country she originates from.
5. According to the STORK idea, the foreign citizen will be authenticated in her home country. Therefore, the citizen is redirected to a single gateway (PEPS – see Section 5.5.3.1 for details) in the foreign country, being part of the STORK infrastructure. For starting this authentication process, MOA-ID transmits a STORK authentication request to the foreign PEPS. The PEPS selects an appropriate foreign IdP (F-IdP), where the citizen actually authenticates.

6. The PEPS forwards the authentication request to the F-IdP.
7. The F-IdP requests the citizen to authenticate using a qualified signature.
8. The qualified signature is returned to the F-IdP.
9. The F-IdP provides the qualified signature as well as other citizen identifying information (first name, last name, date of birth, identifier) to the PEPS.
10. The PEPS assembles these citizen data and returns a STORK response to MOA-ID.
11. MOA-ID extracts this information and sends it to the SPR-GW. The SPR-GW verifies the citizen's signature.
12. The SPR-GW queries the SR to register the foreign citizen in the Supplementary Register for Natural Persons (SR) based on the information received. This registration into the SR is legally based on the Austrian e-Government act [Federal Chancellery, 2008] and the Austrian e-Government equivalence decree [Federal Chancellery, 2010d].
13. The SR calculates a sourcePIN for the citizen, creates and assembles an Identity Link, and returns the signed Identity Link to the SPR-GW.
14. The SPR-GW returns the Identity Link to MOA-ID.
15. This process step is equal to normal Austrian citizen authentication (cf. Section 3.6.4). MOA-ID derives the appropriate ssPIN for the sector the online application belongs to and assembles a SAML assertion/response, which includes the ssPIN and additional citizen data out of the Identity Link.
16. This process step is equal to normal Austrian citizen authentication (cf. Section 3.6.4). MOA-ID returns the SAML response to the online application via HTTP-POST.
17. This process step is equal to normal Austrian citizen authentication (cf. Section 3.6.4). The online application verifies the SAML response and extracts the citizen attributes.
18. This process step is equal to normal Austrian citizen authentication (cf. Section 3.6.4). After successful verification, the online application grants access to the resource.

Details on the used STORK infrastructure and the involved components enabling this use case will be also discussed in the next chapter 5.

3.6.7 A Single Sign-On Architecture

MOA-ID is an identity providing server-side middleware that can be used by service providers to protect their resources with citizen card access. However, MOA-ID is not SSO-capable and citizens accessing applications of different administrative sectors (e.g., finance, justice, etc.) must re-authenticate every single time they are changing applications or switching contexts. Therefore, according to Zwattendorfer et al. [2011a] in this subsection a security architecture that fills this gap by enabling SSO between different administrative sectors using MOA-ID as identity provider is presented. This is achieved by enhancing MOA-ID and by transforming sectoral identifiers using and including an additional attribute provider (SourcePIN Register Authority), which is hosted by the trusted Austrian Data Protection Commission, in the authentication process.

3.6.7.1 SSO Architecture

Currently, if users want to access two or more applications which belong to different sectors, they have to authenticate separately at each application. For instance, consider the scenario illustrated in Figure 3.18. If an online application (A) belongs to sector A, users have to authenticate at the corresponding MOA-ID (A) which protects application (A). MOA-ID (A) calculates $ssPIN_{(A)}$ (on the basis of the user's sourcePIN) for sector A and makes it available for identification at application (A). Since MOA-ID (A) is processing $ssPIN_{(A)}$, it is only allowed to run in sector A. If the same user wants to access another application (B), which belongs to sector (B), she needs to authenticate again by running through the citizen card authentication process at MOA-ID (B). Thus, MOA-ID (B) protecting application (B) calculates $ssPIN_{(B)}$ for identification at online application (B).

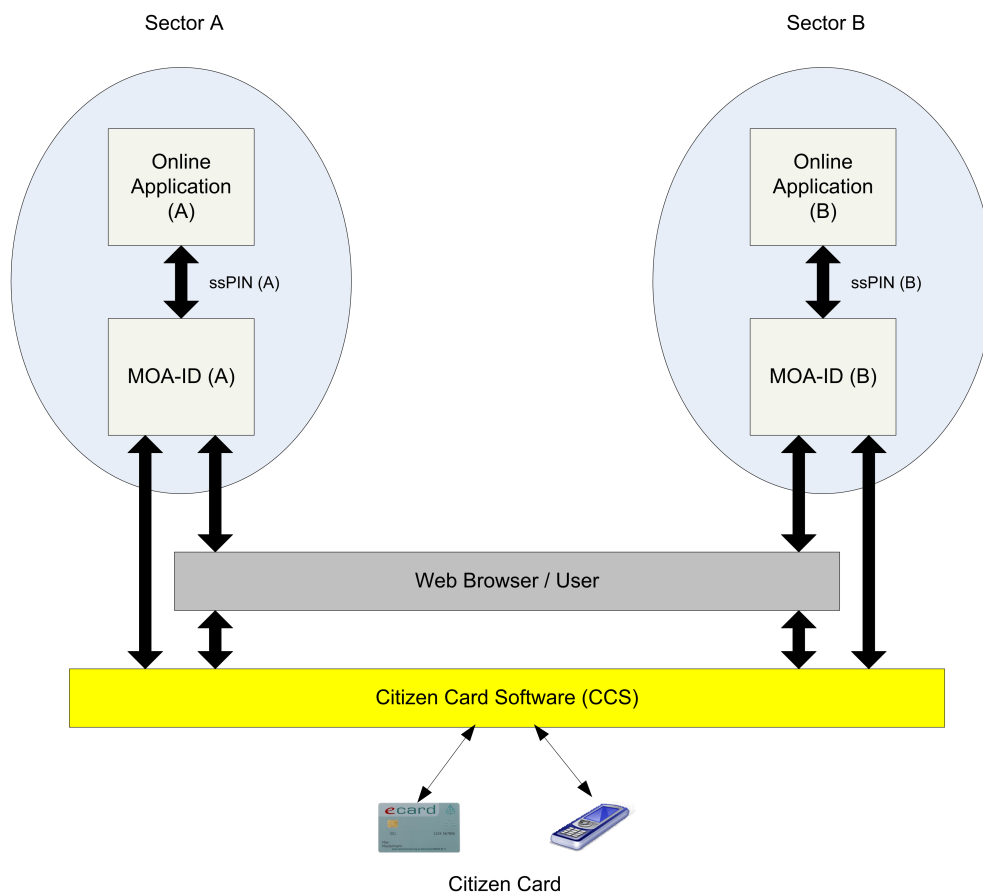


Figure 3.18: Current Cross-Sector Authentication [Zwattendorfer et al., 2011a]

Frequent authentication processes actually do not encourage usability. Therefore, MOA-ID has been enhanced in such a way that single sign-on can be supported by still keeping the same level of security by using the Austrian citizen card. This gives users the ability – if already successfully authenticated for one sector – to authenticate at applications belonging to other sectors without re-authenticating. The respective SSO process is the following: For describing the SSO process, it is assumed that a user has already been successfully authenticated at application (A) via MOA-ID (A). Furthermore, application (A) links to applications of other sectors e.g., the application (B) of sector (B). With the help of the MOA-ID SSO enhancements, users are able to seamlessly authenticate at application (B) without re-authentication. MOA-ID (B) protecting application (B) can grant access because an appropriate trust relationship between MOA-ID (A) and MOA-ID (B) exists. All required authentication and identification data are transferred from MOA-ID (A) to MOA-ID (B) in a user-centric way. Figure 3.19 illustrates this single sign-on scenario.

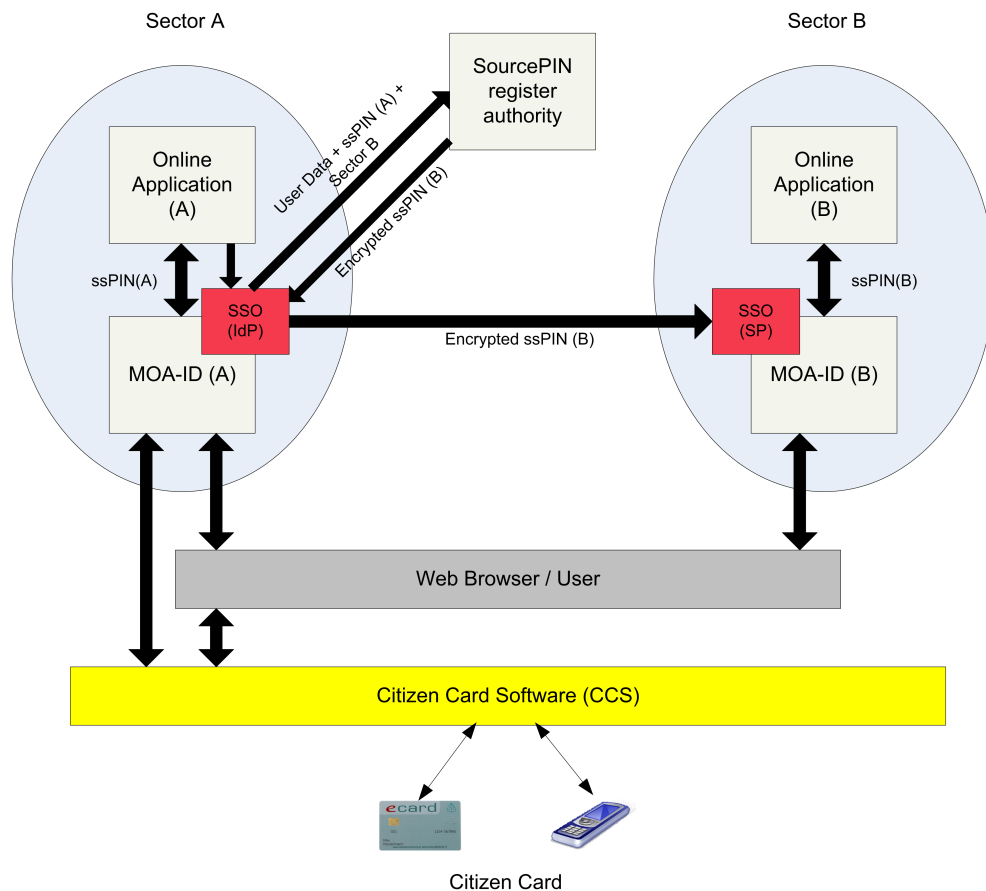


Figure 3.19: Single Sign-On Cross-Sector Authentication [Zwattendorfer et al., 2011a]

Redirection from application (A) and subsequent identification at application (B) requires $ssPIN_{(B)}$ for sector B. However, during authentication at application (A) only $ssPIN_{(A)}$ for sector (A) has been calculated. Hence, for seamless authentication at online application (B) a prior calculation of $ssPIN_{(B)}$ must take place. This calculation is conducted by using the concept of *encrypted ssPINs* [Hollosi and Hörbe, 2007]. Encrypted ssPINs are legally defined by the Austrian e-Government act [Federal Chancellery, 2008] (technically by Hollosi and Hörbe [2007]) and allow applications the processing of ssPINs of foreign sectors without disclosing the actual ssPIN value. An encrypted ssPIN of sector B is calculated by encrypting the concatenation of a timestamp TS , the sector code s , and an existing $ssPIN_{(B)}$. The private/public encryption key pair of an organization belonging to sector B is denoted as $(sk_{(B)}, pk_{(B)})$. The encrypted ssPIN for sector B $ssPIN_{enc(B)}$ is calculated as follows:

$$ssPIN_{enc(B)} = Enc(pk_{(B)}, TS || s || ssPIN_{(B)})$$

Enc denotes the RSA encryption function and $pk_{(B)}$ denotes the official RSA public key of sector (B). Key lengths of public keys must be at least 1024-bits (2048-bit are recommended). The timestamp TS ensures that each calculated value of $ssPIN_{enc(B)}$ is different and thus prevents the tracking of citizens' activities in a different sector. To calculate $ssPIN_{enc(B)}$ within sector A, the SourcePIN Register Authority (SRA) as trusted entity is contacted. The SRA holds a registry of the public keys of all sectors and provides a web service to transform own ssPINs to encrypted ssPINs of other sectors. This transformation requires as input the user's identity data (first name, last name, and date of birth), the $ssPIN_{(A)}$ of sector A, as well as the desired sector code s of sector B. This way, the SRA can search for the user in the central residents register and calculate the user's sourcePIN and $ssPIN_{enc(B)}$ respectively.

3.6.7.2 SSO Process Flow

The sequence diagram in Figure 3.20 illustrates the SSO process flow in more detail. The process has four main steps, which are further discussed in more detail. Furthermore, it is assumed that the user has already been successfully authenticated once using her citizen card at MOA-ID (A). To enable SSO authentications, MOA-ID was enhanced in such a way that a user's authentication session isn't immediately discarded upon assertion devaluation by the online application. The four main steps are as follows [Zwattendorfer et al., 2011a]:

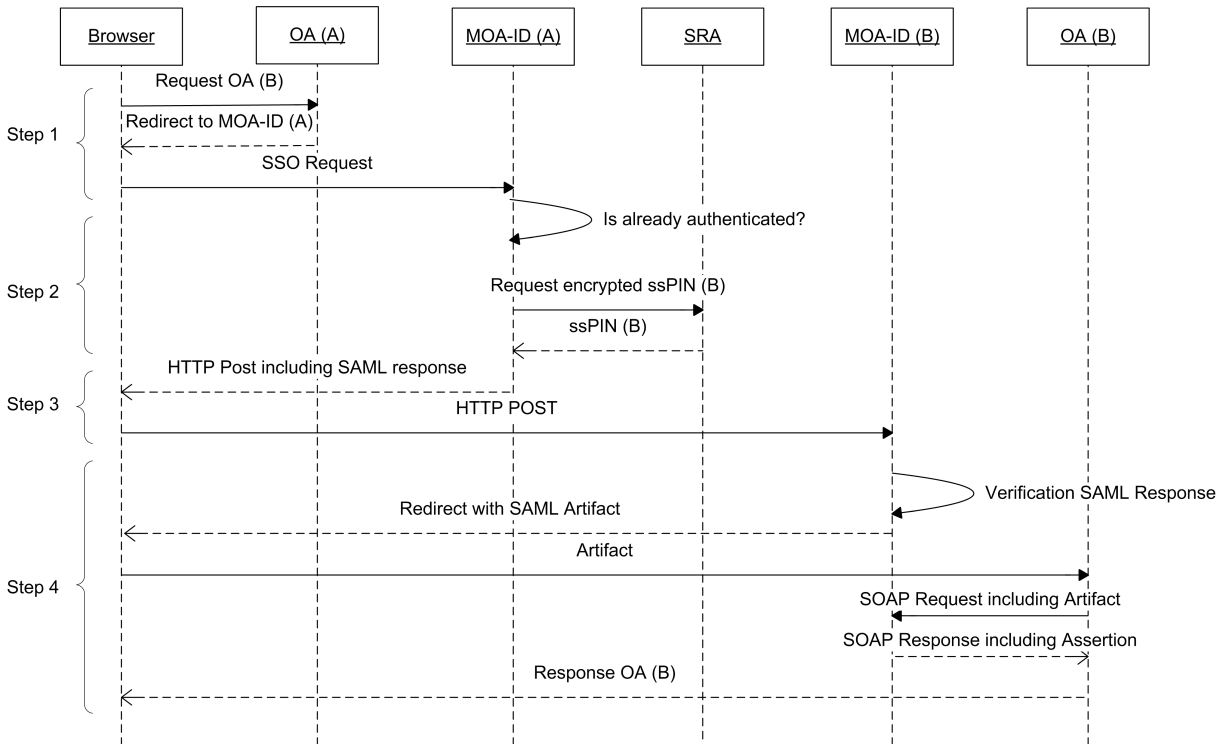


Figure 3.20: Sequence diagram of the SSO process flow [Zwattendorfer et al., 2011a]

Step 1: In this step, the user wants to access a particular service of sector B although currently interacting with an application of sector A. Instead of being directly forwarded to application (B), the user is redirected to MOA-ID (A) in order to check if she has been already successfully authenticated before, i.e. if the authentication session is still valid. MOA-ID (A) further checks if MOA-ID (B) and consequently also application (B) is trusted.

Step 2: If the requirements of Step 1 are fulfilled, MOA-ID (A) submits the user's identification data (name, date of birth), $ssPIN_{(A)}$ and s to the SRA for the calculation of $ssPIN_{enc(B)}$. The communication with the SRA is secured with TLS client authentication.

Step 3: In this step, the actual SSO process takes place. Since the user has been successfully authenticated before, the information of this previous authentication including $ssPIN_{enc(B)}$ is packed into a SAML assertion and digitally signed. This assertion is based on SAML 2.0 and assembled according to the Web SSO profile [Hughes et al., 2009]. The signed assertion is then conveyed by the user through HTTP-POST to MOA-ID (B). By this assertion, MOA-ID (A) asserts MOA-ID (B) the trustworthiness of the previous authentication at application (A).

Step 4: After having verified the assertion, MOA-ID (B) decrypts $ssPIN_{enc(B)}$ with its private key $sk_{(B)}$ and prepares the identification data to be sent to the protected application (B). The communication between MOA-ID (B) and application (B) is based on the SAML Browser/Artifact

Binding 1.0 [Mishra et al., 2002], which is used for legacy applications. Although the SAML assertion transmitted between MOA-ID (A) and MOA-ID (B) is based on SAML version 2.0, the identification data sent from MOA-ID (B) to application (B) is still included in SAML 1.0 assertions. The reason for that is the support of legacy services because currently most Austrian (governmental) online applications are capable of processing SAML 1.0 assertions only. After this process step, the user is successfully and seamlessly authenticated at application (B) without re-authentication at MOA-ID (B). Online applications experience no difference whether users have been authenticated via normal citizen card authentication or via SSO. Hence, legacy applications do not need to modify their authentication environment for supporting SSO.

3.7 Chapter Conclusions

This chapter gave a basic introduction on electronic identity and its importance and usage within the Austrian e-Government strategy and concepts. By having read this chapter, basically the reader should be aware of the existing eID infrastructure and according processes with respect to G2C communications in Austria. Parts of the Austrian eID architecture are subject to enhancements and amendments to support additional use cases such as cross-border identification and authentication (cf. Chapter 5) in the next chapters.

Chapter 4

Cross-Border E-Government

Based on the four freedoms of the EU (free movement of goods, capital, services, and people) the European Commission steadily aims on strengthening the European digital internal market. This further includes that the execution of the four freedoms should be supported by information and communication technologies. At the very first beginning, e-Government usually was tailored to national and domestic requirements only. However, to support the EU's four freedoms electronically, data also needs to be exchanged and accepted across EU member states. This need caused the EU to put efforts into ICT-enabled public administration services to further enable cross-border e-Government. These efforts for achieving pan-European e-Government services are supported by underlying strategic commitments, initiatives, and programmes. In this chapter, the most important EU activities (in particular interoperability solutions) for achieving cross-border e-Government are elaborated.

The chapter is structured as follows. First, Section 4.1 overviews the EU's strategic commitments, initiatives, and programmes aiming on cross-border e-Government. Thereby, the most important EU activities over the past years and at the present time are described. As a result out of these activities, interoperability can be identified as one of the biggest challenges to implement successful e-Government across borders. Thus, Section 4.2 defines interoperability and discusses the European Interoperability Strategy (EIS) and the European Interoperability Framework (EIF), which both aim on facilitating the implementation of interoperable pan-European public services. Finally, Section 4.3 details the EU's interoperability efforts by describing different large scale pilot (LSP) projects, which are co-funded by the EU and aim on getting hands-on experience in real-life applications and scenarios in different areas.

4.1 EU Activities

The European Union has undergone several activities to foster the adoption of e-Government across Europa. Such activities are a strong driver for pushing e-Government not only on national level but also in a cross-border context. In this section, the author briefly elaborates on the most important strategic actions and initiatives undertaken by the EU to foster and facilitate cross-border e-Government over the past years.

4.1.1 Strategic Commitments

For describing the undertaken strategic commitments of the European Union, the author starts with the description of the *Lisbon Strategy* [European Council, 2000a] agreed in 2000. Subsequently, the author describes the so-called *Manchester Ministerial Declaration* of 2005 and concludes with the *Malmö Ministerial Declaration* on e-Government of 2009.

4.1.1.1 Lisbon Strategy

The *Lisbon Strategy* was the result from a meeting of the European Council held in Lisbon in 2000. Thereby, the European Council agreed on new strategic goals for the European Union *"in order to strengthen employment, economic reform and social cohesion as part of a knowledge-based economy"* [European Council, 2000a].

In this meeting, the European Council highlighted the strengths and weaknesses of the EU. Whereas the Council saw an existing strong position of the EU in monetary and fiscal policies and in the economy of a stable internal market, still some weaknesses were identified by the Council. At this time, the EU also suffered from a high unemployment rate, particularly in the service sector and the telecommunications and Internet area [European Council, 2000a]. Furthermore, the Council saw issues in filling existing information technology jobs due to missing knowledge and skills.

These weaknesses lead the Council to formulate new strategic goals for the EU. According to the European Council [2000a], the EU should *"become the most competitive and dynamic knowledge-based economy in the world capable of sustainable economic growth with more and better jobs and greater social cohesion"*. In particular, the Council aimed on strengthening the R&D society and to transfer the EU into a knowledge-based economy and society by particularly strengthening competitiveness and innovation in ICT. Details on the achieved results of this strategy can be found in Rodriguez et al. [2010].

4.1.1.2 Manchester Ministerial Declaration

The *Ministerial Declaration of Manchester* [European Commission, 2005] resulted from a meeting of – amongst others – mostly ministers of EU member states responsible for e-Government held during the e-Government conference *"Transforming Public Services"* in Manchester in 2005. Thereby, the ministers agreed on several strategic actions to be included as action points into the i2010 action plan (cf. Section 4.1.2.2). In the following, the main strategic actions and commitments of this declaration are listed [European Commission, 2005]:

- Public administrations should care that electronic services are also easily accessible for socially disadvantaged or disabled people.
- Public administrations should significantly increase the use of ICT for e-Government to make governmental processes more effective and efficient.
- Offered services should be designed according to customer's (citizens or businesses) needs, in particular in the field of e-Procurement.
- Electronic identification means should be mutually recognized and accepted across the EU and should serve citizens and businesses as trusted means for accessing e-Government services.

For this thesis, in particular the last action point on electronic identification is important. Whereas the Lisbon strategy aimed on fostering the use of ICT in the EU in general, the Manchester Ministerial Declaration explicitly states the demand for mutually accepted eIDs across the EU to increase efficiency in governmental processes. In detail, the action point states that *"by 2010 European citizens and businesses shall be able to benefit from secure means of electronic identification that maximise user convenience while respecting data protection regulations. Such means shall be made available under the responsibility of the Member States but recognised across the EU"* [European Commission, 2005].

This agreement – particularly the passage on member states' responsibility – led to the kick-start and realization of the EU large scale pilot (LSP) project STORK, which will be discussed in detail in Section 5.5.

4.1.1.3 Malmö Ministerial Declaration

Again, the *Ministerial Declaration of Malmö* [European Commission, 2009] resulted from a meeting held at the Ministerial e-Government conference "Teaming up for the eUnion" in Malmö 2009. In this meeting, EU member states ministers agreed on a common vision and strategic policies for 2015. The main agreed policies were [European Commission, 2009]:

- Citizens and businesses should benefit from increased access to public services and greater transparency.
- Mobility of citizens and businesses within the EU should be strengthened. Living, working, or studying across the EU should be facilitated by appropriate e-Government services.
- Efficiency and effectiveness of public services and organizational processes should be increased.
- Appropriate technical and legal preconditions to support these agreed policies should be developed.

The agreed policies were actually further broken down into concrete objectives, which should be fulfilled by EU and member states' public administrations. One important objective was to "*develop cross-border eGovernment services that are based on real social and economic needs*" [European Commission, 2009]. By this objective, it can be seen that the EU and its member states were trying to put a lot of efforts in implementing cross-border services. Particular results of these efforts were the EU LSPs (Large Scale Pilots) which all aim on achieving interoperability for cross-border e-Government services. These LSPs will be discussed in Section 4.3 in more detail.

Relating to eID, the meeting members asked the European Commission to "*identify gaps in cross-border interoperability and mutual recognition [...] such as trustworthy electronic identity, electronic signatures and electronic documents*". Hence, interoperability of eIDs – even though STORK had already been started – can be seen as an important issue at this time. As a result, the European Commission is further pushing the demand of eID interoperability across borders e.g., by discussing a new legal framework for trust services (eIDAS regulation) [European Commission, 2012b] which will supersede the EU signature directive [European Parliament and Council, 1999b].

4.1.1.4 Europe 2020

Europe 2020 [European Commission, 2010c] constitutes the successor programme of the *Lisbon Strategy*, which had been followed by the EU and its member states between 2000 and 2010. Europe 2020 is a 10-years economic strategy that was adopted by the European Council in 2010. Aim is a "*smart, sustainable and inclusive growth*" [European Commission, 2010c] and better coordination of national and European economy. According to the European Commission [2010c], *smart* means that economy should develop based on knowledge and innovation. *Sustainable* refers to the development of a greener and resource efficient economy. Finally, by *inclusive* the development of a high-employment economy delivering social cohesion is meant.

Priorities of this strategy lie on research and development, employment, environment, education, and poverty reduction. To consolidate these priorities, the European Commission determined quantitative aims. The member states are further encouraged to integrate these aims into their national strategies and derive appropriate target values based on the aims given from the European Commission. Referring to the European Commission [2010c], these aims are:

- "*75% of the population aged 20-64 should be employed.*"
- "*3% of the EU's GDP should be invested in R&D.*"

- The "20/20/20" climate/energy targets should be met (including an increase to 30% of emissions reduction if the conditions are right).
- The share of early school leavers should be under 10% and at least 40% of the younger generation should have a tertiary degree.
- 20 million less people should be at risk of poverty."

To achieve these goals, the European Commission initiated seven flagship initiatives that deal with the identified priorities. One flagship initiative dealing with e-Government is the *Digital Agenda* [European Commission, 2010a], which will be discussed in more detail in Section 4.1.2.3.

4.1.2 Initiatives

Based on the defined strategic commitments and its containing policy definitions the European Commission launched several initiatives to foster the use of electronic public services within the EU. The following subsections briefly overview initiatives launched within the time period 2000-2020.

4.1.2.1 eEurope

By the initiative *eEurope* [European Commission, 2000], in December 1999 the European Commission launched a broad discussion on the future of the EU in the information age. Based on the *Lisbon Strategy* of March 2000, member state representatives (ministers) and government leaders engaged the European Commission to work out an action plan [Council of the European Union and Commission of the European Communities, 2000] for all governmental levels (European, national, and regional level). According to the results and agreements from the *Lisbon Strategy*, the aim of this action plan was that Europe should take the lead in the field of ICT in the future. Furthermore, the use of digital media should be fostered and all citizens should get easy access to online services. In detail, the three main aims of the published action plan to be achieved by 2002 were [Europe - Summaries of EU legislation, 2003]:

- Cheaper, faster, and secure Internet
- Investing in people and skills
- Promoting Internet use

In more detail, cheaper and faster Internet access should be available for all EU citizens. In particular, schools, students, and researchers should benefit from this aim. In addition, Internet access should be more secure by using smart cards. Furthermore, the action plan stressed to increase the number of people having skills in ICT to strengthen the vision of a knowledge-based economy. Finally, a stimulation of Internet use should enable easier and convenient access to public online services, online health services, or e-Commerce.

After expiration of the activities of the *eEurope 2002* action plan, still not all aims or objectives could be achieved. Hence, in 2002 the European Commission launched a successor action plan called *eEurope 2005* [Commission of the European Communities, 2002] for continuing the visionary aim of making Europe to a more knowledge-based economy. Whereas the main aim of the action plan 2002 had been increasing the number of Internet connections in Europe, the new action plan of 2005 focused on the use of a higher number of Internet connections. Due to that, the European Commission expected an increase in economic productivity and enhanced quality of services.

By using Internet connections, the action plan 2005 foresaw that Europe should have had appropriate e-Government, e-Health, e-Learning, and e-Business services in place by 2005. Thereby, these action

should be accompanied by widely deployed broadband Internet connections and secure information infrastructures. Summarizing, the *eEurope* programme ran from 2000–2005. An evaluation of the results of the *eEurope* 2005 action plan can be found in the publication of the Commission of the European Communities [2009a].

4.1.2.2 i2010

i2010 [Commission of the European Communities, 2005] constitutes the successor initiative of the *eEurope* initiative and was launched in 2005. The *i2010* initiative mainly defined political policies for the information society in Europe. These policies especially focused on promoting knowledge and innovation by creating new and better jobs at the same time. With *i2010*, the European Commission worked on an integrated and overall concept for establishing a uniform and modern information society and audiovisual politics in the EU. Actions to be undertaken amongst the member states should be coordinated and corresponding challenges appropriately faced.

According to the *i2010* initiative, the European Commission proposed three priority policies to achieve the desired goals [Commission of the European Communities, 2005]:

- Completion of a single European information space
- Strengthening innovation and investment in ICT research
- Achieving an inclusive European information society

The completion of a single European information space should guarantee an open and competitive internal market for ICT and media. In such an internal market, financially feasible broadband communication technologies as well as substantial and diverse digital contents and media should be providable. In more detail, the creation of a single European information space requires an increase of speed for broadband networks, a promotion of new and digital content and media, interoperability between devices and platforms, and higher security on the Internet.

By strengthening innovation and investment in ICT research in Europe, the European Commission wanted to foster the creation of more and better jobs in the ICT sector. For achieving that, the European Commission proposed the following measures: Increase the support in ICT research by 80% by 2010, better coordination of research initiatives, or developing tools to support enterprises and organizations by adopting new and innovative work patterns.

Finally, with *i2010* the European Commission wanted to include all European citizens avoiding any digital divide situation. All citizens should benefit from more cost effective and easier accessible public services which subsequently should improve quality of life. To achieve this goal, actions to be undertaken were e.g., the issuance of e-Accessibility policies, the proposal of an initiative for digital integration (e-Inclusion), or adopting an action plan to foster the use of ICT in the public sector.

4.1.2.3 Digital Agenda

Within the Europe 2020 strategy the European Commission has defined seven flagship initiatives. One of these flagship initiatives is called *Digital Agenda* [European Commission, 2010a], which aims on increasing the roll-out of broadband and fast Internet connections. By that, the Commission expects higher growth of the digital internal market and benefits for citizens and businesses. This aim is clearly stated at the first page of the written initiative:

“The overall aim of the Digital Agenda is to deliver sustainable economic and social benefits from a digital single market based on fast and ultra fast internet and interoperable applications.” [European Commission, 2010a]

The European Commission identifies seven obstacles in the *Digital Agenda*, which makes Europe still lagging behind industrial partners or other countries. Examples of these obstacles are lack of interoperability, rising cybercrime, or lack of digital literacy. To tackle these obstacles, the *Digital Agenda* oriented its key actions according to them. The key actions of the *Digital Agenda* are [European Commission, 2010a]:

- A vibrant digital single market
- Interoperability and standards
- Trust and security
- Fast and ultra fast Internet access
- Research and innovation
- Enhancing digital literacy, skills and inclusion
- ICT-enabled benefits for EU society

Currently, the digital internal market is still fragmented. To get a vibrant digital single market, the Commission proposes actions such as completing SEPA (Single Euro Payment Area) [European Parliament and Council, 2012], revising the EU signature directive [European Parliament and Council, 1999b] for creating a legal framework for eID interoperability [European Commission, 2012b], or reviewing the data protection regulation [European Commission, 2012c]. In particular, the Commission highlights the need for more secure authentication mechanisms than username/password schemes, by stating that “*a legal framework for cross-border recognition and interoperability of secure eAuthentication systems*” [European Commission, 2010a] should be provided.

Interoperability and the use of standards should be increased in EU public administrations. In particular, the Commission promotes the adoption of the European Interoperability Strategy (EIS) (cf. Section 4.2.3) and the European Interoperability Framework (EIF) (cf. Section 4.2.4). Furthermore, legal measures on ICT interoperability and the implementation of standards should be proposed.

Cybercrime is an increasing issue not only in Europe but also all over the world. To protect citizens from cybercrime, the Commission proposes the establishment of a European cybercrime platform, stronger collaboration of national CERTs (Computer Emergency Response Teams), or introducing a CERT for EU institutions.

Fast Internet connections are essential for creating jobs and providing citizens and businesses access to the services and content they need. To achieve a wide broadband coverage, the Commission will rationalize the funding of high-speed broadband Internet connections and foster the investment in broadband networks.

Europe currently still has an investment gap in ICT-related R&D. This gap needs to be tackled as ICT is one of the driving EU industrial strengths besides consumer appliances, health, or automobile. To achieve this, the EU wants to yearly increase the ICT R&D budget by 20% and to leverage more private investment.

It is important for innovation and growth to educate European citizens in the use of ICT. Key actions in this field will be the development of tools for recognizing the skills of ICT users and to promote women to work in the ICT sector.

ICT can help to exploit important information in different sectors to address faced challenges in areas such as aging society, climate change, or reducing energy consumption. Therefore, within the *Digital Agenda* the Commission wants to assess the potential of smart grids and to publish a green paper on solid-state lighting.

An essential part of the *Digital Agenda* is its new action plan [European Commission, 2010f]. Main aim of the action plan is to support member states' public administrations to provide and offer better services by reducing costs at the same time. Better services provide citizens and businesses easier and more comfortable access to public services. The action plan contains 40 concrete measures for the next five years. By achieving these measures, consumption of online public services of citizens and businesses should be increased. Furthermore, it should be possible e.g., to license a business, apply for social or health care services, or enroll at universities online.

This new action plan should foster the transition to a new generation. Online public services should become more open, more flexible, and should function seamlessly on local, regional, national, or European level. The action plan should furthermore ensure functionality of online services in all member states. Member states will play a central role when implementing this action plan. The European Commission more or less just creates an appropriate framework for the implementation and the development of cross-border electronic public services.

Summarizing, the action plan foresees the following main measures to be undertaken [Plattform Digital Austria, 2014a] according to the *Malmö Ministerial Declaration* [European Commission, 2009]:

- Better integration of citizens and businesses into the political decision-making processes.
- Strengthening the internal market e.g., due to cross-border acceptance of eIDs or e-Signatures.
- Increasing efficiency and effectiveness of public sector services.
- Creating necessary preconditions (e.g., open technical specifications or interoperability) for developing electronic public services.

4.1.3 Programmes

Along the strategic commitments and the corresponding initiatives the European Commission installed appropriate programmes to illustrate feasibility of the planned actions and activities. These programmes mostly focus on technical interoperability concepts and frameworks, which are projected and piloted to offer cross-border e-Government services. In the following, the most important programmes installed by the European Commission are discussed.

4.1.3.1 Interchange of Data between Administrations (IDA)

The *IDA* (Interchange of Data between Administrations) programme [European Parliament and Council, 1999a] was initiated in 1995 in a first phase. The second phase had started in 1999 and lasted until 2004. *IDA* aimed on building operational, trans-European telematic networks for exchanging data between member states' public authorities and community institutions. The program focused on interoperability to increase efficiency of public administrations when providing online services to European citizens and businesses.

In particular, *IDA* was following these aims [Europe - Summaries of EU legislation, 2005]:

- Reaching a high grade on interoperability between national telematic networks and between European communities and the member states.
- Combining these networks to a common telematic interface between European communities and its member states.
- Achieving substantial benefits for administrations of the communities and the member states due to a decrease of maintenance efforts for the telematic networks and guaranteeing secure and reliable data exchange.

- Transferring the gained benefits of such networks to citizens and businesses of the European Union.
- Distribution and promotion of innovative telematic solutions in the public sector.

IDA supported the creation of services ensuring secure and efficient electronic data exchange between different public administration levels and was part of the *eEurope* initiative. One communication network infrastructure supporting this data exchange between member states' public administrations was TESTA (Trans-European Services for Telematics between Administrations). [Europe - Summaries of EU legislation, 2005]

4.1.3.2 Interoperable Delivery of European eGovernment Services (IDABC)

The *IDABC* (Interoperable Delivery of European eGovernment Services) programme [European Parliament and Council, 2004] constitutes the successor programme of *IDA*. *IDABC* had started in 2005 and ended in 2009. Whereas the *IDA* programme mainly focused on reliable and secure data exchange between public administrations, the *IDABC* programme also takes citizens and businesses more into account.

According to *IDABC* [2009], the main objectives by using ICT were:

- Fostering the development and support of cross-border services for citizens and businesses in the public sector.
- Increase efficiency and effectiveness of collaboration between public administrations across Europe.
- Making Europe an appealing continent to live and work.

Within *IDABC*, several recommendations, solutions, and services were developed to offer citizens, businesses, and public administrations possibilities to communicate electronically across borders. Important results out of the *IDABC* programme were the *European Interoperability Strategy* and the *European Interoperability Framework*, which will be discussed in more detail in Section 4.2.

The *IDABC* programme was part of the *i2010* initiative. The implementation of the programme has also been evaluated in the publication of the Commission of the European Communities [2009b].

4.1.3.3 Interoperable Solutions for European Public Administrations (ISA)

The *ISA* (Interoperable Solutions for European Public Administrations) programme [European Parliament and Council, 2009] follows the prior *IDABC* programme. The *ISA* programme started in 2010 and will last until 2015. The main objective of the *ISA* programme is to support European public administrations to provide efficient e-Government services to citizens and businesses. Furthermore, *ISA* aims on facilitating cross-border electronic collaboration between European public administrations. Focus lies on interoperability and re-use of common tools and services to save costs and time for European public administrations.

The main actions of the *ISA* programme are [European Commission, 2011]:

- Trusted information exchange
- Interoperability architecture
- Assessment of ICT implications of new EU legislation
- Accompanying measures

The cluster on *Trusted information exchange* mainly deals with assuring secure and trustworthy information exchange between the European Commission and the member states. Sample activities are the improvement of semantic interoperability in European e-Government systems or improving access to governmental base registers.

One part of *ISA* deals with an *Interoperability architecture* that should align with existing cross-border and cross-sector IT infrastructures. Detailed activities in this cluster are defining common architectural guidelines and developing common building and re-usable architectural blocks.

Assessment of ICT implications of new EU legislation should ensure that ICT accompanies EU legislation already early in the drafting procedure. This should ensure that the legislation can be implemented in a timely manner after final adoption.

Accompanying measures should ensure the success of the activities of the other clusters in a horizontal way. In addition, focus lies on communication and collaboration between the involved stakeholders.

The *ISA* programme is part of the *Digital Agenda* (cf. Section 4.1.2.3) and aligns with the corresponding e-Government action plan. Finally, it addresses issues according to the *European Interoperability Strategy* and the *European Interoperability Framework* (cf. Section 4.2.3 and Section 4.2.4).

4.2 Interoperability

One of the biggest challenges to implement successful e-Government across borders (either across organizational, sectoral, or national borders) is the interconnection of heterogeneous systems. Usually, each individual public administration relies on their favorite IT infrastructure of their choice. To provide citizens and businesses transactional and integrated public services across borders, the different IT infrastructures need to be interconnected and must be able to exchange data in between. One possibility to achieve interconnection between fragmented systems is interoperability.

4.2.1 Definition

According to Gottschalk and Solli-Sæther [2009], interoperability refers to the *"property of diverse systems and organizations enabling them to work together"*. Aligning with that definition, dos Santos and Reinhard [2011] put data exchange between systems into focus. dos Santos and Reinhard [2011] see interoperability to be *"established through networks and systems that are able to correctly receive, transfer, and use data from different information systems"*. At the first sight, interoperability often refers to systems working together on technical level. However, achieving interoperability on technical level is mostly not sufficient because interoperability also includes social, political, organizational, or legal aspects [Gottschalk and Solli-Sæther, 2009]. The fact that interoperability includes more than simply exchanging data between systems can also be seen by the definition of the European Commission [2010d], which states that:

"Interoperability, within the context of European public service delivery, is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems." [European Commission, 2010d]

According to this definition, knowledge and information needs to be shared on several levels and not only on technical level. Since this definition is tailored to the requirements of European public service delivery, the author refers to this definition when he speaks about interoperability in the further context of this thesis. Further information on interoperability in e-Government can be found in Goldkuhl [2008]; Misuraca et al. [2011]; dos Santos and Reinhard [2011].

4.2.2 The Need for Interoperability

According to Pardo et al. [2011], interoperability is essential to improve e-Government services and procedures for citizens and businesses. Furthermore, it is a key enabler to accomplish more mature e-Government services such as transactional or integrated services. Moreover, it enables information sharing and data exchange across multiple organizations e.g., across sectors or even across borders [Pardo et al., 2011].

The European Commission [2010d] sees interoperability as facilitator for efficient and effective European public services. According to the European Commission [2010d], interoperability addresses the following needs:

- Cooperation
- Information exchange
- Sharing and re-use of information

Referring to the European Commission [2010d], interoperability requires the cooperation between public administrations for being able to set-up new or more mature services. In addition, information needs to be exchanged to fulfill legal or organizational requirements amongst public administrations. Finally, information should be re-used and shared amongst public administrations to create a more effective and efficient e-Government.

For the European Commission [2010d], when achieving interoperability results and benefits are clear. Citizens and businesses can benefit from improved public service delivery. In addition, public administrations can benefit from interoperable solutions due to lower costs, as information can be shared and re-used, and more sophisticated services can be provided to citizens and businesses.

The European Commission has already undertaken a lot of initiatives and programmes to improve efficiency of public sector services by making systems and information exchange interoperable. The main activities were the presented IDA, IDABC, and ISA programmes (cf Section 4.1.3). Since these programmes are very high level and target various aspects of interoperability, in the following the author describes two key concepts on interoperability that have emerged out of the mentioned programmes.

4.2.3 European Interoperability Strategy (EIS)

Interoperability is crucial for European public services to avoid any barriers for cross-border or cross-sector applications. To *“improve interaction, exchange and cooperation among European public administrations across borders and across sectors for the delivery of European public services”* [European Commission, 2010e], the European Commission introduced the so-called *European Interoperability Strategy (EIS)*. The preparation of the *EIS* had started during the *IDABC* programme (cf. Section 4.1.3.2) whereas the strategy was finalized in the *ISA* programme (cf. Section 4.1.3.3). The *ISA* programme is also responsible for maintaining the strategy document.

According to the European Commission [2010b], the *“European Interoperability Strategy (EIS) can be defined as an action plan to address cross-boundary interoperability aiming at facilitating the implementation of EU policies and initiatives”*. Hence, the aim of this strategy is to prioritize actions needed for achieving interoperability and to guide European public administrations through the process of improving interoperability. Focus is put on defining definite actions on national and EU level [European Commission, 2010b]. Next steps are to convert the strategy into concrete projects and activities within the *ISA* programme.

4.2.4 European Interoperability Framework (EIF)

The *European Interoperability Framework (EIF)* was introduced in its first version [European Commission, 2004] during the IDABC programme in 2004. The existing interoperability framework has been properly amended and modified at the beginning of the *ISA* programme. The current version 2.0 of the EIF [European Commission, 2010d] was finally adopted in 2010.

The European Commission [2010d] defines an interoperability framework as follows:

“An interoperability framework is an agreed approach to interoperability for organisations that wish to work together towards the joint delivery of public services. Within its scope of applicability, it specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices”. [European Commission, 2010d]

Basically, the *EIF* is not a technical document but moreover provides guidelines and recommendations on various interoperability levels for designing and developing interoperable European public services. By this, cross-sector and cross-border interoperability for European public services should be promoted and thus citizens and businesses should benefit from a better integrated internal market. [European Commission, 2010d]

Besides underlying principles and conceptual models for European public services, the *EIF* defines four different levels of interoperability. When implementing a new European public service or intending to interconnect existing ones, then all these levels need to be considered. Figure 4.1 illustrates the different interoperability levels. The definition of different interoperability levels or layers is not unique to the EIF. Similar distinctions can be found in e.g., Goldkuhl [2008]; Gottschalk and Solli-Sæther [2009]; Misuraca et al. [2011]. In the following, the individual interoperability levels are explained according to the European Commission [2010d].

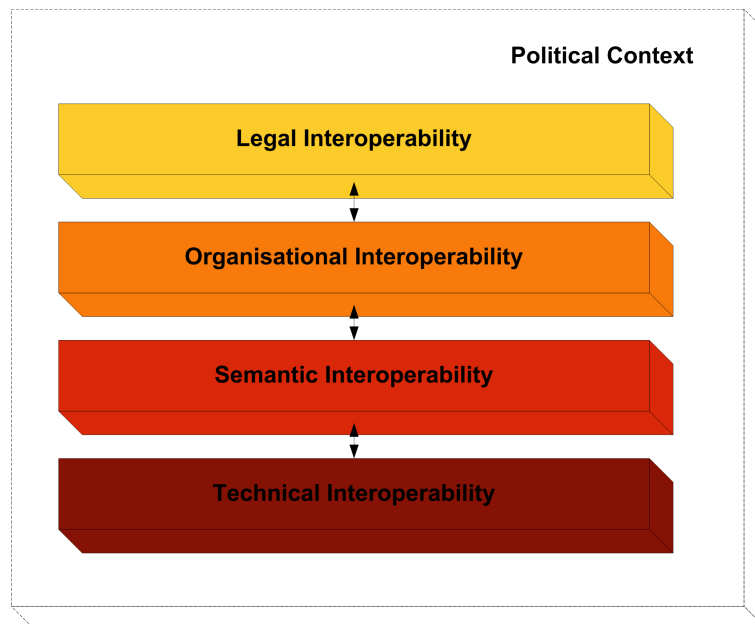


Figure 4.1: Interoperability Levels [European Commission, 2010d]

Technical Interoperability: This interoperability layer covers all technical aspects to interconnect systems. To achieve interoperability on this level, public administrations should rely on common specifications, data exchange formats, or existing standards.

Semantic Interoperability: Interoperability on semantic level means that each public administration is aware of the exact meaning of exchanged data. Multilingualism, which is present all over the EU,

is one of the main issues to be bypassed for achieving interoperability on this level. To achieve semantic interoperability, appropriate vocabulary describing the exchanged data should be used or developed respectively. Furthermore, exchanged data should also be syntactically correct e.g., in terms of grammar or format.

Organizational Interoperability: Cooperation between public administrations – within one country or cross-border – is targeted by this level. Thereby, public administrations agree on the business process to be interconnected and integrated into common services or on the data to be exchanged. Agreements can be mutual or based on joint actions or cooperation.

Legal Interoperability: Public administrations usually provide public services compliant to their respective national law. However, differences in law may exist e.g., between member states. If data are exchanged across borders, it must be ensured that the respective national law stays valid even if data are transferred to another country.

Political Context: Establishing new European public services requires a solid political basis. All stakeholders involved must follow a common and agreed strategy and align with priorities and agreed objectives. The political context paves the way for achieving interoperability of European public services on all prior discussed interoperability levels.

4.3 Large Scale Pilot Projects

A lot of e-Government services exist on national as well as on European level. However, usually they have been tailored to domestic needs only and hence lack in cross-border applicability. To bypass this issue and to foster interoperability of public services across borders, the European Commission had launched so-called Large scale pilot projects (LSPs) in the areas eID, e-Business, e-Health, e-Procurement, and e-Justice. The pilot projects have been initiated and carried out within the *ICT Policy Support Programme (PSP)*, being part of the *Competitiveness and Innovation Framework Programme (CIP)*. Projects run in these programmes are funded by the European Commission with the final aim on achieving the goals defined in the *Digital Agenda* (cf. Section 4.1.2.3). In particular, the aims of the LSPs are the development of interoperable solutions for creating cross-border services in the main key areas (e.g., e-Government, e-Health, etc.), the re-use of existing infrastructure, and making the results publicly available and free to re-use.

In the following subsections, the seven LSPs targeting different policy areas are briefly explained. Three LSPs (STORK, SPOCS, PEPPOL) are already completed whereas the others are still running. Further information on the individual LSPs can also be found in Stranacher et al. [2011].

4.3.1 STORK

The increasing number of e-Business and e-Government services, which process sensitive data, demand also more secure and reliable identification and authentication mechanisms. In the past, many European countries followed this demand by rolling-out national eID solutions (for examples the author refers to Section 5.1). However, legal differences (e.g., data protection requirements) led to country-specific solutions and a heterogeneous eID landscape in Europe. The LSP project STORK¹ (Secure idenTity acrOss boRders linKed) tried to seize this drawback by creating an eID interoperability framework based on the individual national solutions. This framework enables secure identification and authentication of natural persons across borders. STORK started to pilot its interoperability framework in 2010 to evaluate the developed solution.

¹<https://www.eid-stork.eu>

In STORK, two interoperability models exist. In the first model, a so-called PEPS (Pan-European Proxy Service) acts as gateway hiding the national eID solution from the STORK interoperability layer. In the second model, a service provider directly incorporates the national eID solution (Middleware Model). Since cross-border electronic identification and authentication are main parts of this thesis, the LSP STORK will be described in detail in Section 5.5.

4.3.2 STORK 2.0

The STORK project ended in 2011. STORK 2.0² constitutes the successor project of STORK and builds upon the results of the first project. Focus lies on the use of electronic identities for legal persons and on modeling electronic representation between legal persons and natural persons. In addition, STORK 2.0 includes further piloting to evaluate the applicability of the developed and deployed solutions also in stronger cooperation with the private sector.

In general, the main objectives of STORK 2.0 are [STORK 2.0 Consortium, 2013]:

- Develop an interoperability framework based on national eID solutions also for non-natural persons
- Develop common specifications and building blocks for re-use
- Agree on mutual recognition of national eIDs in each member state
- Pilot the developed framework in different areas such as e-Learning, e-Banking, or e-Health

4.3.3 SPOCS

The EU services directive [European Parliament and Council, 2006] stipulates that several procedures, which are related to the exercise and uptake of services activities, must be processable electronically. The implementation of the services directive foresees the installation of so-called "*Point of Single Contacts*" (PSCs). A PSC acts as intermediary between an applicant, who wants – for instance – to open a business in a foreign EU country, and the actual national public authority that is responsible for processing the application. The national public authorities are usually called competent authorities (CAs) in the context of SPOCS.

To facilitate processing of cross-border procedures and to improve existing implementations of PSCs, the European Commission launched the LSP SPOCS³ (Simple Procedures Online for Cross-border Services) in 2009. In particular, provision of cross-border services for EU citizens should be facilitated. SPOCS developed several technical building blocks enabling content syndication, cross-border electronic delivery, or the interoperable cross-border exchange of electronic documents. The cross-border document exchange is supported by a special interoperable container format called OCD (Omnifarious Container for e-Documents) [Stranacher and Zwattendorfer, 2012].

An OCD container consists of a logical and physical structure. The logical structure is based on three layers: *payload layer*, *metadata layer*, and *authentication layer*. The *payload layer* includes the actual electronic document to be transferred. The *metadata layer* contains additional information on the payload and the container itself. Finally, the optional *authentication layer* ensures the possibility to electronically sign the container thereby guaranteeing integrity and authenticity. The physical structure defines the physical implementation of the logical structure. Currently, ZIP-based and PDF-based implementation formats are supported. Further details on the OCD container and its structure can be found in Stranacher and Zwattendorfer [2012].

²<https://www.eid-stork2.eu>

³<http://www.eu-spocs.eu>

The SPOCS project ended in 2012. In the period between 2009-2012 the results of the project were evaluated and piloted supporting different life events in cross-border scenarios.

4.3.4 epSOS

The goal of the LSP epSOS⁴ (Smart Open Services for european patients), which started in 2008 and which is still running, is to achieve interoperability for e-Health services on a pan-European level. In particular, epSOS aims *”to develop a practical eHealth framework and ICT infrastructure that will enable secure access to patient health information, particularly with respect to a basic Patient Summary (PS) and ePrescription (eP, including eDispensation - eD), between European healthcare systems”* [EpSOS, 2008].

According to Hurch and Heider [2010], *”the main functionality of the epSOS LSP environment is the provision of patient health data stored in patient’s home country to a health care professional providing health service in a foreign country”*. Hence, the main objective of epSOS is the establishment of an interoperable infrastructure to achieve cross-border provision and exchange of patient health data. The developed interoperability infrastructure sets upon existing national solutions. In more detail, epSOS pilots three different use cases for cross-border health data transfer. The first piloted use case enables the secure and reliable transfer of patient data across borders (Patient Summary). The second use case deals with the issuance of electronic prescriptions (e-Prescription). Finally, the last use case allows for the cross-border dispense of medication (e-Dispensation).

Basic building blocks of the infrastructure proposed by epSOS are the so-called *National Contact Points (NCP)* that act as interfaces between different national eHealth infrastructures. According to Kolitsi and Wilson [2010], an *”epSOS NCP is identifiable in both the epSOS domain and in its national domain, acts as communication gateway, and establishes a Circle of Trust amongst national Trusted Domains”*. The author discusses the infrastructure and use cases of epSOS a bit more in detail in Section 4.3.8.

4.3.5 PEPPOL

PEPPOL⁵ (Pan-European Public Procurement Online) was the first project of the LSPs and was launched in 2008. The aim of this project was to strengthen the competitiveness of – in particular small- and medium-sized – enterprises by providing an EU-wide electronic procurement system for public authorities. The aim was achieved by interconnecting national procurement systems through well-defined standards and an appropriate interoperability architecture. The PEPPOL interoperability framework thereby consists of the following five components [Stranacher et al., 2011]:

- Electronic signatures for ensuring integrity and authenticity (e-Signature)
- Virtual Company Dossier (VCD) as proof of suitability (e-Attestation)
- Virtual directories as basis for publication of goods or services information (e-Catalogue)
- Electronic ordering of goods and services (e-Ordering)
- Issuance of electronic invoices (e-Invoicing)

All these components are interconnected through the PEPPOL Transport Infrastructure. The results of the PEPPOL interoperability infrastructure have been evaluated and piloted in operational environments until 2011.

⁴<http://www.epsos.eu>

⁵<http://www.peppol.eu>

4.3.6 e-CODEX

The LSP e-CODEX⁶ (*e-Justice Communication via Online Data EXchange*) started in 2010 and will last until 2015. Its aim is making cross-border jurisdictional procedures cheaper, more transparent, and more efficient. Priority of this project is interconnecting existing jurisdictional infrastructures to enable citizens and organizations more flexible access to jurisdictional data.

Summarizing, the main objectives of this pilot are [Stranacher et al., 2011]:

- Qualified identification of citizens and organizations across borders
- Common standard for cross-border recognition and processing of electronic documents
- Cross-border jurisdictional data exchange

4.3.7 e-SENS

In 2013, the European Commission launched a new LSP called e-SENS⁷ (*electronic Simple European Networked Services*) to strengthen the digital internal market. Background of this project are various barriers that still exist and hinder a pan-European usage of electronic public services. Citizens and businesses still need to suffer a high level of bureaucracy for accessing online services. Without interoperability between European public administrations and different member states it is impossible to provide citizens and businesses pan-European online public services. [Plattform Digital Austria, 2014b]

This new LSP does not aim to re-invent the wheel but rather tries to build upon existing results achieved within the other – partly already finished – LSPs. E-SENS aims on consolidation and proper re-use of available building blocks such as eID, e-Signature, e-Documents, or e-Delivery. The main goals of this project are the interconnection of national digital services networks and the provisioning of new public services based on a standardized European infrastructure. Furthermore, setting up a business in a foreign member state should be facilitated and citizen support should be increased e.g., if they live in a foreign member state because of work or education. [Plattform Digital Austria, 2014b]

4.3.8 Comparison between STORK and epSOS

The interoperability objectives of the two LSPs STORK and epSOS are going in the same direction. Both projects aim to establish interoperability between country specific solutions rolled out on the large scale. In this section, the author looks at similarities between STORK and epSOS in more detail and analyzes their significant differences. [Zwattendorfer et al., 2011b]

The most apparent similarity between STORK and epSOS is their operating principle: both LSPs aim to facilitate the secure and reliable cross-border data exchange between EU member states while retaining already existing country-specific infrastructures. The architectures of STORK and epSOS are basically comparable as being illustrated in Figure 3. Both LSPs rely on national gateways, through which cross-border data exchanges are processed. All gateway instances belong to a so called *Circle of Trust* that is based on agreed policies of a particular governance structure in order to mutually establish trust relationships. In STORK, these gateways are called PEPS, while epSOS refers to these components as NCP. Figure 4.2 illustrates the gateway concept of STORK and epSOS. Nevertheless, the basic intention of using one single gateway per EU member state is the same in both LSPs.

In both projects, data are exchanged but not shared between different member states. Admittedly, the requested information is forwarded by the involved gateways for temporary use, but is never stored in the foreign country's infrastructure. Besides the overall architecture, the conceptual and technical

⁶<http://www.e-codex.eu>

⁷<http://www.esens.eu>

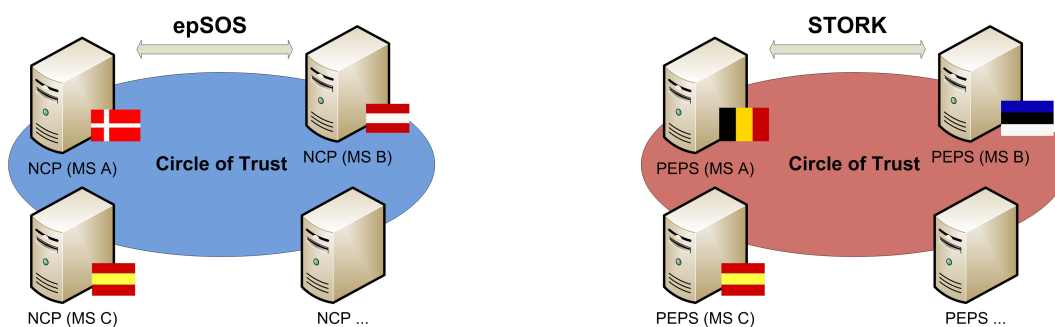


Figure 4.2: Circle of Trust in epSOS and STORK [Campari et al., 2010]

design of those gateways is very similar. Both, the PEPS and NCP concepts internally rely on a platform independent model and make use of web standards based on XML for cross-border communication and data exchange.

Besides these similarities, there are also some significant differences. One apparent difference is the kind of information being exchanged across borders. While STORK basically exchanges only simple attributes, epSOS proposes the exchange and transformation of complex documents. Another major difference is the use case. While STORK supports cross-border identification and authentication of citizens only, epSOS additionally aims at cross-border exchange of patient health data. Besides secure and reliable transmission of patient health data, identification has been identified as a key element of the epSOS LSP. Reliable identification and authentication mechanisms are vital to unambiguously identify patients and to ensure that privacy-sensitive health data are protected and accessed by authorized health care professionals (HCP) only.

Even if both LSPs rely on a common XML-based transport protocol, further differences can be found on message level. For instance, STORK only supports a request/response messaging mechanism, whereas epSOS additionally relies on a notification message. However, for identification and authentication both projects rely on the well-established Security Assertion Markup Language (SAML) standard (cf. Section 3.5.2).

Even though STORK and epSOS have some apparent similarities, also several significant differences between these two LSPs have been identified. Nevertheless, there is much potential to use synergies between these projects. A more detailed analysis of similarities and differences between epSOS and STORK and how synergies could be exploited can be found in Campari et al. [2010]; Leitold et al. [2011]; Zwattendorfer et al. [2011b].

By this example, it can be seen that further take up of the building blocks developed within the individual projects is essential and cohesion is required. Hence, although the individual LSPs provided important results, further initiatives (such as e-SENS or the ISA programme) aiming on making interoperability more mature are crucial.

4.4 Chapter Conclusions

For being able to strengthen the EU internal market, data and services need to be exchanged electronically and accepted also across borders. In order to achieve this, cross-border interoperability of the heterogeneous landscape of existing systems, solutions, and infrastructures in the individual member states has been identified by the EU as one of the biggest challenges. To tackle the challenge of cross-border interoperability in public sector areas such as e-Government, the European Commission made a lot of strategic commitments and installed appropriate initiatives and programmes.

Out of these programmes, large scale pilot (LSP) projects were launched and co-funded by the EU to get some hands-on experience dealing with cross-border interoperability in real life scenarios and

applications. One of this LSPs is STORK, which particularly aimed on achieving eID interoperability across borders. The STORK project is an essential part of this thesis and will be described in detail in the next chapter. However, by this prior chapter on cross-border e-Government the reader should be aware of the importance and need of interoperability across the EU and how STORK fits into the big EU interoperability picture.

Chapter 5

Cross-Border Electronic Identity

While the Austrian citizen card or any other European eID solution are fully able to satisfy national demands and requirements for identification and authentication, they usually lack applicability in other countries. Reasons are their differences on technical, organizational, or legal level. For instance, on technical level some countries rely on secure smart card-based approaches for their eID solutions whereas others still rely on weaker username/password schemes. On organizational level, national eIDs might be issued from governments on national or regional level, or they might be issued by the private sector. Finally, on legal level differences can exist on the use of national identifiers and the compliance to data protection regulations. In some countries the use of one unique identifier across several services and sectors is allowed (e.g., in Belgium) whereas in others it is forbidden by law (e.g., in Austria).

To foster the European internal market and to make the EU a more knowledge-based society, the use of cross-border e-Government services is essential. However, to achieve this, the cross-border acceptance of the various heterogeneous national eID solutions within the EU builds a fundamental basis. Without being able to uniquely identify and securely authenticate EU citizens across borders, e-Government services in a pan-European context will neither work nor they will become integrated reality. To bypass existing gaps for cross-border eID acceptance, the European Commission put a lot of effort in corresponding initiatives and projects. On legal and organizational level, the upcoming new eIDAS regulation [European Commission, 2012b] will build the fundamental basis. On technical level, the European Commission launched the large scale pilot (LSP) projects STORK (Secure Identity Across Borders Linked) and STORK 2.0 to deal with technical issues on eID acceptance for natural and legal persons. Since the author was mainly involved in the design and development process in STORK, the focus of this chapter is put on details to STORK. Nevertheless, the STORK framework will also play an important role in subsequent chapters, hence by reading this chapter the reader should get a detailed knowledge on the basic STORK concepts and its architecture.

The chapter is structured as follows. Section 5.1 overviews four different countries with respect to their eID solutions. This section should illustrate the differences of the existing eID landscape in Europe. Section 5.2 briefly introduces the two basic possibilities for achieving cross-border eID acceptance, namely either rolling-out a unified electronic identity across Europe or making the existing national eID solutions interoperable. Focus of this chapter is on interoperability, thus Section 5.3 summarizes and lists challenges on technical, organizational, and legal level which need to be considered and bypassed when aiming on cross-border eID interoperability. The subsequent Section 5.4 briefly describes early eID interoperability approaches that were conducted over the past years. Finally, details on the last and most popular eID interoperability approach STORK, which was co-funded by the European Commission, are given. Details include descriptions of the four different STORK interoperability models, their implementation, as well as the integration of the STORK framework in Austria.

5.1 Electronic Identities in Europe

Based on the EU signature directive [European Parliament and Council, 1999b] from 1999, EU member states started to roll out national eID solution supporting the national implementation of this directive. In fact, national eID implementations support the features of unique identification and secure authentication in online applications. Early birds having rolled out nation-wide eID cards were Finland (in 1999) and Estonia (in 2002). Austria started in 2003 and did a mass roll out in 2005. In 2003 also Italy started first tests whereas Belgium already went into production in 2003. [Meints and Hansen, 2006]

While all these solutions focused on client-side approaches using smart cards, in the recent years also server-side solutions such as the Austrian Mobile Phone Signature¹ gained popularity. However, all those solutions had been tailored to satisfy national requirements only and lacked in interoperability. Interoperability approaches will be discussed in the next section. In this section, selected national eID solutions are briefly elaborated. Information on other national eID solutions can be found e.g., in Hayat et al. [2004]; Meints and Hansen [2006]; Hayat [2007]; Graux et al. [2009c]; Arora [2008b,a]; Zefferer [2010]; Helmbrecht and Naumann [2011].

5.1.1 Belgium

Belgium was one of the first countries that issued eID cards to all their citizens [Cock et al., 2004]. The Belgium eID card is called BELPIC (Belgian Personal Identity Card). As of June 2009, 7.5 million valid eIDs were issued [Zefferer, 2010]. The BELPIC can be used as both, as a physical and visual ID, and as electronic ID. Personal data are printed on the card as well as are stored electronically on the card [Cock et al., 2004]. Personal data include the citizen's name, date and place of birth, gender, photo, nationality, etc. and a unique national register number (RRN Number) [Cock et al., 2006]. This unique number is assigned to each Belgian citizen by the national register and further used for unique identification at online services. In contrast to the Austrian eID concept (cf. Section 3.6.1), the RRN number is not derived but rather used directly for identification. Moreover, the card holds a handwritten signature of the citizen as well as validity dates [Cock et al., 2006]. In general, the BELPIC is valid for five years [Cock et al., 2006]. All these personal data are stored within a so-called "identity file", which has been digitally signed by the national register [Cock et al., 2006].

Basically, the Belgian eID card supports the following three use cases [Arora, 2008b; Cock et al., 2004]:

- Citizen authentication
- Qualified electronic signature creation
- eID card authentication

All these functionalities are realized by appropriate RSA private/public key pairs and corresponding certificates on the card. The size of all key pairs is 1024bit and they are generated on the card during the initialization process [Cock et al., 2004]. The first key pair and the corresponding X.509 certificate is used for citizen authentication using a SSL/TLS client authentication scheme [Arora, 2008a]. For the creation of qualified electronic signatures the second key pair and the corresponding qualified certificate is used [Cock et al., 2004]. Finally, the third key pair has no corresponding certificate. The national register knows the link between public key and eID card and thus each eID card can be authenticated by the national register [Cock et al., 2004]. The two certificates contain the name and the RNN number of the citizen [Cock et al., 2004]. There is no encryption and decryption functionality on the card [Cock et al., 2006]. Further information on the Belgium eID card can be found in Cock et al. [2004, 2006, 2011]; Graux et al. [2009a]; Keersebilck and Dufraimont [2008], or on <http://eid.belgium.be>.

¹<https://www.handy-signatur.at>

5.1.2 Estonia

Estonia started with the deployment of an identity card already in 2002 [Zefferer, 2010]. As of June 2009, 1.1 million valid eIDs have been issued [Zefferer, 2010]. This is an interesting number as nearly the same number (1.3 million) of residents is entitled to apply for an eID card [Zefferer, 2010]. Similar to the Belgian eID card, the Estonian eID card can be used as physical ID document and as an electronic one [AS Sertifitseerimiskeskus, 2003]. Also the data stored on the card is similar. These data include the card holder's name, birth time, sex, citizenship, etc. and personal code (national ID code – PIC) [AS Sertifitseerimiskeskus, 2003]. This personal code can be used for unique identification and is publicly available [AS Sertifitseerimiskeskus, 2003].

There are two digital certificates stored on the eID. One is used for authentication and one for electronic signature creation. Thereby, qualified electronic signatures can be created according to the EU signature directive [European Parliament and Council, 1999b]. Both certificates follow the RSA 1024bit standard [Zefferer, 2010]. According to AS Sertifitseerimiskeskus [2003], the eID has no restrictions and can be used in the public and private sector. There is also no authorization information stored on the card or within the certificates. However, both certificates contain the card holder's name and the national ID code [AS Sertifitseerimiskeskus, 2003].

According to Martens [2010], applications of the Estonian eID card are:

- Electronic identification and authentication
- Qualified electronic signature creation
- Electronic ticketing in Estonian public transportation
- Partial replacement of a driver's license (only for identification purposes)
- Internet banking
- Internet voting (I-Voting)
- e-Health services

Besides the Estonian eID card, a mobile solution (Mobile-ID) was introduced in 2007. To get the Mobile-ID solution to work, Estonian citizens need to exchange their normal SIM card with a PKI-capable one. After that, the new SIM card needs to be activated as Mobile-ID through a web environment. Main advantage of the mobile solution is that no extra card reader is needed. [Graux et al., 2009b]

Further and detailed information of the Estonian eID solution can be found in AS Sertifitseerimiskeskus [2003]; Graux et al. [2009b]; Martens [2010], and on <http://id.ee>.

5.1.3 Germany

In comparison to the previous countries, Germany was late with rolling out a national eID solution across the country. In 2010, the new German eID card (neuer deutscher Personalausweis - nPA) was distributed to German citizens [Fromm and Hoepner, 2011]. In contrast to all of the other European card-based eID solutions, the German eID card is implemented as contactless smart card [Margraf, 2010]. However, similar to other eID solutions the German eID card has a physical and electronic ID functionality. Data visible on the card is also stored on the card [Fromm and Hoepner, 2011]. The following data can be found on the card [Fromm and Hoepner, 2011]: name, title, date and place of birth, address, etc.

Basically, the German eID card has the following functions [Poller et al., 2012]:

- ePass function

- eID function
- eSign function

The ePass function is similar to an electronic passport and stores an electronic identity – representing all data necessary for passport functions – on the card. These data can be queried also in offline authorization and inspection systems. The eID function can be used in online processes for secure identification of the citizen. Finally, the eSign function allows the creation of qualified electronic signatures. While the ePass function is mandatory, the eID and eSign functions are optional and must be activated by the citizen. [Poller et al., 2012]

In addition to that, the German eID card supports three other functions which are more or less unique in comparison to other European eID solutions. These functions according to Fromm and Hoepner [2011] are the following.

First, the eID card can optionally store biometric data such as fingerprints. These fingerprints are particularly protected and can only be accessed by official authorities when the card is physically present. Hence, biometric data can never be read out via the Internet. [Fromm and Hoepner, 2011]

Second, privacy aspects are taken into account, i.e., the German eID card – for instance – supports data minimization functions. In particular, the German eID card supports the privacy functions of age verification, residence verification, and pseudonymous identification [Fromm and Hoepner, 2011]. The age verification function allows online applications just to verify the age without transmitting the full date of birth (cf. Section 3.1.2.4). The same holds for residence verification, as only a regional identifier is disclosed to a service provider but not the full home address. Finally, the pseudonymous identification functionality is similar to the Austrian approach (cf. Section 3.6.1). The German eID card also allows for the generation of sector-specific identifiers (pseudonyms). [Fromm and Hoepner, 2011]

Finally, the third function concerns mutual authentication. This means that not only the citizen identifies and authenticates at the service provider but also the service provider does so at the citizen. To achieve this, service providers need to get approved by the Federal Office of Administration. Thereby, the service providers get issued a so-called access or authorization certificate, which allows the service provider to read specific data from the citizen's eID card. However, the service provider only gets permission to read the amount of data that are really required for providing the service. With the access certificate, the service provider cannot access as much data as it wants. [Fromm and Hoepner, 2011]

The German eID card has particular advantages in terms of privacy compared to other national eID solutions. More information on the German eID card, its architecture, and used protocols can be found in Hornung and Roßnagel [2010]; Margraf [2010]; Fromm and Hoepner [2011]; Poller et al. [2012].

5.1.4 Italy

Italy started already very early with its first issuance of eID cards in 2001 [Talamo et al., 2011]. The two major eID projects in Italy are the "Carta d'Identità Elettronica" (CIE) and the "Carta Nazionale dei Servizi" (CNS). The CIE is issued on national level and acts as physical travel document as well as eID [Zefferer, 2010]. The CNS card is only deployed on regional level [Zefferer, 2010] and has not the whole functionality of the CIE [Talamo et al., 2011]. As of 2010, 1.8 million Italian citizens have been issued a valid eID [Talamo et al., 2011].

Since the CIE can be used as physical and electronic ID, certain identity data are printed and stored on the card. These are – for instance – the name of the municipality issuing the card, the card holder's name, the date and place of birth, gender, height, address, fiscal code, etc. [Talamo et al., 2011]. For unique citizen identification, the fiscal code (Codice Fiscale) is used [Zefferer, 2010]. Finally, the CIE also contains biometric data (fingerprint templates). However, biometric data is particularly protected as it is only stored on the card and not in any database. Furthermore, biometric data can only be accessed by public authorities in the presence of the card holder [Talamo et al., 2011].

In fact, the CIE includes three different digital certificates supporting three different functions [Talamo et al., 2011]:

- CIE authentication
- Signature creation for citizen-to-government transactions
- Signature creation for citizen-to-business transactions

The first certificate is used for authenticating Italian citizens in online processes. The other certificates are used for creating digital signatures. The Italian eID concept thereby distinguishes between signatures to be used between public administrations and companies of the private sector. However, the certificate used for the public sector is qualified according to the EU signature directive [European Parliament and Council, 1999b]. [Talamo et al., 2011]

As already discussed, biometric data are especially protected. In addition, also citizens' privacy is preserved. The authentication certificate does not include the card holders name but rather the SHA-1 hash of the card holder's personal data [Talamo et al., 2011].

Further information on the Italian eID solution can also be found in Gentili [2001].

5.2 Possible Approaches for Cross-Border eID

As can be seen from the previous section, the eID landscape across Europe is very heterogeneous. The eID solutions vary on different levels (organizational, legal, technical) [Posch, 2008]. On organizational level, differences can be found in issuance or deployment. For instance, eIDs might be issued by both the public and the private sector. Additionally, national or just regional solutions might exist. On legal level, national data protection regulations can show up differences. For instance, Austria uses a sector-specific model for protecting the citizen's unique identifier whereas in Estonia the unique identification code is publicly available. Finally, the individual European countries rely on different technologies. Whereas Belgium, Germany, and Italy just rely on smart cards, mobile solutions are deployed in Austria and Estonia.

These differences and heterogeneity raised the need for the European Commission to start according initiatives to strengthen the European internal market by having eID acceptance across the EU. This need has been manifested in different strategic approaches and initiatives (cf. Section 4.1). Different approaches exist for achieving cross-border acceptance of eIDs. In this section, the two possibly approaches are briefly introduced. The first approach refers to the unification of eID in Europe and the roll out of a uniform eID for all countries. The second approach is interoperability, which aims on cross-border acceptance of national eID solutions without changing the complete national eID infrastructure. In the remainder of this chapter, focus is put on eID interoperability. A summary of initiatives for a pan-European identity management can be found in Graux and Dumortier [2009].

5.2.1 Unifying European Electronic Identity

The first approach for achieving cross-border acceptance of eIDs in Europe is unification. This means that one single eID solution – probably based on different implementations – is rolled out to all European citizens. One effort going in this direction is the so-called European citizen card (ECC). In the following subsection the ECC is briefly elaborated.

5.2.1.1 European Citizen Card (ECC)

The vision of the European citizen card (ECC) concept is the issuance of an ECC card to each European citizen and to facilitate the identification process when using services, either typically during interactions with public administrations or online when doing e-Government or e-Business. The ECC specification defines two interfaces to ease the integration into an electronic identity management system. These interfaces are implemented by a middleware stack.

The European citizen card fits into the initiatives launched by the European Commission to bring the European Union closer to its citizens and to promote a competitive European internal market. The vision is that every European citizen possesses such a high secure and privacy-protecting card. The ECC should help citizens to prove their identity in everyday life when using cross-border services. The CEN/TC 224 WG15 [2012a] defines the European citizen card as *"a smart card issued under the authority of a government institution, either national or local and carries credentials in order to provide all or part of the following services: 1.) verify the identity; 2.) act as an Inter-European Union travel document; 3.) facilitate logical access to e-government or local administration services."*

Thus, on the one hand the ECC should act as an ID card in typical authentication processes like border controls, on the other hand it should ease and enable the secure usage of e-Government or e-Business services and applications respectively. The core of the ECC builds the electronic signature capability which is compliant with the EU signature directive [European Parliament and Council, 1999b]. With this capability, users – who possess an ECC – are able to legally identify themselves online without having any personal contact with the verifying party. This leads to a further step in the development of a European smart card based model for electronic identity management.

The specification of the European citizen card has been released by CEN (Comité Européen de Normalisation). The technical specification (CEN/TS 15480 - Identification card systems - European Citizen Card) consists of a set of five documents describing specifications reaching from general information to smart cards characteristics and to operational profiles. The technical specification developed by the CEN/TC 224 WG15 consists of the following parts:

- Part 1: Physical, electrical and transport protocol characteristics (CEN/TS 15480-1) [CEN/TC 224 WG15, 2012a]
- Part 2: Logical data structures and card services (CEN/TS 15480-2) [CEN/TC 224 WG15, 2012b]
- Part 3: European Citizen Card Interoperability using an application interface (CEN/TS 15480-3) [CEN/TC 224 WG15, 2010]
- Part 4: Recommendations for European Citizen Card issuance, operation and use (CEN/TS 15480-4) [CEN/TC 224 WG15, 2012c]
- Part 5: General Introduction (CEN/TS 15480-5) [CEN/TC 224 WG15, 2013]

Further and detailed information on the European Citizen Card can be found in the individual specifications CEN/TC 224 WG15 [2012a,b, 2010, 2012c, 2013] or in Eurosmart [2008]; Ivkovic and Preliteiro [2010].

5.2.2 Interoperability of European Electronic Identities

Myhr [2008] discusses the creation of a unified European eID. However, he found two major legal and organizational obstacles for achieving a unified eID. According to Myhr [2008], the first obstacle concerns the issuance procedures of an eID. In detail, achieving the vision of a unified eID across Europe would require harmonization of the individual eID issuance procedures or pan-European acceptance of the individual national procedures. However, Myhr [2008] sees difficulties in achieving mutual acceptance

of eID issuance procedures. The second proposed obstacle concerns the content of the eID and the verification of the eID. Thereby, Myhr [2008] raises the question on how citizens could be uniquely identified in a cross-border context since most countries rely on different identification procedures. Furthermore, Myhr [2008] discusses the amount of data necessary on an eID for proving an identity.

Based on these findings, Myhr [2008] concludes that unification cannot be achieved for cross-border eID acceptance in the short run. Hence, the European Commission should follow an interoperability approach. The need for eID interoperability has already been recognized by the European Commission in several initiatives (cf. 4.1) [Krontiris et al., 2011]. Thereby, the European Commission does not roll out a new eID solution to all EU citizens but rather tries to make the individual national eID solutions interoperable. eID interoperability pertains different levels. On legal level, the European Commission is currently drafting a new regulation [European Commission, 2012b] for cross-border identification that should supersede the current legal basis of the EU signature directive [European Parliament and Council, 1999b]. On technical level, the European Commission ran the EU LSP project STORK, which implemented, demonstrated, and piloted a technical eID interoperability framework.

The remainder of this chapter discusses eID interoperability – in particular on technical level – in detail.

5.3 Challenges for Cross-Border Electronic Identity

In order to achieve interoperability in a pan-European and cross-border context between different national eID solutions, several challenges must be met. Too different are the individual eID solutions in most cases. In particular, differences exist on various levels. In the following, based on the work of Majava et al. [2009]; ENISA [2010]; Hayat et al. [2004]; Krontiris et al. [2011] challenges that should be overcome for achieving eID interoperability are discussed on technical, organizational, and legal level.

5.3.1 Technical Challenges

In the following, technical eID interoperability challenges are discussed.

Different eID approaches: According to Majava et al. [2009], differences in the eID approach between EU countries exist. Some countries rely on a centralized approach whereas others prefer a decentralized approach for their eID system. For achieving interoperability, both eID approaches need to be interconnected.

Different credentials: Member states rely on different credentials or tokens [Majava et al., 2009; ENISA, 2010]. For instance, eID credentials can be smart cards, mobile phones, or even username/password pairs [Majava et al., 2009].

Standards: Different eID implementations rely on different standards. Hence, harmonization of standards can be seen as technical challenge. [Majava et al., 2009; Hayat et al., 2004]

Different middleware: In case client-side solutions such as smart cards are used as eID implementation, usually a piece of software (middleware) is installed within the user's domain. However, the middleware usually provides access to the specific national smart card only and not to smart cards of other countries [Hayat, 2007].

5.3.2 Organizational Challenges

In the following, organizational eID interoperability challenges are discussed.

Semantics: Referring to Majava et al. [2009], semantic interoperability between national eID infrastructures is essential. Common agreements on eID data need to be achieved.

Different certificate authorities (CAs): Currently, electronic identification is based on qualified electronic certificates according to the EU signature directive [European Parliament and Council, 1999b] in most EU member states. Hence, cross-border acceptance of eIDs is also dependent on the acceptance of various qualified CAs. While this is legally ensured by the EU signature directive, technical enforcement still produces practical issues [Hayat, 2007]. An approach to bypass technical issues are trust-service status lists (TSLs) [Stranacher et al., 2013b].

User habits: According to Hayat [2007], citizens have different habits in using IDs. These habits can also influence the use of eIDs. In addition, the implementation of an eID (e.g., smart card, mobile phone, USB token, etc.) can influence its usage. Moreover, users must have appropriate confidence, trust, and control in using the eID [Backhouse, 2005; Krontiris et al., 2011].

eID issuer: Electronic identities can be issued by public authorities or the private sector. In the public sector, eIDs can be issued on national, federal, or regional level. Regardless whether the eID is issued from the public or private sector, they can have the same quality. [Krontiris et al., 2011]

Coverage: According to Krontiris et al. [2011], eIDs can be issued mandatory or optional by voluntary activation. Electronic identities can have full national coverage or can be issued just on demand.

Representation: Electronic representation of natural or legal persons and its modeling in electronic processes is still scarce in Europe [Graux et al., 2009c]. Thus, this is even a greater challenge in a cross-border context [De Cock, 2006].

5.3.3 Legal Challenges

In the following, legal eID interoperability challenges are discussed.

Legal framework: Cross-border acceptance of national eID solution requires a thorough and comprehensive legal framework. According to Majava et al. [2009], this is currently one of the key interoperability issues. Currently, the EU signature directive [European Parliament and Council, 1999b] constitutes the legal basis for eIDs. However, the European Commission is currently working on a new regulation [European Commission, 2012b] that should substitute the signature directive.

Trust: Referring to Majava et al. [2009], across the member states *"there is no consensus or common position on how trust in identity information or identity infrastructure can be established at the cross border level"* [Majava et al., 2009]. The individual member states rely on different credential types, some providing more security (e.g., smart cards) and some providing less security (e.g., username/password schemes). For cross-border eID, a common agreement on mutual acceptance of credentials needs to be achieved. One possibility is the classification of credentials and assigning them to appropriate authentication levels. [Majava et al., 2009; ENISA, 2010; Krontiris et al., 2011]

Unique identification: It must be assured that citizens can be uniquely identified across Europe in electronic processes [Majava et al., 2009]. In addition, there is no common usage of unique identifiers. In some countries, unique identifiers for natural persons are publicly available (e.g., Estonia)

whereas in other countries they require special protection due to data protection regulations (e.g., Austria). [Majava et al., 2009; Hayat et al., 2004]

Amount of information: Individual national eID solutions contain a different amount of identity data stored on the eID. According to Hayat [2007], *“there are no standards that define the minimum or maximum amount of information that an eID may contain about its holder”* [Hayat, 2007]. In addition, there is no standard how identity information is stored on the eID [Hayat, 2007].

5.4 Early Interoperability Approaches

Efforts for bypassing the described challenges are not new within the EU. Based on several initiatives (cf. Section 4.1) the EU stipulated projects to achieve eID interoperability across Europe. In the following, early approaches aiming on eID interoperability across Europe are briefly discussed. A good overview on early eID interoperability initiatives is given in Hayat [2007].

5.4.1 Modinis-IDM

The Modinis-IDM project² (Study on Identity Management in eGovernment) emerged because of the actions proposed with respect to interoperability in the i2010 initiative (cf. 4.1.2.2) and the corresponding action plan. According to the European Commission [2006], the general aim of Modinis-IDM was *“to build on expertise and initiatives in the EU Member States to progress towards a coherent approach in electronic identity management in eGovernment in the European Union”*. The project started in 2005 and ended after a period of 26 month in 2007.

In fact, the following results were achieved within Modinis-IDM [De Cock, 2006]:

- Different country profiles through analysis of national identity management systems.
- Identified barriers to pan-European identity management (technical, organizational, and legal problems).
- A conceptual framework for European identity management systems (cf. [European Commission, 2006]).

Besides analyzing different national eID solutions and identity management use cases, Modinis-IDM additionally proposed a common terminology on eID related terms [Modinis, 2005] and a roadmap for pan-European identity management systems.

5.4.2 FIDIS

FIDIS³ (Future of Identity in the Information Society) was a five year lasting EU-funded research project within the EU's FP6 programme. FIDIS had started in 2004 and finished in 2009. According to FIDIS [2004], the vision of FIDIS was *“develop a deeper understanding of how appropriate identities and identity management can progress the way to a fair(er) European information society”* [FIDIS, 2004]. This vision should be persisted through technology research activities in the fields of identity and identification, interoperability of identity and identification concepts, ID-theft, privacy and security, and profiling and forensic implications [FIDIS, 2004]. Within that, FIDIS published a huge set of deliverables about the interoperability of identities and identity management systems. Sample topics of these deliverables

²<https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome>

³<http://www.fidis.net>

are structured approaches on interoperability, interoperability requirements for identity management systems, or surveys on citizens' trust in identity management systems. The individual deliverables can be downloaded from <http://www.fidis.net>.

5.4.3 Guide

The full title of the Guide project [Stefanova et al., 2005, 2010] is "Creating a European Identity Management Architecture for eGovernment". The consortium that worked on it consisted of 16 commercial and academic partners. The aim of this European Union funded research project was to develop an architecture for eID services and transactions in the field of e-Government. Guide should address the issue of identity theft and trust between public administrations and identity providers, especially crossing member state borders.

When developing a viable identity management solution, it is not enough to concentrate only on technical and technological problems. An eID architecture encompasses also social, political and legal context areas. Due to the heterogeneity of e-Government services and legislation of EU member states, an eID solution must also be flexible. Thus, Guide addressed different member states' requirements and tried to consider changes over time or after critical events. The key goal was the improvement of collaboration between administrative functions at a pan-European level.

Guide demonstrated electronic identity interoperability of cross-border services on two successful trials. The first trial was on the E101 form, which keeps social security information for migrant workers. The trial was tested in Belgium, the Netherlands, and Estonia. The second trial involved electronic procurement in Germany, Spain, and Finland. It demonstrated a solution for cross-border identity confirmation.

Cross-border identity management solutions like Guide are not standalone services for citizens. They actually act as enabler for migrating existing e-Government services developed by individual member states to a pan-European level.

5.4.4 PRIME, PrimeLife

PRIME⁴ (Privacy and Identity Management for Europe) was a research project within the EU's FP6 programme that ended in 2008. PRIME aimed on designing and developing a prototype for a privacy-enhancing identity management system. The work especially focused on the inclusion of privacy-enhancing concepts such as the use of pseudonyms, claims, or private credentials [Camenisch and Lysyanskaya, 2003]. PRIME demonstrated their work in real-world scenarios and different identity management use cases.

PrimeLife⁵ was the successor project of PRIME within the EU's FP7 programme and ended in 2011. Besides addressing the remaining challenges of PRIME, PrimeLife targeted on bringing privacy into the web and on developing tools for integrating privacy in identity management systems. PrimeLife particularly focused on policy languages, web service federations, and privacy-enhancing cryptography.

Although both projects focused on privacy in identity management, they still made valuable research for eID interoperability in Europe.

5.4.5 Smart Card Interoperability

In general, smart cards have emerged to be an appropriate technology for secure identification, authentication, and digital signatures [Arora, 2008a]. All secure cryptographic functions are carried out on the smart card device. To facilitate access to smart card functionality for applications, usually a piece of

⁴<https://www.prime-project.eu>

⁵<http://primelife.ercim.eu>

software is installed in the user's domain. This software (called middleware) encapsulates smart card specifics from the application and provides easy smart card access through a well-defined interface. The Austrian security layer interface [Hollosi et al., 2014] is a typical example.

Supporting different types of smart cards (e.g., from different countries) within a middleware implementation constitutes a first step for achieving interoperability, at least for smart card-based eIDs. In the following subsections different approaches for achieving smart card interoperability of eIDs are briefly elaborated.

5.4.5.1 OpenSC

OpenSC⁶ constitutes an open source library providing and managing access to various smart cards or national ID cards. OpenSC supports – for instance – the Belgium, Estonian, and Portuguese eID smart card implementation. Basically, the general idea of this library is the provision of an abstract layer enabling easy and flexible smart card access for applications, irrespective of the underlying smart card implementation. One use case of the OpenSC library is acting as a so-called middleware, being an intermediary software layer between the smart card and an application. Due to that, applications get the possibility to easily access and use smart card functionality without knowing any card specifics. All card specifics are implemented by the OpenSC library and thus are hidden from the application.

The interface implemented and used by the OpenSC library for smart card access is PC/SC⁷. For communication with applications the standardized PKCS#11 [RSA Laboratories, 2009] interface can be used. This interface is supported by most operating systems and web browsers providing smart card access e.g., for identification or authentication. As an example, the Belgian eID middleware implementation is based on the OpenSC library. However, for achieving eID interoperability the usage of this library limits eIDs to smart card-based approaches only.

5.4.5.2 Austrian Middleware

Tauber et al. [2010] address the issue on interoperability by proposing an identification and authentication solution that supports smart card-based eIDs of different EU member states. Thereby, a service provider is able to identify and authenticate citizens from different EU member states if they use their smart card eID for authentication. The solution actually relies on qualified electronic signatures for authentication and the mutual recognition of qualified certificates.

In more detail, the proposed solution relies on the same middleware architecture as illustrated in Figure 3.14 in Section 3.6.4. However, Tauber et al. [2010] focus on smart card-based implementations only and besides the Austrian eID also smart card-based eIDs of other EU countries are supported. In fact, they enhanced the server-side middleware MOA-ID and the client-side middleware MOCCA to enable authentication at online applications also for foreign eIDs.

In the following, the enhancements of MOA-ID and MOCCA are briefly described.

Enhancement of MOA-ID The Austrian citizen card stores identity data in a special data structure (identity link). However, eID implementations of other EU member states usually store identity information as part of their qualified signature certificate. Hence, instead of reading the identity link, MOA-ID requests the qualified certificate from the client-side middleware to retrieve identity data such as a unique identifier or the citizen's full name. The identification and authentication process steps to be carried out by MOA-ID remain actually the same as in the Austrian case. For the identification process, the only exceptions for foreign eIDs is that the qualified certificate is read instead of the identity link. For the authentication process, no severe changes in MOA-ID were required. Nevertheless, to ensure successful

⁶<https://github.com/OpenSC/OpenSC>

⁷<http://www.pcscworkgroup.com>

signature verification, all root and intermediate certificates of the certification authorities of the various EU member states must be installed in the certificate- and trust-store of MOA-ID in order to be able to build a trusted certificate chain.

Ivkovic and Stranacher [2010] rely on the same approach as Tauber et al. [2010] using client-side and server-side middleware implementations. However, Ivkovic and Stranacher [2010] go a step further as they integrated the complete solution also within the overall Austrian eID concept. Hence, the implementation of Ivkovic and Stranacher [2010] fully complies to the underlying legal framework of the Austrian e-Government Act [Federal Chancellery, 2008] for accepting foreign eIDs in e-Government processes.

Enhancement of MOCCA For the implementation of the client-side middleware, Tauber et al. [2010] rely on the open source and Java Applet-based middleware MOCCA. While the basic functionality of the Java Applet (e.g., implementation of the security layer interface) is provided by MOCCA, still some adaptations were necessary. In particular, the existing card recognition mechanism has been extended. Furthermore, smart card specifics for card communication were implemented for foreign eID cards. This means, the client-middleware has been extended in such a way that it can read identity data and trigger signature creations from several European eID cards.

5.5 Secure Identity Across Borders Linked (STORK)

The various national eID solutions are very heterogeneous across Europe. They differ on technological, operational, and legal level. Due to that, in 2008 the European Commission launched the European large scale pilot (LSP) project STORK⁸ (Secure Identity Across Borders Linked), which involved 18 EU member states. STORK aimed on achieving cross-border eID interoperability between various national eID systems. The project finished at the end of 2011 and successfully demonstrated and piloted cross-border eID federation between the participating countries. By the help of STORK, citizens are able to securely authenticate at online services located in foreign European countries by actually using their own national eID, which has been issued by the citizens' home country. For example, via the STORK framework Austrian citizens are able to authenticate at Spanish governmental online services by using their Austrian eID, namely the Austrian citizen card. STORK is currently heavily pushed by the European Commission and will probably be the relevant eID framework across Europe in future. In the following subsections details on the STORK project and framework are given.

5.5.1 Goals and Challenges of STORK

The general aim of STORK was to achieve cross-border interoperability of secure citizen identification and authentication amongst the participating EU member states. In other words, STORK tackled the gap of a heterogeneous eID landscape across Europe. To achieve that, STORK developed an interoperability layer on top of the existing national solutions to avoid any severe changes in the individual national infrastructures. The basic idea was to gain experience and to see in real production environments, where issues arise or one even might get stuck. In particular, trust framework considerations, security concerns, questions of accountability and liability, data protection or legal issues had to be taken in mind. [Zwattendorfer et al., 2012b, 2013c]

Summarizing, the following goals were addressed by STORK [Leitold and Zwattendorfer, 2011; Koulolias et al., 2011]:

- Mutual recognition of national eIDs within the EU (STORK participating countries)

⁸<https://www.eid-stork.eu>

- Clarifying operational and also – to some extent – legal issues
- Establishment of a common trust model
- Achieving consensus on data protection
- Addressing security and privacy issues

To achieve the proposed goals, in a first phase the STORK consortium agreed on a common eID acceptance framework (see next section on the STORK Quality Authentication Assurance Model). After that, STORK continued to develop common specifications for a cross-border eID interoperability framework. Finally, the last phases included the implementation of the developed specifications and their piloting to demonstrate their applicability in real life applications. [Leitold and Zwattendorfer, 2011]

5.5.2 STORK Quality Authentication Assurance Model

The individual national eID solutions and systems of the participating STORK member states differ on technical, organizational, or legal level. Some countries still rely on simple username/password mechanisms for identification and authentication, whereas others use more sophisticated and secure PKI-based solutions implemented on smart cards or involving citizens' mobile phones. To make the individual national eID solutions comparable, STORK qualitatively modeled the strength of the different authentication mechanisms and quality of eID registration to STORK defined quality authentication assurance (QAA) levels. Thereby, STORK assigned each national eID to one of four QAA classes, giving a service provider equivalence of foreign solutions to national solutions. The STORK QAA levels are similar to levels of assurance (LoA) in other frameworks, such as the LoA from the NIST (National Institute of Standards and Technology) [Burr et al., 2013], from Kantara [Glade, 2009], or from ISO/IEC [ISO/IEC JTC 1, 2012].

STORK has defined four different QAA levels, all reflecting different strength in the citizen registration and authentication process. The four STORK QAA levels are [Hulsebosch et al., 2009]:

- **QAA Level 1:** No or minimal assurance
- **QAA Level 2:** Low assurance
- **QAA Level 3:** Substantial assurance
- **QAA Level 4:** High assurance

The four STORK levels are based on the IDABC study of 2007 [Graux and Majava, 2007]. The use of a STORK level depends on the severity of damage for an identity threat [Hulsebosch et al., 2009]. All national eID solutions that base on the EU signature directive [European Parliament and Council, 1999b] are assigned STORK QAA Level 4 [Krontiris et al., 2011; Hulsebosch et al., 2009].

In general, for determining a STORK QAA Level a series of requirements must be met. In Hulsebosch et al. [2009] the requirements are divided into requirements for the *registration phase* and requirements for the *authentication phase*.

The registration phase involves the following quality factors [Hulsebosch et al., 2009]:

- "Quality of the identification procedure"
- "Quality of the identity issuing process"
- "Quality of the entity issuing the identity credentials"

The "*quality of the identification procedure*" is a measuring factor how a citizen is identified before an authentication credential is issued. This measuring factor – for instance – checks if the citizen is physically present during the identification process or not, or whether the presented attributes are from high quality and can be validated using appropriate means. The factor on determining the "*quality of the identity issuing process*" mainly refers to the quality of the credential delivery process. For instance, credentials can be sent via e-mail link or delivered personally. Finally, "*quality of the entity issuing the identity credentials*" refers to the quality of the entity that issues credentials to the citizen. Entities issuing credentials can have no government agreements in place for lower QAA levels whereas QAA Level 4 requires qualification according to the EU signature directive [European Parliament and Council, 1999b]. [Hulsebosch et al., 2009]

In addition to the registration phase, the authentication phase includes the following quality factors [Hulsebosch et al., 2009]:

- "*Types and robustness of the identity credential*"
- "*Security of the authentication mechanism*"

The first quality factor "*types and robustness of the identity credential*" mainly refers to the different credentials or tokens that can be used for an authentication process. Username/password mechanisms are less robust against security attacks than qualified certificates based on hardware tokens. The second factor "*security of the authentication mechanism*" constitutes the robustness against a specific set of attacks (e.g., man-in-the-middle attacks, replay attacks, etc.) as defined in Hulsebosch et al. [2009]. High secure credentials must be robust against all of these attacks. [Hulsebosch et al., 2009]

Combining the quality of the individual factors results in the final STORK QAA level for a particular identification and authentication mechanism. It is important to mention that the weakest link of the individual quality factors is in fact responsible for defining the overall security and QAA level respectively. I.e., if the quality of the identification procedure is assessed to level 3 but all other factors are assessed to 4, the final and overall quality cannot be higher than 3. More information and more details on the STORK QAA levels can be found in Hulsebosch et al. [2009]; Koulolias et al. [2011]; Körting and Ombelli [2011]; Leitold [2011].

5.5.3 Basic Models

At the beginning of STORK, the participating member states discussed different identity models to be applicable in a cross-border context. In the end, they defined two basic models that are applied in the respective member states and which need to be made interoperable. In the following, the two basic models (proxy model and middleware model) defined within STORK are described on a general and abstract level. The basic models are defined in detail in Eichholz et al. [2010].

5.5.3.1 Proxy Model

Figure 5.1 illustrates the general proxy model. In this scenario, a proxy⁹ acts as intermediary between the service provider and the identity provider. When the user wants to authenticate at the service provider (online application), the user is first forwarded with her authentication request to the proxy. The proxy determines the appropriate identity provider the user can rely on for authentication. Hence, the authentication request is again forwarded by the proxy to the identity provider. At the identity provider, the actual authentication process of the user takes place. After that – assuming that the authentication was successful – user's identity and authentication data are transferred back to the service provider via the proxy. Based on the information received from the proxy the service provider can either grant or deny the

⁹The proxy can also be seen as a broker.

user access to the online application. Since the proxy acts as intermediary between the service provider and the identity provider, the brokered trust model as discussed in Section 3.1.6 applies. All entities are operated in separate domains.

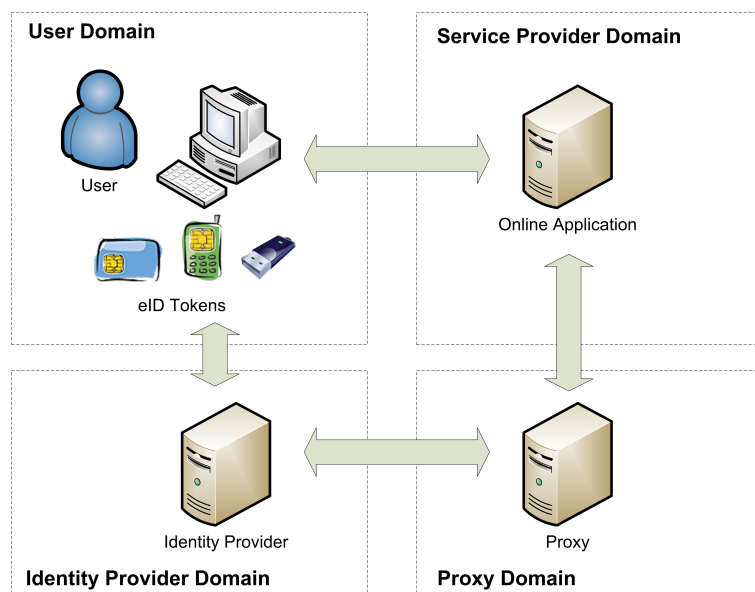


Figure 5.1: Proxy Model

In the context of STORK and thus in cross-border scenarios, the proxy model is called PEPS model (Pan-European Proxy Service). Within STORK the PEPS model is a proxy-based approach with identity intermediaries. A national gateway (the PEPS) serves as single interface to other countries and encapsulates specifics of the national eID infrastructure (i.e., the communication to service providers, identity providers, and/or attribute providers). Additionally, a PEPS implements the protocols and functionality for cross-border authentication. In a cross-border authentication process, the PEPS is an intermediary between the service provider and the actual (foreign) identity provider. The PEPS asserts the service provider that a user has been successfully and properly authenticated by a foreign identity provider. The advantage of this proxy model is that each PEPS only needs to serve its national eID infrastructure and the common STORK protocol [Alcalde-Moraño et al., 2011] for cross-border communication. Thus, in a cross-border scenario specifics of the national eID infrastructure are hidden from other involved entities of other countries. This also hides national or proprietary protocols from other countries, as the PEPS leverages to the common cross-border protocol. [Zwattendorfer et al., 2013c]

5.5.3.2 Middleware (MW) Model

Figure 5.2 illustrates the general middleware (MW) model. The MW model actually consists of two components, the client-side middleware and the server-side middleware. The client-side middleware runs directly in the user's domain. On the one hand, the client-side middleware manages access to the underlying eID token and, on the other hand, it communicates with the server-side middleware. The server-side middleware retrieves eID token specific information from the client-middleware and provides this information in a structured way to the actual online application that requires authentication. In an authentication scenario, the online application triggers the server-side middleware to request authentication. The server-side middleware communicates with the client-side middleware to retrieve user's identity information. After successful retrieval, identity and authentication information are provided by the server-side middleware to the online application. Since the server-side middleware is operated in the service provider's domain and the client-middleware in the user's domain, the online application has more or less a direct communication channel and trust relationship (cf. the direct trust model in Section

3.1.6) with the underlying eID token of the user. This model can also be associated to the user-centric model as classified in Section 3.3.

Giving a concrete example of this model, the Austrian eID architecture follows the MW approach (cf. Figure 3.14 in Section 3.6.4). Thereby, the Austrian citizen card software constitutes the client-middleware and MOA-ID the server-side middleware. In the context of STORK, national server-side middleware implementations such as MOA-ID are called *SPWare*.

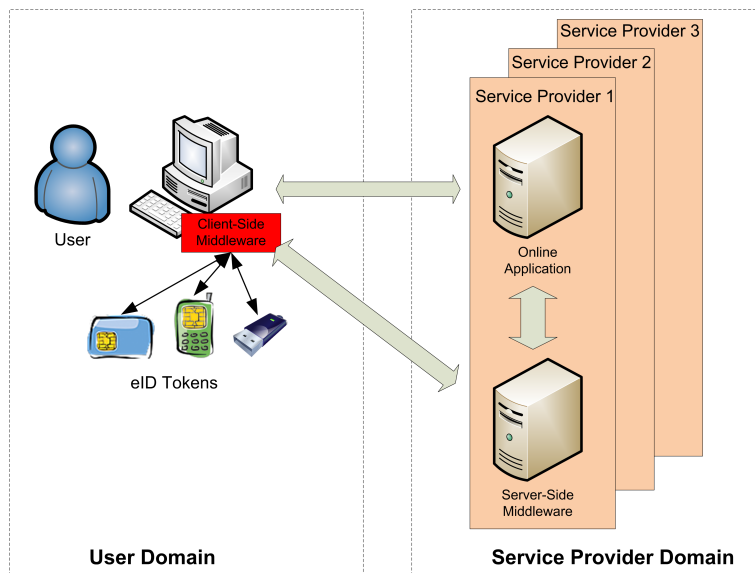


Figure 5.2: Middleware Model

Also in a cross-border MW model users directly authenticate at the service provider. This means that the service provider itself supports all desired identification and authentication methods of the individual member states. For supporting the middleware model for cross-border authentication in STORK, service providers install and deploy the server-side middleware *VIDP* (Virtual Identity Provider), which is operated in the service provider's infrastructure. The VIDP constitutes a common server-side middleware that supports different eID solutions of member states, which rely nationally on the MW approach. More precisely, the VIDP integrates and communicates with different SPWares. Finally, as will be seen in the description of the interoperability models in the next section, the VIDP acts as bridge to interconnect the Proxy model and the MW model in cross-border identification and authentication scenarios.

The MW model particularly preserves privacy because identity data are stored in the user's domain and no intermediaries are involved. Another advantage of this model is end-to-end security, as the user's eID (such as a smart card) can establish a direct communication channel to the service provider. A drawback is, however, that service providers need to integrate the various protocols and eIDs of foreign countries.

5.5.4 Interoperability Models

STORK implemented both models PEPS and MW as well as its combinations, which are called interoperability models. I.e., citizens from MW countries can authenticate at service providers of PEPS countries and vice versa. Combining both models, four scenarios can be distinguished [Eichholz et al., 2010; Zwattendorfer et al., 2012b, 2013c]:

- A citizen from a PEPS country (PEPS infrastructure nationally deployed) wants to securely authenticate at a service provider in another PEPS country.

- A citizen from a MW country (MW infrastructure nationally rolled-out) wants to securely authenticate at a service provider in another MW country.
- A citizen from a PEPS country wants to securely authenticate at a service provider in a MW country.
- A citizen from a MW country wants to securely authenticate at a service provider in a PEPS country.

5.5.4.1 PEPS-PEPS Model

Figure 5.3 illustrates the first interoperability model (cross-border PEPS model) showing, on the one hand, the trust relationships between the participating entities and, on the other hand, the logical authentication process flow. A PEPS can either act as so-called S-PEPS (PEPS in the state of the service provider) or as C-PEPS (PEPS in the state of the citizen). An S-PEPS communicates with the service provider and the corresponding C-PEPS and thus depicts an intermediary between those two entities. In comparison, a C-PEPS receives authentication requests from an S-PEPS and triggers the identification and authentication process at an identity and/or attribute provider.

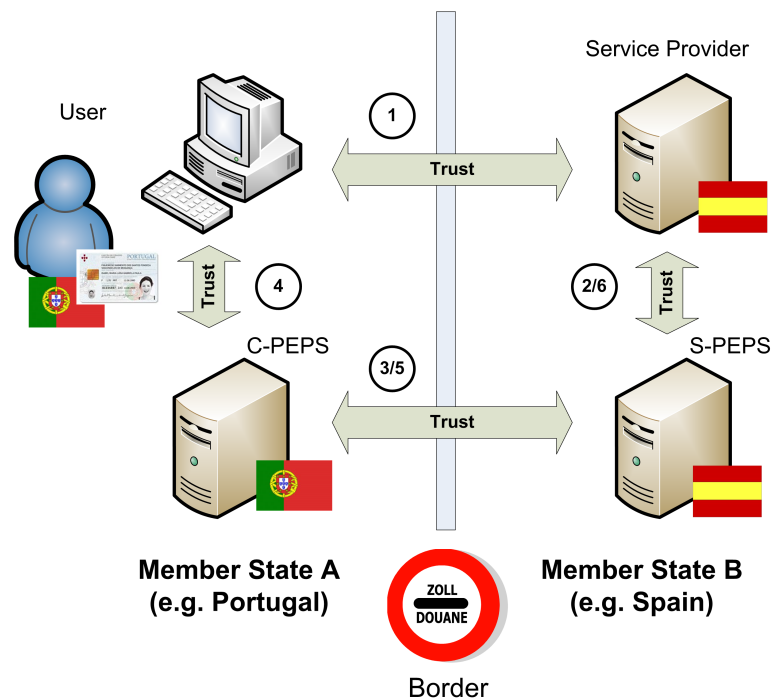


Figure 5.3: PEPS-PEPS Interoperability Model [Zwattendorfer et al., 2013c]

In this sample scenario of Figure 5.3 a Portuguese citizen wants to authenticate at a Spanish service provider. It is assumed that the authentication process is started by accessing a resource at the service provider (Step 1) that requires authentication. The user is redirected to the S-PEPS of the service provider – the Spanish S-PEPS in this example (Step 2). At the S-PEPS, the user gets presented a country selection page. On this page, the user selects the country where she is originally from. This information is necessary to forward the authentication request and the user to her correct national C-PEPS (Step 3). The C-PEPS carries out the actual authentication of the user by contacting connected identity and/or attribute providers. For simplicity, the connected identity and/or attribute providers are not shown in Figure 5.3. For authentication, the citizen uses her national (Portuguese) eID (Step 4). Retrieved identification and authentication data are returned from the C-PEPS to the S-PEPS (Step 5). The S-PEPS in turn forwards these data to the authentication requesting service provider which now can grant or deny access to the

protected resource (Step 6). If the authentication process was successful the Portuguese citizen has authenticated at a Spanish service provider using her own national Portuguese eID token.

During this authentication process, identity data are transferred or routed through several entities. The C-PEPS asserts the S-PEPS and the S-PEPS asserts the service provider that the user has successfully authenticated. Because of this proxied architecture, a segmented trust relationship exists between the user and the service provider. Three point-to-point trust relationships are given: (1) between service provider and S-PEPS; (2) between the identity provider and the C-PEPS; and (3) between the C-PEPS and the S-PEPS. With the segmented (brokered) trust relationships, the intermediaries must be secured properly. This is comparable to securing an identity provider's infrastructure. Note, however, that a C-PEPS may proxy several national identity providers and an S-PEPS several service providers. This highlights the central, and thus security-critical role of a PEPS.

5.5.4.2 MW-MW Model

Figure 5.4 illustrates the STORK interoperability model where both countries rely on the MW approach. In the pure MW model no common national gateway exists. Instead, each service provider installs a server-side middleware module (VIDP) directly in its domain. The VIDP is capable of several national eID token's security functions and manages the identification and authentication process for the service provider.

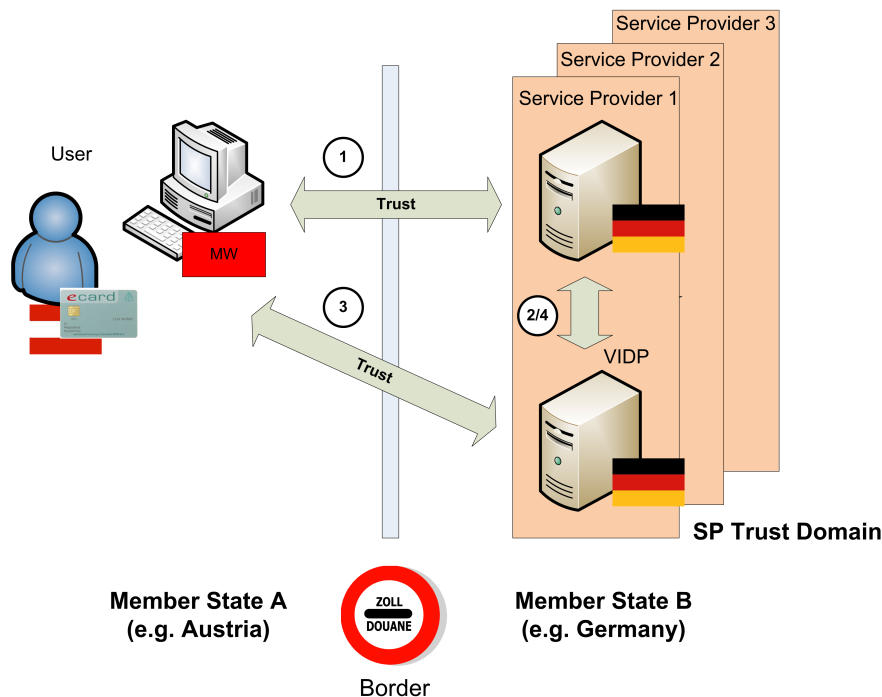


Figure 5.4: MW-MW Interoperability Model [Zwattendorfer et al., 2013c]

In this use case illustrated in Figure 5.4, an Austrian citizen wants to authenticate at a German service provider (Step 1). It is assumed that no security context between the service provider and the citizen has been established before and thus the authentication request is forwarded to the VIDP (Step 2). Based on the citizen's nationality, the VIDP triggers the corresponding national middleware module. In the STORK project as well as in the remainder of this paper the individual national middleware modules are called SPWare modules. For simplicity, the involved national middleware module (SPWare) is not shown in Figure 5.4. The SPWare module directly communicates with the citizen's eID token (Step 3). Received identity and authentication information is returned to the service provider via the VIDP (Step 4).

The foreign citizen is directly authenticated at the service provider via the VIDP and the corresponding SPWare. The VIDP (SPWare) communicates with the citizen's eID token without intermediaries. Both modules are installed and deployed in the service provider's domain, hence no explicit trust relationship between the service provider and the VIDP is required. The only clear trust relationship is given between the user and the service provider. As indicated in Figure 5.4 by three planes, each service provider supporting the MW model operates a VIDP.

5.5.4.3 MW-PEPS Model

Figure 5.5 illustrates the authentication scenario where a user of a PEPS country (Portugal) wants to authenticate at a service provider located in a MW country (Germany). Basically, this scenario shows a combination of the PEPS and the MW model. In the first two steps on delegating the authentication to the VIDP, the authentication process flow is identical as in the pure MW model (Step 1 and 2 – cf. Figure 5.4). However, instead of triggering a national SPWare module the authentication request is forwarded to the C-PEPS of the user's home country (Step 3). The C-PEPS manages the actual authentication process (Step 4) and returns the identification and authentication data to the VIDP and the corresponding service provider (Step 5 and 6).

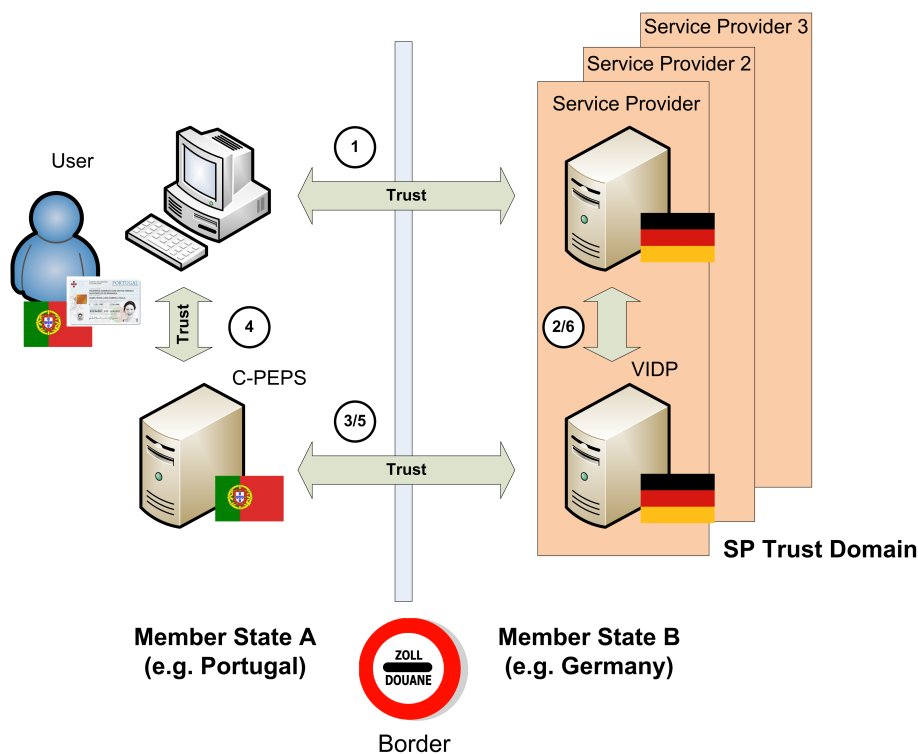


Figure 5.5: MW-PEPS Interoperability Model [Zwattendorfer et al., 2013c]

From the service provider's perspective the C-PEPS is an intermediary. The trust relationships thus are again segmented (brokered). This breaks the end-to-end security paradigm of the pure MW model. A trust relationship between the service provider's VIDP and the C-PEPS, and between the C-PEPS and the user is needed. Again, the VIDP and the service provider are in the same trust domain; hence no explicit trust relationship is necessary here.

5.5.4.4 PEPS-MW Model

Figure 5.6 shows the final combination of the STORK basic models. In this scenario a user of a MW country (Austria) intends to authenticate at a service provider located in a PEPS country (Spain). Steps

1 and 2 on delegating the authentication to the S-PEPS are as in the normal cross-border PEPS model scenario (cf. Figure 5.3). Step 3 is different because a VIDP, which is installed and deployed in the S-PEPS domain, is triggered instead of forwarding the authentication request to a C-PEPS. This VIDP manages the authentication with the citizen's eID token (Step 4). If authentication was successful the VIDP returns the authentication and identity information to the S-PEPS which forwards the data to the service provider (Step 5 and 6).

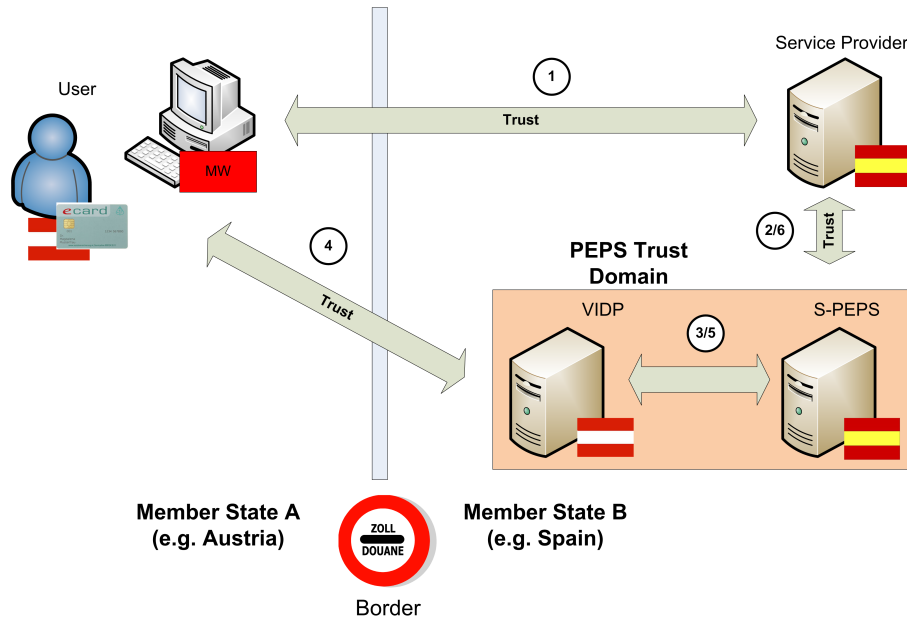


Figure 5.6: PEPS-MW Interoperability Model [Zwattendorfer et al., 2013c]

In this model the S-PEPS acts as a service provider like in the classical MW model. The VIDP is hosted in the PEPS domain and hence no explicit trust relationship between those two entities is required. Similar to the PEPS-PEPS scenario segmented trust relationships exist between the service provider and the user and the service provider and the S-PEPS.

Summarizing, STORK is a framework that consists of two conceptual basic models, middleware and PEPS. Depending on which model countries of the citizen and the service provider opted for, four scenarios exist. In fact, common specifications and protocols have been designed so that STORK is seen as a single framework that supports both central and decentralized deployment. Identity and authentication data exchange is based on the well-known and standardized Security Assertion Markup Language (SAML) (cf. Section 3.5.2). Details on the protocol for cross-border data exchange are given in the STORK interface specification [Alcalde-Moraño et al., 2011].

5.5.5 Architecture and Implementation

Besides the design of a conceptual architecture another aim of the STORK project's common specifications has been the implementation of the interoperability framework. The implemented components are used in the pilots acting as enabler for cross-border identification and authentication. Further and detailed information on the PEPS and MW architecture and its implementation can be found in Berbecaru et al. [2011b]; Alcalde-Moraño et al. [2011]; Berbecaru et al. [2011a]; Sumelong et al. [2011]; Leitold and Zwattendorfer [2011]; Zwattendorfer et al. [2012b, 2013c]; Zwattendorfer and Sumelong [2011]. Emphasis lies on the architecture and implementation of the common middleware component (VIDP) as the author was mainly involved in its design and development process.

5.5.5.1 Pan-European Proxy Service (PEPS) Architecture

Figure 5.7 illustrates the basic architecture of a PEPS server including the functionality for authentication (*AuthenticationPEPS*) and validation (*ValidationPEPS*).

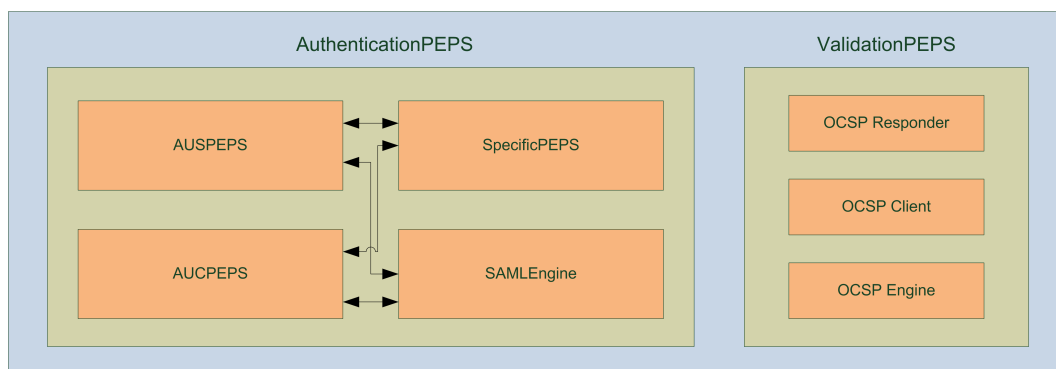


Figure 5.7: PEPS Architecture [Leitold, 2011]

Both functionalities, S-PEPS and C-PEPS, are implemented in the same component. That means, a PEPS can either act as S-PEPS or C-PEPS or can support both functionalities. Details on the PEPS architecture can be found in the respective STORK deliverables [Berbecaru et al., 2011b,a].

Authentication PEPS The *AuthenticationPEPS* consists of four main components – the *AUSPEPS*, the *AUCPEPS*, the *SpecificPEPS*, and the *SAMLEngine*.

The *AUSPEPS* component manages the authentication process between a SP and a S-PEPS. Authentication requests from a service provider are received at this component whereas authentication responses are returned to the calling SP.

The *AUCPEPS* component reflects the inbound functionality of a C-PEPS. Authentication request messages sent from an S-PEPS are received and handled by this component. Furthermore, responses containing either citizen's identity and authentication data or an error message are returned to the requesting S-PEPS.

The *SpecificPEPS* component covers country specific functionality and must be implemented by each PEPS country. The Specific PEPS component is in charge of communicating with national identity providers and attribute providers and the translation of the identity information and national protocol into the common STORK format.

The *SAMLEngine* component encapsulates all SAML related functionality necessary for STORK processing. This engine supports methods for the generation and validation of SAML AuthnRequest and SAML Response messages as well as methods for digitally signing or verifying them.

Validation PEPS The *ValidationPEPS* implements the business logic for digital certificate validation. The main sub-components include an online certificate status protocol (OCSP) engine as well as an OCSP client and responder. The *OCSP Responder* is in charge of handling OCSP requests either sent from an SP or a partner PEPS. Additionally, the responder generates OCSP responses to be returned to the requesting entity. The *OCSP Client* component is responsible for generating OCSP requests for certificate validation to be sent to a partner PEPS. Similar to the *SAMLEngine* component the *OCSP Engine* implements methods for the generation and processing of OCSP request and response messages.

5.5.5.2 Middleware (MW) Architecture

The middleware model represents the decentralized deployment option of STORK. It has merit from an end-to-end security and from a privacy perspective. It however faces the scalability challenge that service providers need to support several (possibly many) foreign eID tokens that can be based on different protocols. This asks for a modular and scalable architecture. This section describes the modular architecture of the VIDP, the main entity of the STORK middleware approach. Details on the MW architecture and its implementation can be found in Berbecaru et al. [2011b]; Sumelong et al. [2011]; Leitold and Zwattendorfer [2011]; Zwattendorfer and Sumelong [2011]; Zwattendorfer et al. [2012b, 2013c].

The MW model has been developed by Austria and Germany – both countries operating their national eID in a MW model: Austria has a national eID solution based on the MW concept and supporting several smart cards and a mobile phone eID in use since 2003 (cf. Section 3.6.2). Germany has set up a MW infrastructure for the so-called "neuer Personalausweis" (nPA) on national level in 2010 (cf. Section 5.1.3).

Figure 5.8 illustrates the common MW architecture. To satisfy modularity and scalability requirements, it consists of a common component that can be extended by plug-ins and plug-ons for the national eID and SPWare protocols.

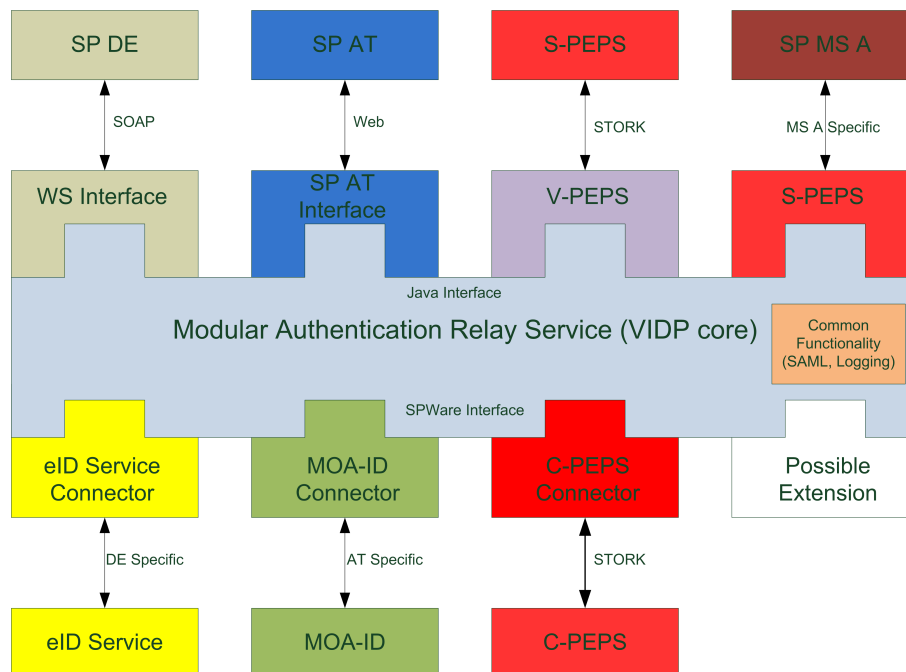


Figure 5.8: MW Architecture [Leitold, 2011]

The common component is the *Modular Authentication Relay Service* (MARS). To integrate new countries' eIDs, two MARS-interfaces need to be implemented: (1) the *Java Interface* and (2) the *SPWare Interface*. Modules implementing the Java Interface handle incoming authentication requests of service providers (SP). These authentication requests are transformed and routed to the desired *SPWare Connectors*. The SPWare Connectors implement the SPWare interface and define connectors to the national MW module (SPWare). Figure 5.8 illustrates the SPWare Connectors to the German MW (eID Service) and the Austrian MW (MOA-ID).

Countries following the PEPS approach are also supported by this architecture. In this case (cf. Figure 3) the so-called *C-PEPS Connector* acts as SPWare Connector, which forwards an authentication request to the respective country PEPS (C-PEPS). Subsequently, the user authenticates at the according national PEPS which in turn wraps the identification and authentication data into a SAML token and returns it to the VIDP. The VIDP verifies the validity of this token and transmits the data through

the respective national interface to the requesting service provider. The protocol for cross-border data exchange is based on the STORK interface specification [Alcalde-Moraño et al., 2011], which is SAML.

The modular approach does not only provide the opportunity to easily integrate other countries' authentication systems but furthermore allows the conversion and restructuring of the VIDP to an entire PEPS. The realization by means of this architecture can simply be achieved by utilizing and invoking the modules S-PEPS and C-PEPS Connector together.

The implementation of this architecture contains the following components:

- *WS Interface*: This SOAP-based interface is used for receiving authentication requests sent by German service providers. German service providers send authentication requests to the VIDP and receive responses including identity and authentication data via this web service interface.
- *SP AT Interface*: This interface is web-based and supports authentication requests of Austrian service providers. They can use this interface for providing foreign eID access to legacy applications.
- *V-PEPS*: Via this interface the VIDP receives STORK authentication request messages from an S-PEPS. STORK authentication response message also pass this interface. In particular, this interface is involved in the cross-border PEPS-MW scenario (cf. Figure 5.6).
- *eID Service Connector*: This connector is responsible for the communication between the VIDP and the German eID service. The German eID service constitutes the national German MW solution (SPWare).
- *MOA-ID Connector*: This connector forwards and transforms an authentication request to the Austrian national middleware MOA-ID (SPWare). Authentication responses from MOA-ID are also managed by this connector.
- *C-PEPS Connector*: The C-PEPS connector is the endpoint of the VIDP for outgoing and incoming messages to and from a C-PEPS. By the help of this connector, users originating from a PEPS country get the ability to authenticate at service providers supporting the MW model (MW-PEPS scenario – cf. Figure 5.5).

Implementation of the MW Architecture This subsection describes the actual implementation of the STORK middleware. To guarantee high flexibility and dynamics for the implementation, EJBs¹⁰ (Enterprise Java Beans) web services technologies had been chosen. Additionally, smooth interfaces were defined to allow flexibility for decoupling individual modules and dynamic deployment. Hence, adding or removing of modules during runtime does not negatively impact the system.

Figure 5.9 illustrates the component diagram of the implemented middleware architecture. To achieve great dynamism and flexibility, the implementation has been split into three separate deployable modules:

- VIDP-Services
- VIDP-SPWare
- VIDP

The *VIDP-Services* module is responsible for general or support tasks e.g., managing authentication sessions (*SessionManager*) or handling the communication with the external database (*PersistenceService*). The database holds all required configuration information for the individual modules and components.

¹⁰<http://www.oracle.com/technetwork/java/index-jsp-140203.html>

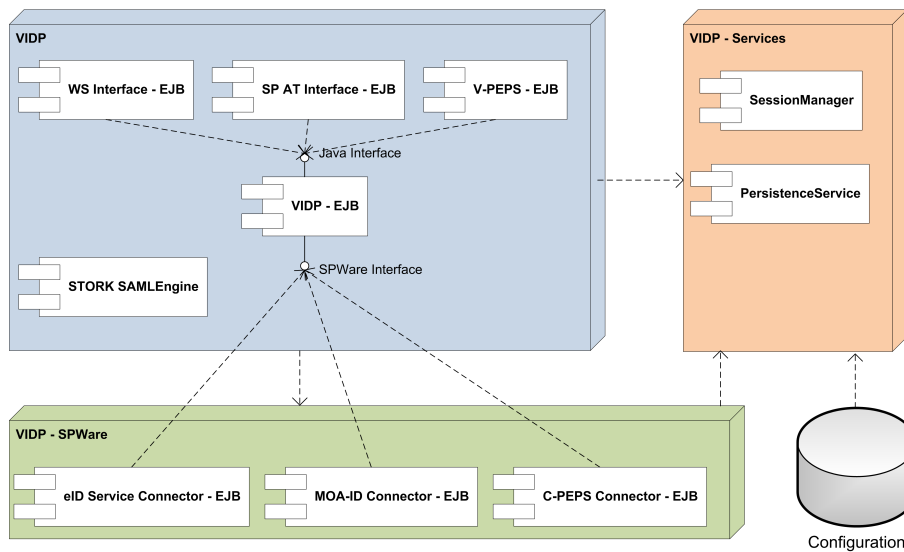


Figure 5.9: Component Diagram of the STORK Middleware [Zwattendorfer et al., 2013c]

The *VIDP-SPWare* module contains the country-specific *SPWare* Connector components (*eID Service Connector* and *MOA-ID Connector*). These connectors handle the communication with the national MW module (*SPWare*). The *C-PEPS Connector* component constitutes a special component as it manages the communication with foreign *C-PEPS*s if a particular country relies on the *PEPS* and not the MW model. All connectors are modeled as *EJB*s. For configurations, the *VIDP-SPWare* module accesses the *VIDP-Services* module.

The *VIDP* module constitutes the main module of the MW implementation. The routing functionality is implemented in the *VIDP-EJB* component. The service provider specific authentication interfaces are also modeled as *EJB* components (*WS Interface*, *SP AT Interface*, and *V-PEPS*). The national MW connector modules (*SPWare* Connectors) are included in the *VIDP-SPWare* module and thus the *VIDP* only connects to them. The separate *STORK SAMLEngine* component handles all tasks relating to the common *STORK* interface protocol which is based on *SAML*. Again, for configurations also the *VIDP* module relies on the *VIDP-Services* module.

Because of the separation of the *VIDP* functionality into different modules, also different deployment options exist.

Deployment Options The middleware implementation shown in Figure 5.9 allows a flexible arrangement of the modules for deployment. Depending on availability of resources or other desired properties such as flexibility or maintenance efforts, different deployment strategies can be chosen. Moreover, static or dynamic extensibility of the *VIDP* is supported. In this context, the term dynamic means that modules (e.g., *C-PEPS Connector*, *VIDP-SPWare*, etc.) can easily be added or removed during runtime without negatively influencing the complete *VIDP* operation.

The following deployment opportunities are supported:

- Coupled Deployment
- Loose Deployment

When choosing a coupled deployment, all *VIDP* modules (*VIDP-Services*, *VIDP-SPWare*, *VIDP*) are deployed on a common server instance. The advantage of this approach is that all modules reside on the same machine which gives less maintenance effort but less flexibility and performance.

Within a loose deployment model, the VIDP modules such as VIDP-Services or VIDP-SPWare can be deployed individually as single and distributed instances. This increases flexibility in case of performance and scalability bottlenecks. Nevertheless, the distribution of components raises the risk that components may be inaccessible because of network errors or shutdowns [Paal et al., 2003].

To support this diversity of flexible and scalable deployment approaches, APIs based on the J2EE-Interfaces *Local*, *Remote* and *Web Services* (SOAP) for the individual modules had been defined. The transition from one interface to another one (e.g., from *Remote* to *Web Services*) can easily and dynamically be carried out during runtime without interfering the operation of the respective module.

Security Discussion Security plays a major role in the STORK context as well as in its framework implementations. Personal data of EU citizens are transmitted across borders, are processed, and are temporarily stored. These personal data define valuable assets, which must be protected. STORK had a dedicated security team that defined security requirements and principles [Stern, 2011]. These have as well been implemented by the VIDP. The security principles follow a *threat – objective – security function* approach: A *threat* analysis has been carried out. Threats include impersonation or a possible loss of confidentiality, integrity, or availability of personal data identified. These threats lead to security *objectives* that need to be met by security functions. These *security functions* must be implemented by the individual STORK components or modules. A selection of these security functions and their implementation in the VIDP are described in the next subsections.

The interfaces between entities or components define the critical parts where impersonation or a loss of security can occur. Figure 5.10 illustrates the critical interfaces of the VIDP which must be especially protected.

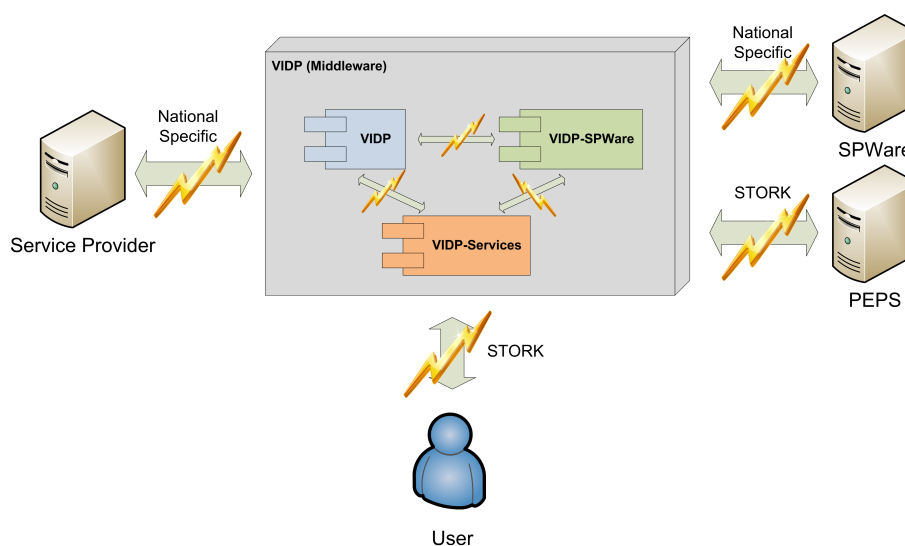


Figure 5.10: VIDP Critical Interfaces [Zwattendorfer et al., 2013c]

Critical interfaces can be identified internally and externally to the VIDP. The protection of internal interfaces is especially important if a loose deployment option is preferred, where the VIDP implementation components (VIDP-Services, VIDP-SPWare, VIDP) are distributed. The external interfaces must be protected in every situation where an external entity of the VIDP (e.g., service provider or PEPS) is involved. In other words, whenever personal data leave the VIDP and are transferred to another entity the data must appropriately be protected. In the following it is described how these external and internal interfaces were secured [Zwattendorfer et al., 2013c].

VIDP External Interfaces:

In the following the critical external interfaces of the VIDP are identified and it is shown how the predefined security requirements of STORK were met.

SP \Leftrightarrow VIDP Interface: Via this interface data are transferred between a national service provider and the VIDP. In the MW model, the general idea is that the VIDP is directly installed in the SP domain to enable end-to-end security between the user and the service provider. Thus, there are no further security requirements that must be fulfilled for the VIDP except for the SP itself. In fact, the VIDP can be seen as being a part of the SP. However, the SP has to ensure that the internal SP \Leftrightarrow VIDP connection is secured properly.

In case this SP \Leftrightarrow VIDP interface is externalized, the VIDP needs to support the security functions of the national specific service provider interface and its protocol. The current VIDP implementation supports national SP interfaces of Austria and Germany. The connection between an Austrian SP interface and the VIDP is secured by the use of TLS/SSL certificates. The German SP interface is web service-based and requires a mutually secured and authenticated TLS communication channel.

VIDP \Leftrightarrow SPWare Interface: Identification and authentication data are exchanged between the VIDP and the national MW module (SPWare) through this interface. According to the main idea of the MW model, all supported national MW modules are installed close to the VIDP within the SP domain. Hence, this interface can be assumed as SP internal interface which does not require higher protection than the SP domain itself. However, in case of externalization of this interface (as illustrated in Figure 5.10) the data passing through must be appropriately protected. Similar to the SP \Leftrightarrow VIDP interface, the current VIDP implementation supports connections to the Austrian and German national MW module. Both countries rely on a mutually authenticated TLS communication channel for data transfer between the VIDP and the SPWare.

VIDP \Leftrightarrow PEPS Interface: This interface implemented by the VIDP relies on the common STORK interface specification and its protocol [Alcalde-Moraño et al., 2011]. The common STORK protocol is used for the secure data transfer between a VIDP and a PEPS. Since this protocol bases on SAML 2.0 also all security related functionality is aligned to this well-established standard. In particular, for data transfer between STORK entities the SAML Web SSO Profile [Hughes et al., 2009] with the HTTP Post Binding [Cantor et al., 2009a] is used. Thereby, all in- and outgoing messages must be properly digitally signed using the XML-Dsig syntax [Bartel et al., 2008]. Digital signatures ensure message integrity, non-repudiation, and authenticity. Authenticity can be guaranteed because only digital certificates issued for STORK entities are trusted.

To further improve security, the STORK specification allows to encrypt parts (especially user data) of the transmitted messages. For encrypting such parts, the XML Encryption syntax [Imamura et al., 2002] can be used. In addition, instead of the SAML Web SSO Profile the SAML Holder-of-Key (HoK) Profile [Lockhart and Hardjono, 2010] may be used. This profile ensures a stronger authentication and security context between the identifying and authenticating provider, the service provider, and the user's client. This higher strength is based on client's presentation of the same X.509 certificate, which results from the TLS handshake, to both providers. However, the HoK Profile is currently not widely adopted in standard components e.g., web browsers.

VIDP \Leftrightarrow User Interface: Through this interface required interactions between the user and the VIDP are handled. The user accesses this interface by a standard web browser. To guarantee a high level of security, all connections to the VIDP are secured by the use of TLS/SSL. Users are able to verify the authenticity of the VIDP by checking the corresponding X.509 certificate.

In general, users are not required to enter any data into a web page or form presented by the VIDP. However, all input messages or input data are validated by the VIDP against syntax, range,

length, etc. to prevent e.g., cross-site scripting attacks. Additionally, during the implementation and testing phase the developers considered several web application security issues, especially the ones presented by the OWASP¹¹.

VIDP Internal Interfaces:

The VIDP internal interfaces constitute those interfaces between the three VIDP implementation components (VIDP-Services, VIDP-SPWare, VIDP). For the VIDP internal interfaces security issues only come into play if a loose deployment option for the VIDP is chosen. In this deployment option, the VIDP implementation components can be deployed remotely and distributed for achieving higher flexibility and scalability.

For implementing the VIDP, EJB technology has been chosen. This shifts application security aspects to the server implementation hosting the VIDP [Roman et al., 2005]. This simplification holds especially for a coupled deployment of the VIDP individual components, but it cannot be relied on when applying a distributed (loose) deployment model. To achieve the same level of security independent of the deployment option, so-called security gateways were implemented protecting the remote communication between the three VIDP implementation components.

Those security gateways are modular available and are responsible and were especially designed for supporting individual security functions such as authentication and authorization, signature or encryption services, or preventing denial-of-service (DOS) attacks. Authentication between components is based on mutual SSL/TLS authentication. For authorization between the individual components the well-known Role Based Access Control (RBAC) models [Sandhu and Samarati, 1994] and Attribute Based Access Control (ABAC) models [Yuan and Tong, 2005] are supported. Again, for signature and encryption functionality the XML-Dsig and the XML-Enc standard had been chosen. The DOS protection security gateway only allows a maximum number of requests to a VIDP implementation component during a certain time frame. In addition to these security service gateways, gateways supporting supplementary functionality such as XML schema validation or message logging for auditing purposes were implemented.

Privacy Discussion Most of the data processed within the STORK environment are personal data according to the EU data protection directive [European Parliament and Council, 1995]. This section discusses some fundamental privacy principles and furthermore how these were tackled by the VIDP implementation. The following privacy-preserving principles were considered [Zwattendorfer et al., 2013c]:

- Exchange of national identifiers
- Minimum disclosure principle for personal attributes
- User-centricity
- Data unlinkability

Article 8 (7) of the data protection directive states that "*Member States shall determine the conditions under which a national identification number [...] may be processed*" [European Parliament and Council, 1995]. This article has been implemented individually by each EU Member State into national law. What several implementations of the directive have in common is that the use of unique identifiers is restricted. A consequence is that cross-border use is not possible in many cases. To overcome that situation, the STORK framework and its implementation supports the calculation of transient identifiers. Such transient identifiers can be generated using one-way hash algorithms (e.g., the SHA family [Gallagher,

¹¹https://www.owasp.org/index.php/Top_10_2010-Main

2012]) by deriving the unique identifier for a specific country, specific sector, or specific application. Such calculations are also supported by the VIDP implementation. In fact, context-specific identifiers are a core privacy function of both the Austrian and the German eID system – the supporters of the MW model.

The minimum disclosure principle specifies that only a relevant amount of personal data must be processed. Article 6 (1) (c) of the EU data protection directive states that personal data must be *“equated, relevant and not excessive in relation to the purposes for which they are collected and/or further processed”* [European Parliament and Council, 1995]. STORK follows this principle and only allows the transfer of data which are really required. Service providers can request mandatory or optional attributes and users can allow or deny the personal attribute transfer.

User-centricity within the STORK context means that users can always control how their personal data are obtained and how the data are transferred. This requirement is fulfilled by asking the user’s consent for data transfer and data processing. Consenting defines a fundamental requirement of the EU data protection directive and is stipulated in Article 7 (a). For the VIDP, the process of consenting is actually individually implemented by each national MW module.

Unlinkability refers to a property that data shall not be shared unless the user consents or such sharing is legitimate. It defines one major privacy principle within STORK. Data linkage or even profiling of users mostly takes place if central services are involved. Since there does not exist a central instance of the VIDP this privacy requirement can be easily fulfilled by the MW model. Context-specific identifiers that are specific for a service provider prevent from linking to a user’s account at other service providers.

Focus of these security and privacy discussions was put on the MW model and the VIDP implementation because the author was mainly responsible for the design and development of this component. Further and more general information on STORK security and privacy also including the PEPS model can be found in Koulolias et al. [2011].

5.5.6 Integration of STORK in Austria

Based on the work of Tauber et al. [2012] this subsection describes the challenges as well as implementation and integration considerations of the Austrian eID concept into the STORK architecture. As the Austrian eID infrastructure relies on the middleware approach because of liability and privacy reasons, the focus is on the middleware model in the remainder of this section.

Although the STORK framework already provided interfaces for the integration of the national infrastructure, there were still a lot of challenges that had to be overcome on technical, legal, and organizational level. During integration of STORK functionality into the Austrian eID infrastructure, two different use cases had to be considered. The first use case covers the identification and authentication of Austrian citizens in foreign member states, while the second use case concerns the acceptance of foreign citizens at Austrian online applications. On a technical level, for both use cases the approved Austrian eID module MOA-ID, which has been introduced in Section 3.6.3, built the fundamental technical basis. This module was further enhanced to meet the requirements for achieving cross-border interoperability for the Austrian eID concept.

The main challenges that had to be faced during the integration of the Austrian eID concept were as follows [Tauber et al., 2012]:

- Technical integration of the Austrian eID concept into the STORK framework
- Mapping between national and common STORK attributes
- Treatment of electronic identifiers
- Authentication Levels

- Privacy Preservation
- User Consent
- Legacy Support

The next two subsections describe in more detail how these challenges were met, distinguishing between the two different use cases on user identification and authentication.

5.5.6.1 Authentication of Austrian Citizens in Foreign Member States

The Austrian eID concept follows a middleware approach. Hence, for this use case the STORK interoperability framework foresees the installation and deployment of a common server-side middleware (VIDP) in the foreign country. Depending on the national interoperability model to be used the VIDP is either directly installed in the service provider domain (if the MW approach is followed – cf. Section 5.5.4.2) or in the PEPS domain (if the foreign country relies on the PEPS approach – cf. Section 5.5.4.4). However, in both scenarios the VIDP is responsible for the communication with the Austrian eID modules and manages the integration of the Austrian national eID solution.

In general, the VIDP defines a server-side middleware solution developed together by Austria and Germany [Zwattendorfer et al., 2012b]. The VIDP is set up on a modular architecture and defines lightweight interfaces for easy integration of national eID modules. Austria has implemented these interfaces by connecting the VIDP to the Austrian open-source middleware module MOA-ID. In this case, core components of MOA-ID remained unchanged while only the interfaces to the VIDP needed to be implemented. On the one hand, the implementation of these interfaces triggers the authentication process with MOA-ID and, on the other hand, receives the identification and authentication data from this Austrian module after successful authentication.

Figure 5.11 illustrates the sample scenario of authenticating an Austrian citizen (middleware country) at a service provider in a foreign country such as Spain (PEPS country). In this example, an Austrian citizen wants to access a protected resource at a Spanish service provider. It is assumed that the user has not been authenticated before and thus is redirected to the corresponding national Spanish S-PEPS. After providing information on the respective home country, the user is redirected to the installed VIDP as Austria follows the MW approach. The VIDP is responsible for triggering the authentication process at MOA-ID and the user runs through the same authentication process as used when authenticating at Austrian service providers. After having received the identity and authentication information from MOA-ID, the VIDP returns this information back to the requesting S-PEPS and service provider respectively.

Moreover, after having received the data from MOA-ID, the VIDP is responsible for mapping the national Austrian eID attributes (national identifier, first and last name, date of birth) to the according STORK attributes. The exact mapping has been already specified in the design phase. However, as STORK follows the minimal data disclosure principal according to the European data protection directive [European Parliament and Council, 1995], only requested attributes are transmitted. Although a user may have consented to the transmission of all her identity data, only required attributes are transferred to the requesting service provider by the VIDP. At this point it is important to mention that the user gives her consent for the transmission of identity attributes by providing a qualified digital signature. This behavior is completely equal to a traditional authentication process when authenticating at an Austrian service provider (cf. Section 3.6.4).

A special attribute acts as the user's national electronic identifier which allows unique identification of Austrian citizens in foreign countries. As described in Section 3.6.1, each Austrian citizen is assigned a unique identification number (sourcePIN) which is stored on the Austrian citizen card. Preserving privacy equally to the domestic Austrian requirements also across borders, this unique identifier must not be transferred to service providers of foreign countries. Therefore, MOA-ID can be configured in

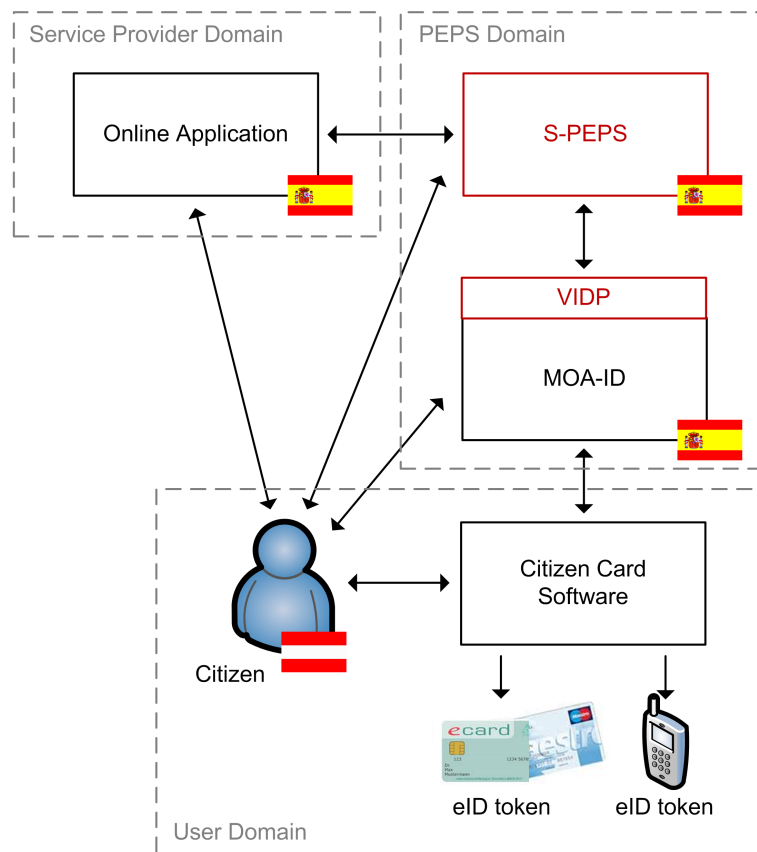


Figure 5.11: Authentication of Austrian citizens in foreign member states [Tauber et al., 2012]

such a way that the unique identifier is specifically derived for one single country only by using one-way hash functions. This derived identifier remains unique per country and can be further derived or used regarding the needs and requirements of the destination country. Within the European Union there are no common legal agreements or regulations on how citizen identifiers are treated in a cross-border context. STORK tried to take up this gap and had defined ways and possibilities on how identifiers are used in cross-border scenarios. However, although STORK had provided common recommendations on identifier treatment and usage, the national regulations are so heterogeneous that it was decided to leave the responsibility of identifier usage to each member state.

Another challenge STORK had to tackle was the quantification of the various existing national authentication possibilities. Therefore, STORK defined four different authentication levels to get a common understanding on security for the various authentication mechanisms used across countries (cf. Section 5.5.2). The Austrian eID concept is based on qualified electronic signatures and thus allows secure and reliable authentication with the highest authentication level of four in the STORK context.

5.5.6.2 Acceptance of Foreign Citizens in Austria

The acceptance of foreign citizens at online applications using an enhanced Austrian eID framework defines the second relevant cross-border use case. Austria was the only country out of the 18 member states participating in STORK that has a nation-wide legal basis for the acceptance of foreign citizens at domestic governmental applications. Correct interpretation and implementation of these legal requirements is the main challenge to bear in mind when technically implementing the communication with the STORK framework on a national level.

Since the Austrian eID concept is based on qualified electronic signatures, for identification and authentication of foreign citizens the same level of security is required for granting foreigners access

to domestic applications. To achieve this, the create-signature functionality of the STORK protocol [Alcalde-Moraño et al., 2011] is used. By using this functionality, foreign users are requested to give their consent for accessing an online application by creating a qualified electronic signature. Taking the MW-PEPS interoperability model (cf. Section 5.5.4.3) as an example, the VIDP located in the service provider environment initiates the signature-creation process within the authentication request being sent to the desired C-PEPS. The C-PEPS is responsible for users' signature creation and further returns the created signature to the requesting service provider or VIDP respectively.

In this scenario, the VIDP constitutes the module MOA-ID enhanced by STORK functionality. This enhancement includes the implementation of the STORK protocol as well as specifics for foreign citizen treatment according to the Austrian E-Government equivalence decree [Federal Chancellery, 2010d]. According to this decree, European citizens can be equally treated as Austrian citizens in governmental as well as commercial online processes. To achieve this, foreign citizens must be registered in the Austrian supplementary register as described in Section 3.6.1. The registration is based on foreign citizens' consent expressed by a qualified electronic signature. The identity data to be used for registration covers the foreign unique identifier, first and last name of the citizen, and the date of birth if present in the citizen's qualified certificate. Details on the registration process in the supplementary register can be found in Ivkovic and Stranacher [2010]. However, in order to protect privacy, not the foreign unique identifier itself is stored, but a special derivation of it. Due to that, foreign users experience the same privacy protection as Austrian citizens. Even if foreign citizens want to access certain services of different sectors, the unique identifier stored in the supplementary register is uniquely derived for every target sector as it is currently done for all Austrian citizens using the sector-specific model (cf. Section 3.6.1).

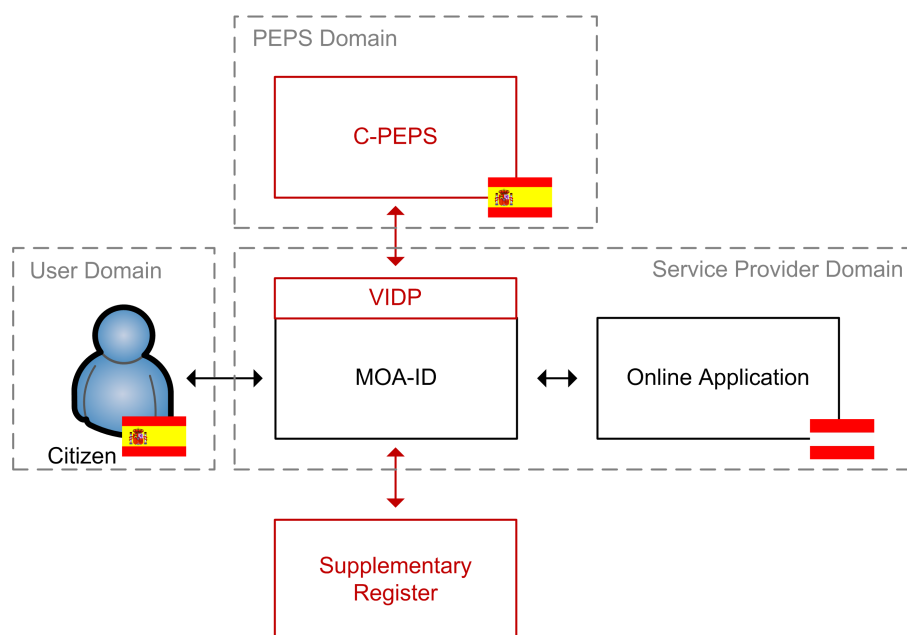


Figure 5.12: Acceptance of foreign citizens in Austria [Tauber et al., 2012]

Figure 5.12 illustrates the implemented architecture for accessing the STORK framework in Austria. In this sample scenario, a Spanish citizen wants to access certain protected resources at an Austrian service provider. The online application of the service provider is protected by the STORK-enabled version of MOA-ID (VIDP), which enables cross-border authentication. In this example, via a country selection template, the user can select her original nationality and hence is redirected through the enhanced MOA-ID module to the Spanish C-PEPS. The authentication request also contains a signature creation request as Austrian governmental service providers require a qualified signature for authentication. The Spanish C-PEPS manages the complete authentication and identification process. There may be other national specific services involved in this process but these details have been omitted for the sake of clar-

ity. However, the C-PEPS is also responsible for creating a qualified electronic signature of the citizen. If successfully authenticated, the C-PEPS transmits a message including identification, authentication, as well as citizen signature data back to the requesting VIDP. The VIDP verifies this message and registers the foreign user in the supplementary register based on the data received. The registration takes place completely on the fly, no further user interaction is required. If the user has successfully been registered, identification and authentication data are transferred to the online application and access to the protected resource is granted.

To support foreign citizen identification and authentication, MOA-ID was amended by the integration of connectors to the STORK framework. However, STORK also defines its own communication possibilities for service providers to start an authentication process. One main requirement before enhancing the MOA-ID module was the support for legacy applications. Therefore, MOA-ID implements a mapping between the national authentication protocol and the STORK protocol. Due to that, existing applications can remain untouched but still can experience the features of cross-border authentication possibilities.

A simplified process flow of this authentication process has already been described in Section 3.6.6. A detailed sequence diagram of this authentication scenario is given in Sumelong et al. [2011].

5.5.7 Pilot Applications

Besides the design and the development of an eID interoperability framework, STORK aimed on demonstrating its results in real world applications. Therefore, STORK deployed and integrated the resulting software components in running applications to show their applicability in cross-border scenarios. In the final phase of the project, STORK evaluated the results in six pilot applications for approximately 1.5 years. In the following, a few details on the individual pilot applications and their goals are given. Details on the individual pilots can be found in Leitold and Zwattendorfer [2011]; Krontiris et al. [2011].

Cross-border authentication platform for electronic services: According to Leitold and Zwattendorfer [2011], the aim of this pilot was the integration of the STORK framework into different national e-Government portals. Thereby, citizens should be able to authenticate at various portals using their own eID. The participating portals range from huge national e-Government portals to regional and sector-specific portals. In Austria, the *help.gv.at* portal took part in this pilot. [Leitold and Zwattendorfer, 2011]

Safer Chat: In this pilot, unique identification was less important [Krontiris et al., 2011]. Moreover, the aim was to allow pupils and students secure authentication based on an age range. For instance, pupils were only allowed to enter piloted chat rooms if they were aged between 14 and 16. No further information was transmitted to the chat application (e.g., the real age or the date of birth), just the boolean information whether the authenticated person fits into the requested age range or not. On the one hand, this ensured privacy of the participating pupils and, on the other hand, only persons of the same age were able to safely communicate with each other [Krontiris et al., 2011]. More information on this pilot and in particular how the STORK framework was integrated into the chat applications is described in Knall et al. [2011].

Student mobility: The aim of this pilot was to facilitate student mobility across the EU based on eID authentication. Since many universities already have some information management system deployed, the goal of this pilot was the integration of the STORK framework into such systems. By the help of the STORK framework, foreign students should be able to enroll already from abroad using their eID. In Austria, the information management portal of the University of Technology in Graz (*TUGraz Online*)¹² participated in this pilot. The integration of the STORK framework into an Italian student portal is described in Berbecaru et al. [2011c].

¹²<https://online.tugraz.at>

Electronic delivery: Electronic delivery focuses on the reliable and secure transfer of electronic data between entities. One aim of this pilot was to integrate the STORK framework into national e-Delivery service applications. Thus, EU citizens are able to authenticate at various national e-Delivery service applications using their eID issued from their home country. As a further aim, in this pilot it was tried to setup an interoperable cross-border electronic delivery framework relying on the properties of certified mail. To achieve this, similar to the PEPS model, STORK followed a gateway approach, where the gateways hide the national specifics of e-Delivery solutions and the gateways communicate with each other using a common protocol. General information on cross-border e-Delivery can be found in Tauber [2012]. Further information with respect to the STORK pilot is given in Tauber et al. [2011d].

Change of address: The aim of this pilot was to facilitate the movement of natural persons across borders. To achieve this, STORK piloted the transfer of attributes – in particular address attributes – between cross-border e-Government applications [Krontiris et al., 2011]. Based on that, required address changes during movements were facilitated.

ECAS integration: ECAS (European Commission Authentication Service) is a central authentication platform for European Commission services and applications. The aim of this pilot was the integration of the STORK framework into the ECAS platform. Hence, by now it is possible to use various national eIDs for authentication at European Commission services and applications.

5.5.8 Cross-Border Legal Identity Management

The main focus of STORK lay on secure cross-border identification and authentication of natural persons only. However, many e-Government transactions are conducted by legal persons or professional representatives. Electronic mandates are one example to model the empowerment between a natural person and another natural or legal person. According to Graux et al. [2009c], electronic mandate solutions modeling representation are still rare across Europe. By the time of this report (2009), only “[...] *only two countries have implemented systems of mandate/authorisation management [...]*” [Graux et al., 2009c]. These countries were Belgium and Austria. In the meantime, also the Netherlands introduced an approach to model empowerment and representation [Zwattendorfer et al., 2012c].

Nevertheless, while some countries already have solutions for legal identity management nationally in place, the identification and authentication of legal persons is still unresolved in a cross-border context. In the following, two approaches for achieving cross-border legal identity management are described. The first approach of Zwattendorfer et al. [2012c] builds upon the STORK framework for natural persons developed in the STORK project. Thereby, just one interoperability model (the PEPS-MW model as described in Section 5.5.4.4) was enhanced to support also cross-border identification and authentication of legal persons. The second approach briefly describes STORK 2.0, the successor project of STORK which particularly aims on the cross-border acceptance of legal persons. In STORK 2.0, all interoperability models support legal person identification and authentication in a cross-border context.

5.5.8.1 Early Approach

Most electronic representation systems are usually tailored to satisfy domestic and national requirements only. Currently, there exists a gap of cross-border applicability of various heterogeneous legal person or representation systems. To bypass this gap, Zwattendorfer et al. [2012c] took up the STORK interoperability framework to demonstrate cross-border identification and authentication of legal persons since issues for transferring data of natural or legal persons across borders are similar. To show the feasibility of their solution, Zwattendorfer et al. [2012c] selected one out of the four STORK interoperability scenarios to demonstrate the cross-border transfer of legal person attributes. Therefore, Zwattendorfer et

al. [2012c] set up the STORK infrastructure and connected it to the Austrian national mandate management system (as additional attribute provider) within a laboratory environment. For the demonstration, Zwattendorfer et al. [2012c] took the PEPS-MW model (cf. Section 5.5.4.4) as a basis and coupled the middleware (VIDP) with this additional attribute provider responsible for national legal person identification. In the proposed scenario, legal person identification is based on the name of the legal person and its register number e.g., the company name and company number. Figure 5.13 illustrates the rough and extended architecture of this set up.

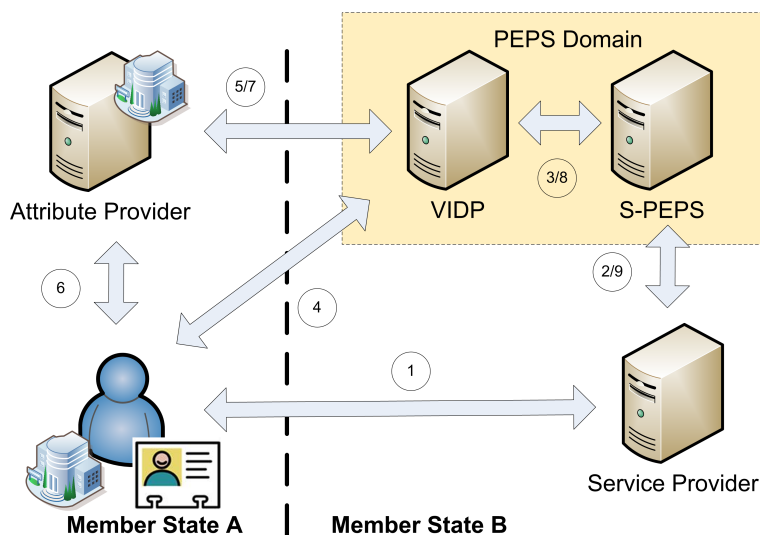


Figure 5.13: PEPS-MW Model including legal identity representation [Zwattendorfer et al., 2012c]

In this proposed scenario, a citizen originating from the middleware member state A wants to access a service provider of the PEPS in member state B (Step 1). In contrast to the normal STORK scenario shown and described in Figure 5.6, in this case the citizen wants to authenticate and act on behalf of a legal person, e.g., a company, at the service provider. Equally to the normal use case for natural person authentication, after accessing the service provider, the citizen is forwarded to the national S-PEPS (Step 2). However, before being redirected to the S-PEPS the citizen needs to state that she wants to be authenticated as representative for a legal person. This statement can be easily achieved by a simple check box or selection box. By selecting represented authentication, additional attributes are requested from the S-PEPS. Since the citizen originates from a country that relies on the MW approach, the authentication request (including additional requested attributes for legal person representation) is forwarded to the MW component (VIDP) hosted in the PEPS domain (Step 3). In a first step, identification and authentication of the citizen is required (Step 4). Again, this is achieved by direct communication between the MW component (VIDP) and the citizen's eID token. Because the citizen wants to act on behalf of a legal person, after successful citizen authentication a separate and additional attribute provider needs to be invoked¹³ (Step 5). This attribute provider is responsible for trustworthy managing the relationship between the citizen and the represented legal person (Step 6). Moreover, this attribute provider asserts the VIDP that the citizen is allowed to represent the desired legal person and transmits the corresponding legal person's name and number (e.g., company name and company's commercial register number) as evidence to the VIDP (Step 7). This information combined with the citizen's identification data are assembled to an authentication token by the VIDP to be returned to the S-PEPS (Step 8). According to the normal authentication scenario, the identification and authentication data are transferred back to the requesting service provider (Step 9). In addition to the citizen's personal identification data the service provider receives information on the legal person the citizen wants and is allowed to represent within the online service.

¹³In this scenario it is assumed that no representation information is stored on the citizen's eID token.

5.5.8.2 STORK 2.0

STORK 2.0¹⁴ is the successor project of STORK and continued with the work on interoperable eIDs in Europe in 2012. 58 partners out of 19 countries are currently working on the three years lasting project [STORK 2.0 Consortium, 2013]. While STORK focused on identification and authentication across borders for natural persons only, STORK 2.0 tackles the challenge by extending and amending the STORK interoperability framework also for legal persons [STORK 2.0 Consortium, 2013]. To achieve this, the STORK 2.0 working groups in particular re-discussed the STORK QAA levels, identified challenges and issues in legal entity identification, assessed on available attribute sources and mandate management systems, and finally amended the STORK interface specifications and processes to support legal entities too. [STORK 2.0 Consortium, 2013]

In detail, STORK 2.0 started with the assessment of existing attribute sources/sinks in the participating member states. These attribute sources can be further used within the pilots. The analysis of attribute sources was based on questionnaires sent out to the participating member states. In particular, focus is put on available mandate information in the individual countries. The results of this analysis on attribute providers/sources can be found in WP2 Team [2012].

Covering legal entities in a cross-border context is one of the key challenges of STORK. Therefore, STORK 2.0 has analyzed available information on legal entities and how they can be represented. Again, for information gathering appropriate questionnaires were disseminated [Parrilli and Graux, 2012]. Since mandates play an important role in the identity management of legal persons, STORK 2.0 additionally analyzed challenges and issues for the cross-border use of mandates. The summary of these challenges and issues can be found in Parrilli [2012].

The inclusion of legal entities into the STORK framework required also an adoption of the STORK QAA levels. Hence, The existing STORK QAA levels were revised by STORK 2.0 in Graux [2012]. This revision includes the coverage of identification procedures for legal entities as well as the application of QAA levels also to attribute providers.

Based on this prior analyses, STORK 2.0 started to amend the existing process flows to incorporate additional use cases with respect to legal entities. The different use cases including e.g. authentication on behalf or empowerment are described in detail in WP4 Core Team [2012]. On architectural level, STORK 2.0 additionally included attribute providers into the basic interoperability models defined in STORK (cf. Section 5.5.4). Hence, a STORK PEPS or STORK VIDP is not only able to connect to an identity provider or SPWare but rather also to affiliated attribute providers. The individual four architectural models including connections to an attribute provider are illustrated in WP4 Core Team [2013]. Finally, to support cross-border use of mandates and legal entities identification STORK 2.0 extended the STORK interface specification with additional attributes. The extended interface specification is described in detail in WP4 Core Team [2014].

5.6 Chapter Conclusions

Currently, the eID landscape across Europe is very heterogeneous. However, the cross-border acceptance of eIDs is crucial for the support of pan-European e-Government services. Two possibilities for achieving cross-border eID acceptance in Europe exist. The first possibility is rolling-out a unifying eID such as the European citizen card to all EU citizens. The second possibility is achieving interoperability of all existing national eID solutions in Europe. Focus of this chapter was put on interoperability. In particular, technical interoperability based on the EU LSP project STORK was discussed. The individual interoperability approaches of STORK were discussed in detail because the basic concepts were taken up or enhanced in further work carried out in this thesis. In particular, in the chapters 7 and 8 it will be relied on the STORK framework when applying the framework in the cloud computing context.

¹⁴<https://www.eid-stork2.eu>

Chapter 6

Cloud Computing

Cloud computing has already been occupying the information and communication technology (ICT) landscape since a couple of years. This buzz word has never disappeared and still can be found often in many news headlines. Hence, it can be expected that in the long term cloud computing will continuously play an important role in the IT sector. Cloud computing brings up several benefits such as high scalability or cost savings due to its IT resource provisioning on demand and flexible pay-as-you-go pricing model. Combining or adopting cloud computing with other concepts such as e-Government or electronic identity can utilize its benefits also in these areas. However, cloud computing can bring up also new obstacles – in particular privacy issues – that need to be taken into account when processing or storing data in the cloud. Before digging into the detailed adoption of cloud computing in the identity management landscape, this chapter gives an overview on cloud computing in general and elaborates on its applicability in the general e-Government sector.

The chapter is structured as follows. First, Section 6.1 explains and defines the term cloud computing and elaborates on different cloud computing models. In the next Section 6.2, public cloud storage services, which constitute a popular use case of cloud services, and how they can be made more secure are described. Finally, the subsequent Sections 6.3, 6.4, and Section 6.5 elaborate on the use and applicability of cloud computing in e-Government in and beyond Europe.

6.1 Cloud Computing in General

Cloud computing does not define a new technology but instead more or less a new way of providing and selling IT resources such as computation power or data storage capacity [Cloud Security Alliance, 2011]. This business model allows provision of IT resources just on demand, hence only the amount of resources really consumed is charged.

The main reason for the hype on cloud computing are its advantages e.g., the enormous potential for cost savings due to the on-the-fly availability of resources. Harms and Yamartino [2010] foresee a move from traditional IT systems into the cloud in the long run. According to them, reasons for such a move are [Harms and Yamartino, 2010]:

- Larger data and computation center can offer IT resources much more cheaper than smaller ones
- Resources can be requested on demand and hence are better utilized
- Multi-tenancy decreases costs for administration and maintenance

The actuality and importance of this IT field is also indicated by the report "Priorities for Research on Current and Emerging Network Trends", which was published by the European Network and Information

Security Agency (ENISA) in 2010 [Gorniak et al., 2010]. This report emphasizes the importance of cloud computing as research topic because several issues such as data protection in the cloud have not been fully solved yet. According to Marketsandmarkets.com [2010], the market growth of cloud computing will increase from \$37.8 billion in 2010 to \$121.1 billion in 2015. This can also be seen as evidence that cloud computing will gain more importance in the next years.

Due to the advantages of cloud computing – especially on economic level – cloud computing can and will also play a major role in the public sector and will influence upcoming e-Government activities. For instance, this was stated by Millard [2011], visioning the eight megatrends for e-Government until 2020. In his vision, cloud computing will gain increasing relevance in the next years. Additionally, this importance has also been emphasized by the European Commission in the ministerial declaration of Malmö [European Commission, 2009] (cf. Section 4.1.1.2) for fulfilling the strategic aims of a digital single market. In the Digital Agenda for Europe [European Commission, 2010a] (cf. Section 4.1.2.3), which is derived from the Malmö declaration, the term cloud computing is explicitly highlighted for governmental services (e.g., indicated by the sentence “[...] *develop an EU-wide strategy on “cloud computing” notably for government and science*” [European Commission, 2010a]).

Cloud computing and its flexible business model of consuming IT resources such as computing power or data storage just on demand promises a lot of benefits and advantages e.g., high scalability and cost reductions. These advantages also the public sector and governments can benefit from. Hence, cloud computing is already on the agenda of governmental policy and decision makers. This section explains cloud computing and its basic idea of a pay-as-you-go pricing model. Additionally, the individual cloud computing models (service and deployment models) are explained.

A good general overview on cloud computing can also be found in Armbrust et al. [2009]; Baun et al. [2011]; Bohm and Mason [2010]; Cloud Security Alliance [2011]; Furht and Escalante [2010]; Pallis [2010].

6.1.1 Definition and Features

Cloud computing is one of the most stated and referenced terms in the IT landscape at the moment. Currently, there is no common definition of cloud computing. Hence, cloud computing providers as well as cloud computing customers usually describe this topic from different viewpoints. Due to the lack of a common view and definition, this section highlights two frequently cited definitions on cloud computing stated by important key actors in the field of cloud computing. The goal of this subsection is to get a common understanding on the term to be used in the remainder of this thesis.

The probably most cited definition of cloud computing comes from the National Institute of Standards and Technology (NIST) [Mell and Grance, 2010]:

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

A similar definition is given by the Cloud Security Alliance [2011]:

“Cloud enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing. More specifically, cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down; providing for an on-demand utility-like model of allocation and consumption.”

Comparing the two definitions, similarities can be found although both statements are formulated differently. However, when synthesizing both definitions, cloud computing can be seen as enabler for an on demand use of services, resources, or data that are provided over a network. This on-demand provision

of desired resources or services (e.g., computing power, data storage, etc.) must be emphasized as it enables cost effective business models for cloud service providers and cost savings for cloud consumers. Hence, cloud computing can be more seen as a new way of providing services than a new technology [Cloud Security Alliance, 2011].

The definitions above already include features of cloud computing. In the following – based on the cloud computing definition of Mell and Grance [2010] – major aspects of cloud computing are highlighted. The following properties are stated by the NIST as essential cloud computing characteristics [Mell and Grance, 2010]:

On-Demand Self Service: Resources (e.g., computing power, data storage, etc.) can be provided by cloud computing service providers to customers automatically and on demand without any human interaction.

Broad Network Access: Resources of a cloud computing service provider are provided through a network and can be accessed by any client (e.g., laptop, mobile phone, etc.)

Resource Pooling: Cloud computing sets up on a so-called multi-tenant model, where both physical and virtual resources are dynamically distributed to customers on demand. In general, the resources are provided in a location-independent way. However, by negotiating appropriate contracts or agreements, specific storage locations (e.g., country, data center, etc.) can be fixed.

Rapid Elasticity: Resources or services are provided fast and elastically by a cloud service provider. Thus, customers do not experience any resource bottlenecks and get the feeling of infinite resource or storage availability.

Measured Services: For bringing the used services to account, transparency defines a key issue for customers. Therefore, cloud service providers measure and monitor customers' used capacity or resources for further charging.

Basically, these five characteristics summarize the main capabilities of cloud computing. IT resources such as computational power or data capacity can be provided to costumers automatically and on-demand without any additional human interaction. The services are provided over a broadband network irrespective of the client used for consumption (e.g., personal computer, mobile phone, etc.). Furthermore, the resources are provided dynamically, highly elastic, and they can be consumed location independent. The consumed resources are measured by the provider and charged to the customer guaranteeing an appropriate level of transparency.

6.1.2 Cloud Computing Architectures and Models

According to Baun et al. [2011]; Mell and Grance [2010], cloud computing can be differentiated into different types of models. Mell and Grance [2010] distinguish between models, which relate more to technical and service aspects (*service models*), and models, which focus on operation of clouds and its organizational aspects (*deployment models*). Referring to Mell and Grance [2010]; Baun et al. [2011], in the following subsections these different types of cloud models are briefly introduced to illustrate which type and kind of model could be applied in the governmental and public sector.

6.1.2.1 Service Models

In this architectural model, according to Mell and Grance [2010], cloud computing is explained using a tier architecture. In most cases, a three tier architecture is referred to. However, the author extends this three tier or level architecture with a fourth layer to indicate that cloud computing can support even more services. Figure 6.1 illustrates this four tier architecture. In the following, these layers are briefly described according to Mell and Grance [2010]; Baun et al. [2011]:

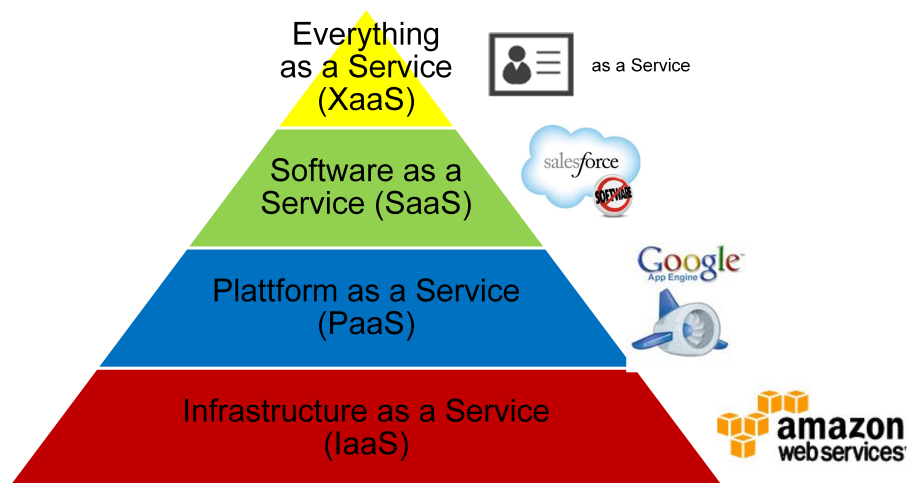


Figure 6.1: Cloud Computing Service Models

- *Infrastructure as a Service (IaaS)*
In this service model, cloud service providers offer their customers fundamental IT resources such as computing power or data storage on demand. Customers are allowed to install their own operating systems and software components but direct access to the infrastructure is denied. *Amazon EC2*¹ is a typical supplier of this service model.
- *Platform as a Service (PaaS)*
In this layer, cloud service providers offer special interfaces to access the cloud infrastructure. Customers can develop their own applications based on these interfaces. An example for this model is the so-called *App Engine*² provided by Google.
- *Software as a Service (SaaS)*
A complete software solution in the cloud is offered by the cloud service provider in this case. E-mail or calendar services to be consumed are typical examples. Google for instance provides such services (*Google Apps*³).
- *Everything as a Service (XaaS)*
IaaS, PaaS, and SaaS usually build the main service layers for cloud computing. However, a lot of other services can be offered in the cloud such as Security or Identity as a Service [Bundesamt für Sicherheit in der Informationstechnik, 2011] (In the Chapters 7 and 8 Identity as a Service will be elaborated in more detail). The author indicates such offerings by extending the three tier model with a fourth layer, where "everything" could be offered as a service [Schaffer, 2009].

6.1.2.2 Deployment Models

Applying this model, cloud computing is reflected by distinguishing how cloud services are deployed and operated. In most cases, cloud computing is differentiated into the operation of a private cloud, community cloud, public cloud, and hybrid cloud. For the following brief explanation to Mell and Grance [2010] is referred. Figure 6.2 illustrates the different cloud deployment models.

- *Private Cloud*
A private cloud is only deployed and operated for a single organization. The private cloud can

¹<http://aws.amazon.com/ec2/>

²<https://developers.google.com/appengine/>

³<http://www.google.com/enterprise/apps/business/>

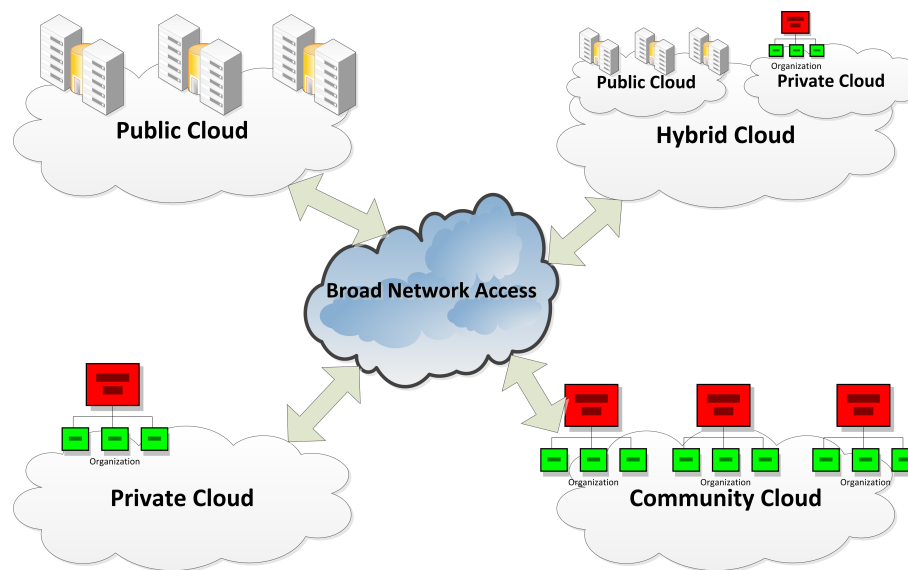


Figure 6.2: Cloud Computing Deployment Models

be deployed by the organization itself or by any other trusted organization, which provides cloud resources to one single organization.

- *Community Cloud*

A community cloud is deployed and operated for a couple of organizations that share common interests. Usually, a trusted third organization acts as cloud provider for a union of organizations, which share the cloud resources.

- *Public Cloud*

A public cloud is deployed and operated for the general public and can be used by everyone. There are no constraints on who shares or consumes the resources.

- *Hybrid Cloud*

A combination or interconnection of different cloud models (e.g., between public, private, and community clouds) is called hybrid cloud. In many cases, organizations operating a private cloud additionally rely on public clouds. The reason is that in case of resource bottlenecks of private clouds resources of public clouds can be added to bypass such bottlenecks.

6.2 Public Cloud Storage Services

Cloud computing and in particular storage services in a public cloud are frequently used to save data on external systems e.g., for archiving or backup purposes. Popular examples of such public cloud storage services are e.g., DropBox⁴ or Google Drive⁵. These cloud storage services enable data storage and file synchronization in the cloud. Furthermore, the stored data can be accessed through various clients and thus data access is independent of location and device. This especially is essential as mobile devices such as smartphones or tablets gain more and more popularity.

While insensitive information and data can simply be stored on such public cloud providers, security and confidentiality plays an inevitable role if sensitive data needs to be stored in the cloud. Most cloud providers cannot easily fulfill such requirements, as the providers usually are able to inspect the stored

⁴<https://www.dropbox.com>

⁵<https://drive.google.com>

data. Even if the cloud provider encrypts the data and stores it in encrypted format, the provider is always in possession of the decryption key.

To still be able to store sensitive data securely and confidentially in the cloud, some cloud providers offer solutions where data are encrypted on client-side prior to its transfer to the cloud. Such solutions are briefly introduced in the next Subsection 6.2.1. However, most of those solutions have the drawback that the encryption and decryption process relies on software-based keys, which are stored on the respective client device and under some conditions could be accessible by unauthorized parties. To bypass security issues raised with that approach, in Subsection 6.2.2 a solution is proposed which uses a hardware-based key pair kept on a smart card to protect data stored in the cloud. The proposed solution relies on the Austrian citizen card (cf. Section 3.6.2). The usage of the Austrian citizen card has the advantage that it is based on a solid and independent Public-Key-Infrastructure (PKI). Hence, data can be practically encrypted for each Austrian citizen and securely stored and shared in the cloud.

6.2.1 Software-based Secure Cloud Storage Services

Software-based secure cloud storage services use software-based keys for the encryption and decryption process of data before storing the data in the cloud. In this section, three existing cloud storage services that rely on software certificates are briefly elaborated. The elaboration is based on Derler [2013]; Zwattendorfer et al. [2013d].

6.2.1.1 Boxcryptor

Boxcryptor⁶ is available for multiple platforms e.g., Windows, Mac OS X, iOS, Android, and Windows Phone. Boxcryptor provides support for the cloud storage services DropBox, SugarSync⁷, Microsoft OneDrive⁸, and Google Drive. A basic version of BoxCryptor is offered for free. In addition, an unlimited version of Boxcryptor can be purchased. Main feature of the purchased version is filename encryption. Boxcryptor manages the data storage in volumes, i.e., each volume corresponds to a specific cloud storage service. If files are copied into a volume, the files are automatically encrypted and copied into a corresponding subfolder of the cloud storage service directory. For instance, if a file is copied into a volume named "Google Drive", the file is encrypted and stored in the "Boxcryptor" folder, being a sub-directory of the "Google Drive" directory.

6.2.1.2 CloudFogger

CloudFogger⁹ is freely available for Windows, Mac OS X, Android, and iOS platforms. Supported cloud storage services are DropBox, Microsoft OneDrive, and Google Drive. Users need to specify which cloud storage services they wish to protect, with the option of disabling protection for subfolders. Protected cloud storage service directories can be accessed and manipulated as usual. However, before uploading files to the cloud storage, CloudFogger encrypts each file and uploads the encrypted file instead.

6.2.1.3 Viivo

Viivo¹⁰ is a free software and available for iOS, Android, Mac OS X, and Windows platforms. The cloud storage services supported by Viivo are again DropBox, Microsoft OneDrive, and Google Drive. Encryption functionality is similar to the two previously discussed solutions. If a file is copied into the

⁶<https://www.boxcryptor.com>

⁷<https://www.sugarsync.com>

⁸<https://onedrive.live.com>

⁹<http://www.cloudfogger.com>

¹⁰<http://www.viivo.com>

”Viivo” folder, the file is encrypted and stored in a specific subfolder of the underlying cloud storage service. Subsequently, the file is uploaded and synced with the DropBox, OneDrive, or Google Drive servers. Decryption works the opposite way around. If an encrypted file is added to the subfolder of the underlying cloud storage service, the file is automatically decrypted and moved to the ”Viivo” folder.

6.2.1.4 Browser-Based Encryption Tool

All of the previous described solutions require binary client software or a special browser plug-in to be installed on the user’s local machine. To bypass this requirement, Lenz et al. [2013] proposed a solution that allows client-side data encryption for cloud storage without installing separate software modules or browser plug-ins. Thereby, Lenz et al. [2013] fully rely on browser-based technologies such as JavaScript or HTML5 [Berjon et al., 2014], which are supported by most popular web browsers. By the help of this framework, data or files can simply be stored encrypted on a remote server or in the cloud using a standard web browser. Moreover, users are able to simply drag and drop files into their web browser, which are further encrypted and stored on a remote server.

6.2.2 Hardware-based Secure Cloud Storage Services

While software-based secure cloud storage services are a promising approach to keep data confidential with respect to the cloud storage service, they still have the drawback of using just software certificates for encryption/decryption. Under certain conditions software certificates might be accessible by unauthorized parties. To bypass this issue, Zwattendorfer et al. [2013d,e] proposed a cloud storage service solution that relies on hardware-based certificates. To achieve this, they used the Austrian citizen card (cf. Section 3.6.1) in combination with the open source software CCE (cf. Section 2.2.3.2). In the following, details of the work of Zwattendorfer et al. [2013d,e] are given.

6.2.2.1 Architecture and Implementation

To achieve a hardware-based cloud storage service, the CCE software has been extended in order to be able to store data also at public cloud providers and not only in the local storage. Citizens can thereby select between different cloud storage services where data should be stored. Besides local storage, the current implementation supports the providers DropBox and Google Drive.

Figure 6.3 illustrates the architecture for secure encryption and decryption of data by using the Austrian citizen card functionality and storing the encrypted data in the public cloud. In this architecture, in fact three different entities are involved: (1) the citizen who wants to store a file or directory securely in the public cloud, (2) the Austrian citizens the files or directory should be encrypted for, and (3) the public cloud provider where the encrypted files will be stored.

Figure 6.3 also illustrates the encryption process using CCE and subsequently the process of storing the encrypted data in the public cloud. In a first step (Step 1), the citizen selects the files and directories she wants to store securely and confidentially in the cloud. In the next step (Step 2), the citizen selects one or more persons (Austrian citizens) the chosen files or directories should be encrypted for. If citizens’ encryption certificates are not known by CCE yet, they can be queried from the central LDAP directory¹¹. In this directory, all public certificates of every Austrian citizen registered in the Austrian eID system are stored. Before starting the encryption process, the validity of the encryption certificates of the selected persons is checked. Finally, in Step 3 the data are encrypted for the intended citizens and transferred to the selected public cloud provider. Authentication credentials for accessing the public cloud provider need to be provided during the configuration and setup of CCE. During the data transfer, the credentials are retrieved from the CCE configuration and provided to the public cloud provider automatically.

¹¹The querying of the external LDAP service is not necessary if the users have exchanged the certificates by other means e.g., by using e-mail.

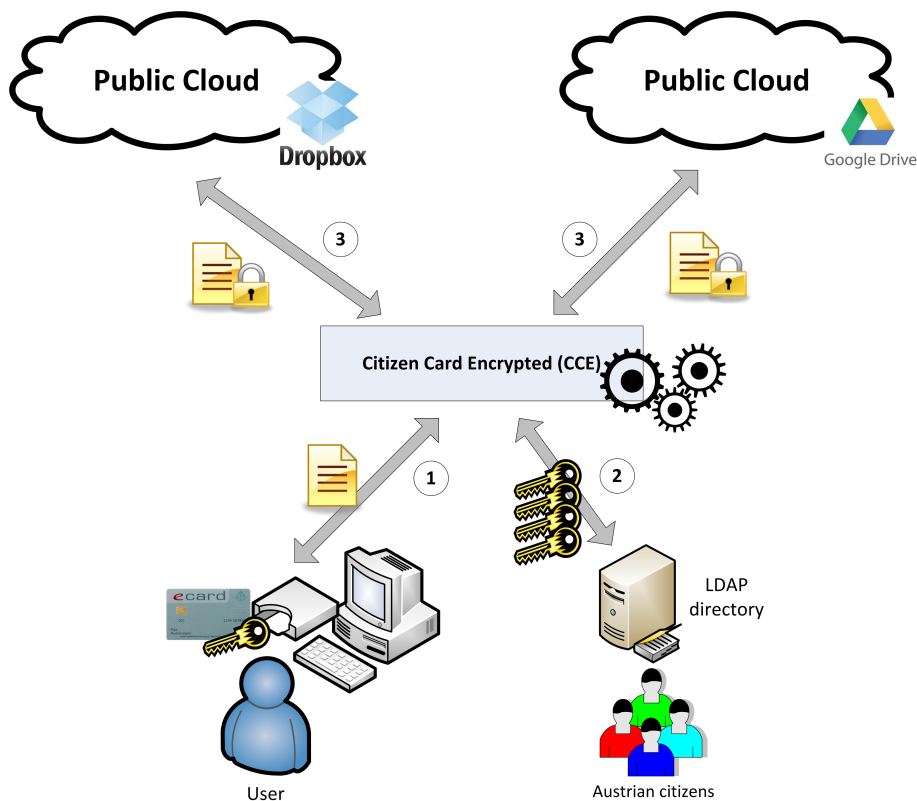


Figure 6.3: Architecture for securely storing data in the public cloud using the Austrian citizen card [Zwattendorfer et al., 2013d]

The decryption process is similar to the encryption process, hence the decryption process will not be illustrated. In the decryption process, the encrypted data are downloaded from the public cloud into the local file system by the user. Afterwards, the data are decrypted by using CCE and invoking the citizen's citizen card. Now, the citizen is able to inspect the plain data.

For supporting public cloud storage as an option, CCE had to be amended and extended accordingly. In particular, emphasis was put on flexible adding of additional public cloud providers besides DropBox and Google Drive. For adding an additional cloud provider, the server communication with the cloud provider and its configuration management needs to be implemented. The existing modular internal architecture of CCE allows for an easy implementation of new providers.

The creation of a new public cloud provider configuration requires a smart card because the smart card is linked to the credential information necessary to access cloud provider services. The credential information for the cloud provider is thereby encrypted by the affiliated smart card, stored in the local file system, and assigned to the corresponding person. Hence, an automatic mapping between smart card and cloud provider authentication credentials is achieved. The advantage of this approach lies in the fact that cloud specific authentication data need to be entered just once during configuration, it is then accessed automatically during each subsequent cloud data transfer.

In detail, configuration of authentication credentials for cloud provider access is as follows. Authentication at the cloud provider is based on the authorization protocol OAuth (cf. Section 3.5.4) for both cloud providers DropBox and Google Drive. Required authentication tokens of OAuth are ascertained during the configuration of a new cloud provider in CCE. This requires the input of the authentication credentials from the user, which in turn adds CCE as trusted cloud application for the user at the cloud service provider and which gives CCE access to the user's cloud account. Subsequently, CCE receives an access token from the cloud provider for the secure access to the cloud storage. According to the OAuth protocol, this access token can be continuously used for cloud provider authentication so that additional

provision of user authentication credentials is not required anymore.

To store data confidentially, users are able to select their desired storage location. The default location is the local file system, whereas users are now able to also store encrypted data at different cloud providers, which are linked with their citizen card. During data upload, saved cloud provider credentials are decrypted by using the user's smart card and are used for cloud provider authentication. Besides extending the pure CCE application, integration into the operating system's file system has been implemented too. In this case, users are able to copy files into a specific folder of the personal HOME directory and files are then automatically encrypted and transferred to the cloud. When moving files into this specific folder, the CCE wizard starts automatically. Recognition of moved or newly created files in this specific folder is implemented using WatchServices¹², which observe file system operations. Using the CCE wizard, not only files can be automatically encrypted but also desired recipients can be selected. For distribution of encrypted files the existing mechanisms of the respective cloud provider can be used.

6.2.2.2 Evaluation

In this subsection, the proposed hardware-based cloud storage solution of Zwattendorfer et al. [2013d,e] is evaluated and compared against existing software-based cloud storage solutions. In particular, advantages and disadvantages are discussed.

Advantages: The following advantages of Zwattendorfer et al. [2013d,e] compared to other solutions can be identified.

Use of external PKI infrastructure: All of the introduced software-based solutions rely on their own proprietary encryption system. To finally be able to encrypt and decrypt data, all participating users must be registered at the same cloud service provider. The advantage of the proposed hardware-based solution is the use of an external PKI infrastructure, which is governmental-based and can be freely used by all Austrian citizens. As soon as the Austrian citizen card is activated, neither the citizen encrypting the data nor the citizen decrypting the data requires any further registration process. Citizens can easily encrypt data for other citizens without requiring (personal) contact with the other citizen e.g., to exchange certificates or passwords. In particular, CCE is not limited to the use of the Austrian PKI infrastructure but also other infrastructures, e.g., from an enterprise which rely on smart cards, can be integrated.

No vendor lock-in: The decryption keys are not managed by CCE but rather from an external authority. This in particular means that CCE is neutral and independent from the cloud provider. Users can easily switch the cloud storage provider without necessitating any change in internal organizational processes.

Secure hardware-based decryption: In case of CCE, for decryption a secure hardware-based device (smart card) is used. This increases security compared to software-based solutions. Security is increased because (1) the private key cannot be extracted or read out from any software application and (2) for decryption a two-factor based authentication mechanism (cf. Section 3.1.2.2) is used. In contrast, software-based solutions just rely on passwords for decryption which are stored directly on the user's local machine. This increases the risk that passwords can be phished by malware and thus unauthorized access to the encrypted data might be possible.

Open source implementation: The CCE software is published as open source. In addition, S/MIME [Ramsdell and Turner, 2010] is also publicly available. Hence, new features can be easily integrated and extensions are easily possible. For instance, new cloud storage services can be easily

¹²<http://docs.oracle.com/javase/7/docs/api/java/nio/file/WatchService.html>

added, new container or additional container formats could be used, and further smart card support including a different PKI infrastructure could be incorporated.

Disadvantages: The following disadvantages of Zwattendorfer et al. [2013d,e] compared to other solutions can be identified.

No web or mobile client: Compared to existing software-based solutions, CCE is currently only available as desktop platform. In addition, the use of smart cards in connection with mobile devices is inconvenient. Currently, no mobile or web-browser solutions are available. However, the integration of the work of Lenz et al. [2013] could help in developing a browser version which uses smart cards for decryption.

No file synchronization: Existing software-based cloud storage services have the advantage that files are automatically synced with the remote server also during the encryption process. CCE does not support this functionality. Moreover, in CCE the files are encrypted locally first and afterwards uploaded to the cloud server.

Card reader required: The adoption of the proposed hardware-based solution requires the use of a card reader. This requirement may limit the choice of systems, as card readers might not be available at all clients.

6.3 Cloud Computing in E-Government

Cloud computing is penetrating many areas because of its advantages. High scalability, low maintenance efforts, enormous cost savings potential, and several other benefits make cloud computing also interesting in e-Government. Especially, the increasing tightness of governmental budgets can benefit from cloud computing adoption, as the amount of IT expenditures could be decreased [Wyld, 2009]. Saving costs in the governmental sector is essential. For instance, the aim of decreasing costs for public services was also anchored in the Austrian governmental programme [Austrian Ministry of Finance, 2012]. The cost savings potential of cloud computing in the governmental sector is enormous. Alford [2009] estimates a saving potential between 50 to 67% by moving governmental applications into private or public clouds. Harms and Yamartino [2010] conclude similarly in their economic analysis of cloud computing for the public sector. Particularly, Harms and Yamartino [2010] argue that public clouds have always higher cost benefits for public services compared to private clouds, irrespective of the required amount of IT resources or the cloud size. In the following, benefits and issues of cloud computing in e-Government are discussed according to Zwattendorfer et al. [2013b]. Further advantages and disadvantages can also be found in Parycek et al. [2011].

6.3.1 Benefits for E-Government

Besides cost benefits, cloud computing has several further advantages for public services. Bhisikar [2011] lists a couple of advantages of cloud computing for the public sector. Based on these findings, the most important advantages of cloud computing in the governmental sector are listed [Bhisikar, 2011]:

- Scalability
- Pay-as-you-go pricing model
- Easy implementation
- Low maintenance

- Availability

One main advantage of cloud computing for public services is *scalability*. Depending on the e-Government application, only resources, which are actually required, are consumed. This especially helps to absorb high load peaks of applications (e.g., e-Procurement, tendering, or election days), which may have higher access rates in a limited time period. The flexible pricing model of clouds allows for just paying the very amount of IT resources, which effectively have been consumed. This *pay-as-you-go pricing model* enables public services to save a lot of IT costs. Cloud applications are *easy to implement*. Public authorities do not need to buy hardware or software licenses for their services but just can use the IT infrastructure (IaaS, PaaS, or SaaS – cf. Section 6.1.2) of the cloud service provider. Usually, cloud service providers offer some kind of APIs (application programming interfaces), where individual cloud applications can be developed to. The use of cloud services also *lowers maintenance* tasks. Patch or update management can be fully handled by the cloud service provider, hence no manual maintenance tasks, e.g., for updating operating systems or installing security patches, are required. Finally, the use of clouds can increase *availability* of applications. Applications can be deployed in different cloud data centers, distributed around the world. In case of a breakdown of one data center, the application may still continue running in another cloud data center of the cloud provider.

6.3.2 Issues and Challenges for E-Government

Although cloud computing offers a lot of advantages to public services, several issues and challenges need to be considered or met when applying cloud computing in the public sector. Hindering issues might be, for instance, security, privacy, or data protection concerns when processing or transferring sensitive data into the cloud [Sen, 2013; Zissis and Lekkas, 2012; Pearson and Benameur, 2010; Helmbrecht, 2010]. The author briefly lists some requirements, which must be fulfilled when taking advantage of cloud computing in the public sector. Of course, whether those requirements can be simply fulfilled or not, heavily depends on the cloud computing deployment or service model applied. According to Deussen et al. [2010]; Reichstädter [2012]; Wyld [2009]; Repschlaeger et al. [2012] the main issues and challenges for adopting cloud computing in the public sector are:

- Security
- Data protection and compliance
- Interoperability and data portability
- Identity and access management
- Auditing

Providing a high level of *security* for public sector cloud computing is essential. Security requirements must be fulfilled on several layers. This means, for instance, that network, application, or data security must be assured by the cloud.

Data protection defines one of the main issues when talking about cloud computing. In e-Government applications and services usually sensitive data are processed, hence meeting this requirement is indispensable. Particularly, some data protection regulations do not allow the storage of sensitive data in other countries, which is basically not accomplished by most cloud service provider as their data centers are usually spread around the world. For instance, the reason is that data stored on servers in the USA might be inspected by the US government without notifying the data owner. Such possible inspections are legally anchored by the USA Patriot Act [Senate of the United States, 2001]. Hence, being *compliant* to such regulations is essential.

Cloud computing has a fast growing and emerging market. Up to now, this mainly led to a heterogeneous landscape on service and interface offerings of cloud service providers. Due to that, the so-called "lock-in" effect can be often recognized. This means that although another cloud service provider offers better pricing conditions than the current one, switching to the other cloud service provider is still uneconomic because the opportunity costs for *data* and application transfer (*porting*) are too high. To bypass this issue, standardized services and interfaces might help to achieve *interoperability* between cloud service providers.

E-Government applications usually require more secure and reliable *authentication and identification mechanisms*. While most traditional e-Government services stick to stronger authentication and identification techniques, current cloud applications still lack in adoption of such techniques. However, e-Government services in the cloud require the same strength of authentication and identification as current e-Government applications do.

Auditing becomes essential e.g., in situations where compliance to specific regulations or policies must be verified. Cloud providers currently do not offer detailed auditing possibilities, hence further research in this field is required.

Summarizing, e-Government applications and services in the cloud have to fulfill stronger and stricter requirements as needed e.g., for simple informational cloud services. A more comprehensive list on requirements of e-Government applications in the cloud can be found in Section 6.3.5.

6.3.3 Evaluation of Cloud Computing Models for E-Government

All the previously defined cloud models of Section 6.1.2.1 and Section 6.1.2.2 have their advantages and disadvantages. In fact, all models could be used for governmental applications and public services taking several limitations into account for each model. In the following sections, the three basic cloud computing service models and the four main cloud computing deployed models are evaluated on their applicability for the use in e-Government.

6.3.3.1 Evaluation of Cloud Service Models

The various offered service models constitute the fundamental basis for deploying or operating e-Government applications in the cloud. Therefore, the three basic service models (IaaS, PaaS, SaaS – cf. Section 6.1.2) are evaluated for their applicability in e-Government.

Outsourcing of IT infrastructures into cloud environments, i.e., using IaaS, generates the most economical advantage for organizations [Harms and Yamartino, 2010]. Existing applications can easily be migrated into cloud environments using the IaaS model. In the IaaS model, the operating systems or application runtime environments for the underlying cloud infrastructure can be chosen by the cloud customer, which in this case are governments or public authorities. Moreover, the cloud customer has full control over the operating systems and the runtime environments. However, this freedom of choice regarding operating systems or supported runtime environments also increases administrative complexity for customers. For example, customers have to maintain security or any other updates for the operating systems on their own. [Harms and Yamartino, 2010]

In contrast, the development of an e-Government application based on a PaaS model has several advantages. Developers can fully focus on the development of the application itself, as they do not need to waste any thoughts on scalability due to the high computing power of cloud environments. There is also less effort required for administrative work because operating systems and runtime environments are provided and maintained by the cloud provider. Of course, existing applications must be amended to support the cloud provider interfaces for a cloud migration. However, new applications can be easily developed in such a way to fully utilize all cloud features. [Harms and Yamartino, 2010]

The administrative complexity can actually be minimized by applying the SaaS model. However,

applying this model reduces flexibility, as applications are offered in a very generic way and cannot easily be enhanced or amended to specific needs. Specific amendments require high efforts and are thus very cost intensive. Currently, the bigger cloud providers mainly offer e-mail or office services as cloud applications. In contrast, e-Government applications are usually tailored to support specific requirements of authorities or legal frameworks and thus will probably not be offered by bigger public cloud providers as service models soon. Such applications will rather be developed and provided by smaller companies taking PaaS models of public cloud providers as a basis for hosting their own SaaS model. [Harms and Yamartino, 2010]

Based on these considerations, it can be concluded that PaaS and SaaS models suit best as a basis for e-Government application developments. On the one hand, the PaaS model is suitable because applications can be developed using the interfaces provided by cloud providers to utilize highly available resources. On the other hand, using PaaS provides the ability of staying independent from the underlying infrastructure. The SaaS model is suitable too as the same arguments take effect when application development and migration is outsourced.

In summary, it can be stated that the transfer of IT infrastructure or applications into cloud environments can be of great interest for public authorities or governments, such as municipalities or even smaller countries. While basically all service models are applicable for e-Government [Roessler, 2010], the situation is more complex regarding the choice of the correct deployment model [Catteddu, 2011]. Various studies on cloud computing and e-Government recommend the use of private cloud models or community cloud models for public-sector applications. Nevertheless, the use of public clouds can play a major role for public administrations, as especially the cost effectiveness constitutes a major and noteworthy advantage. The following subsection elaborates and evaluates the use of cloud deployment models in the public sector.

6.3.3.2 Evaluation of Cloud Deployment Models

Besides service models, deployment models are an important instrument to characterize cloud computing and its features. In this section, the four main cloud computing deployment models are evaluated according their applicability in e-Government scenarios. The evaluation is based on a SWOT¹³ analysis carried out by Catteddu [2011]. The following Table 6.1 compares strengths and weaknesses of all cloud deployment models for their e-Government adoption.

Private Cloud: A private cloud is usually operated for a single organization only. Since the resources are not shared amongst others, this deployment model offers stronger control over the resources and the data processed in the private cloud. Additionally, the operator of the private cloud can easier be compliant to legal regulations, as requirements need to be fulfilled of one single organization only. Compared to public clouds, private clouds allow for more detailed logging and auditing possibilities. Since the private cloud provider is trusted, also more sensitive data might be stored and logged at the private cloud provider.

Disadvantages of private clouds are its higher costs, its lack of elasticity, and being a specific point to attack. Since the private cloud is operated for one single organization only, cost advantages of pure cloud computing, where resources are shared, cannot take effect. In addition, private clouds cannot provide as much elasticity because their resources are limited. Finally, a private cloud constitutes a single point of attack as the computation power is more concentrated.

Community Cloud: Community clouds bundle IT resources for a couple of organizations that share the same interests. They are higher elastic than private clouds because more IT resources are required

¹³Strengths-Weaknesses-Opportunities-Threats

Table 6.1: Evaluation of Cloud Computing Deployment Models [Zwattendorfer and Tauber, 2012c, 2013]

Private Clouds	
<i>Strengths</i>	<i>Weaknesses</i>
<ul style="list-style-type: none"> • Strong control • Detailed logging/auditing • Compliance with legal regulations 	<ul style="list-style-type: none"> • Higher costs • Specific point to attack • Lack of elasticity
Community Clouds	
<i>Strengths</i>	<i>Weaknesses</i>
<ul style="list-style-type: none"> • Lower costs than private cloud • Elasticity • Compliance with legal regulations 	<ul style="list-style-type: none"> • Competition between consumers • Specific point to attack • Consensus between involved parties required • No accurate prediction on required resources • Who is the legal entity in case of liability
Public Clouds	
<i>Strengths</i>	<i>Weaknesses</i>
<ul style="list-style-type: none"> • High availability • Reliability • High elasticity • Facilitated patch management • Distribution for failure safety • Low costs 	<ul style="list-style-type: none"> • Compliance with legal regulations • Isolation issues due to multi-tenancy • Less detailed logging capabilities • Proprietary interfaces
Hybrid Clouds	
<i>Strengths</i>	<i>Weaknesses</i>
<ul style="list-style-type: none"> • Flexibility • Stronger control 	<ul style="list-style-type: none"> • Complexity • Compatibility issues due to different interfaces • Classification of data (sensitive data should not be stored in public clouds)

for multiple organizations. Community clouds are also more cost-effective than private clouds, as expenditures are shared amongst several organizations. Finally, they also allow for compliance with legal regulations as the cloud can be operated according special requirements of the participating organizations.

Equally to private clouds, the community cloud constitutes a specific point to attack, which is one of the disadvantages of community clouds. Another disadvantage is the competition between consumers

regarding resource consumption. Since resources are shared amongst several organizations, consensus between the involved parties is required. Concerning setting up a community cloud, predictions on the amount of required resources are needed. It is very difficult to give accurate predictions on that. Finally, liability issues may arise in case of any problems, because the community cloud is operated for several legal entities and not only one. Hence, the question arises which legal entity will be responsible e.g., in case of data protection violations.

Public Cloud: Public cloud providers offer IT resources to the general public. Main advantages of public clouds are their high scalability and their low costs. Public cloud providers usually have huge data centers, which guarantee high availability on the one side and allow for low cost offerings on the other side. Due to these huge data centers, customers get the impression of being able to consume unlimited resources, so high elasticity is given. For most big public cloud providers the data centers are distributed around the world, which enables failure safety in case of a breakdown of one data center.

Although public clouds have a lot of advantages, also several disadvantages with respect to e-Government can be identified. One main disadvantage of public clouds is the difficulty of being compliant with legal regulations. This requirement is especially important for e-Government applications, as in this area usually legal requirements, e.g., data protection regulations protecting citizen's privacy, must be fulfilled. Guaranteeing data protection is essential for most e-Government applications. This means that in sensitive applications data should not unintentionally be disclosed. However, currently public cloud providers have still problems in solving isolation issues due to the provided multi-tenancy. In addition, the full logging functionality of public cloud services cannot be used as for many governmental services it is not allowed to store sensitive data in private sector applications such as public clouds. Since the private sector currently is the driving force behind public clouds, standardization efforts and the adoption of standards are not driven by the private sector. The use of proprietary interfaces of private sector cloud providers allows for easier vendor lock-in and does not enable data portability, which is important for e-Government services.

The public cloud offers a lot of advantages, but still has severe disadvantages which might hinder e-Government adoption of public clouds. However, in Section 6.3.4 the author describes why the advantages of public clouds outbalance its disadvantages. Moreover, it is argued that public clouds are worth more than a short spot for e-Government adoption if certain issues can be bypassed.

Hybrid Cloud: A hybrid cloud is a consolidation of different cloud deployment models, such as between public, private, or community clouds. A hybrid cloud allows for stronger control than a pure public cloud because main functionality may be encapsulated in a private cloud. Moreover, a hybrid cloud is flexible in terms of resources. For instance, if consumed resources of a private cloud are going to run out, additional resources of a connected public cloud can be requested.

Nevertheless, hybrid clouds also have their disadvantages. They are more complex as several different cloud models must be combined. Due to this combination, also compatibility issues can occur because current cloud implementations lack in fully compatible and standardized interfaces. Moreover, classification of data is required because sensitive data should not be stored in a public cloud but instead should rather be processed in a private cloud.

6.3.4 The Public Cloud for E-Government

All cloud computing deployment models described and evaluated in the Sections 6.1.2 and 6.3.3 have their advantages and disadvantages. The desired model to be applied strongly depends on the intended use case and its derived requirements. Although the enormous cost savings potential and high resource capacity argue for a highly adoption of public clouds, requirements such as control possibilities or legal compliance constrain for the use of private or community clouds. Especially in e-Government, criteria

such as security or data protection play a strong role. However, also cost savings are an important success factor for e-Government.

Various studies have already investigated the use of cloud computing for public services. Most studies recommend the use of private and community clouds for public authorities. For instance, due to the heterogeneity of national laws and regulations also ENISA recommends these two models for e-Government. More concretely, they state that *"in terms of architecture, for sensitive applications private and community clouds appear to be the solution that currently best fits the needs of public administrations since they offer the highest level of governance, control and visibility [...]"* [Catteddu, 2011]. Additionally, all current cloud computing adoptions in various countries target more the private cloud than the public cloud (cf. Sections 6.4 and 6.5).

However, although current studies recommend the use of private and community clouds for governments and most countries even rely on these models, the use of public clouds should not be excluded for more sophisticated public and governmental services as long as certain requirements (e.g., legal compliance, data protection, security, etc.) can be fulfilled. The reason for this statement is simple because public clouds offer the best advantages of cloud computing (low costs, high availability, less maintenance, etc.). Especially, the possibility of cost reductions for IT infrastructure and services must be emphasized.

According to Harms and Yamartino [2010], IT infrastructure costs take the main share of IT expenditures, namely 53%. In addition, 36% apply to maintenance of existing services and 11% to the development of new applications [Harms and Yamartino, 2010]. For these areas, cloud computing can effectively help to decrease IT expenses. Concerning IT infrastructure, IT costs can be decreased by shifting parts or the complete infrastructure to a public cloud provider. Furthermore, such a move also transfers maintenance burdens such as installing software patches to the cloud provider. Additionally, applications need not to be expensively developed for the public cloud but can simply be consumed as a service from the cloud.

Overall, the study of Harms and Yamartino [2010] sees public clouds always more economical than private clouds, irrespective of the organization size or the number of required servers or computing power. Figure 6.4 illustrates this cost effectiveness of public clouds (total cost of ownership per server compared to the number of servers) of Harms and Yamartino [2010].

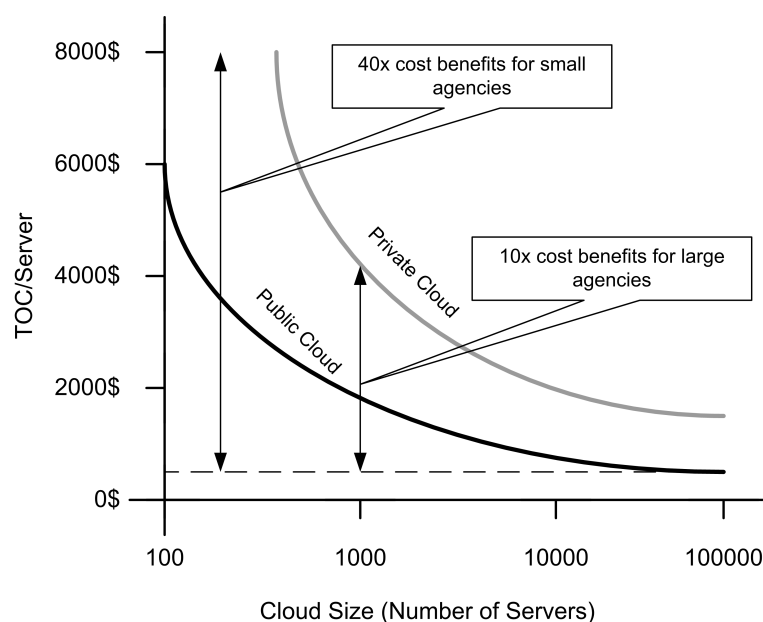


Figure 6.4: Economic benefits of public clouds compared to private clouds [Harms and Yamartino, 2010; Zwattendorfer and Tauber, 2013, 2012c]

The highest cost saving potential is given if organizations just require a couple of hundreds server only. The cost benefit is given under a factor of 40 if a public cloud is preferred over a private cloud. Increasing the number of required servers, the cost benefit shrinks down to a factor of 10. Nevertheless, according to Figure 6.4 public clouds will be always more beneficial than private clouds. What this figure does not illustrate are investment costs for setting up a private cloud. Since there are no real investments (e.g., computer hardware) required for using a public cloud, the economic benefits of public clouds compared to private clouds may be even higher. [Harms and Yamartino, 2010]

This economic advantage and flexibility of public clouds is especially interesting for public authorities and municipalities. Referring to Figure 6.4, smaller municipalities do not require an own data center with more than hundred servers. Since in this area of the chart the cost savings potential is the highest, municipalities can save a lot of money by transferring IT infrastructure or applications into the public cloud. They can further focus on forcing e-Government activities instead of maintaining and setting up their own data center.

The use of public clouds in e-Government may have several advantages, but still some issues can be identified, which may delay or even hinder its adoption. In Table 6.1 the use of public cloud computing in e-Government has been evaluated by listing several advantages and disadvantages.

One main advantage of using public clouds in e-Government is that public authorities do not have to spend money for setting up their own cloud or IT infrastructure. Public clouds provide as many IT resources as required to its customers, which are governments or public authorities in this case. Hence, for governments or public authorities there is no need for planning required IT resources because they can be easily consumed just on demand from a cloud service provider. This advantage can save the public sector a lot of costs. In addition, costs can be saved due to lower maintenance demands. For instance, operating system updates or security patches for application servers are installed by the public cloud service provider and do not require any manual interaction from the cloud customer. Finally, the public cloud offers high availability and high elasticity to governmental applications. High availability is guaranteed because public cloud providers usually operate several huge computational centers distributed.

By relying on public cloud providers, public authorities do not need to specifically maintain extra replication services. In terms of elasticity, there is no need for public authorities to develop or design their applications for high load, if high load can only be expected at peak times. Peak times at online applications are easily absorbed by the infrastructure of the public cloud.

Nevertheless, although public clouds can provide a lot of benefits to governments or public authorities, still some disadvantages may hinder the adoption of public clouds in the public sector. One main point of criticism is compliance with legal regulations, such as data protection. For instance, in EU countries legislation forbids sensitive data storage in countries outside the European Union. However, many public cloud providers offer their services in other countries, such as the US, and thus public cloud resource consumption from these providers may violate EU law. Another disadvantage is less control. Since all services and data are moved to the public cloud provider, the public authority has to trust the public cloud provider that it treats the data according to given contracts or agreements. Furthermore, customization of cloud services might be expensive. As an example, cloud services offered as SaaS are mostly developed for the general public, hence adjusting such applications to domestic or national requirements could definitely increase costs. The development of customized services could also lead to some kind of dependency to the cloud service provider (frequently called "vendor lock-in"). I.e., if – for instance – the provider suddenly changes its business model and a provider switch is desired, switching can be much more expensive than staying at the provider. The reasons are the enormous migration effort and costs making a switch to another provider uneconomical.

Summarizing, comparing and balancing the advantages and disadvantages of public clouds for e-Government, they still provide more advantages, especially in terms of costs, than disadvantages. While the identified disadvantages currently still exist, at the moment a lot of research and standardization efforts are going on in these directions, especially in the field of security. Hence, it can be expected that

some of these disadvantages can be mitigated already in the near future. If public-sector applications are migrated to public clouds, several requirements must be met to assure an appropriate level of security. To leverage the awareness of this issue, the following section lists certain requirements that must be met if e-Government applications are deployed in public clouds.

6.3.5 Requirements for E-Government Applications in the Public Cloud

This section discusses and summarizes the most important requirements that must be met for developing and running e-Government applications in a public cloud. The listed requirements can serve as starting point for policy makers, researchers, managers, or developers of the public sector if they intend to design, develop, or migrate e-Government applications to the public cloud. The defined requirements must be met or fulfilled by a cloud-based e-Government application in order to protect citizens' privacy and to stay compliant with according laws. The author focuses on the public cloud only, as this deployment model takes best advantage of the general cloud computing benefits. In addition, the presented requirements for e-Government applications in the public cloud examine only PaaS and SaaS models without considering IaaS approaches. PaaS or SaaS applications can be easily applied in public cloud offerings, whereas IaaS applications require much more maintenance and management effort, which in turn increases costs.

In the next subsections 17 requirements are introduced by the author in total. These requirements address technical, organizational, legal, and economic aspects. The identified requirements are classified into these four categories. Needless to say, this classification is not written in stone as some requirements may target several categories. Although the requirements have been classified based on these four different aspects, they are mostly discussed on technical level. The listing of these requirements is partly based on the work of Catteddu and Hogben [2009]; Paquette et al. [2010]; Pearson and Benameur [2010]; Catteddu [2011]; Subashini and Kavitha [2011]; Gongolidis et al. [2014].

6.3.5.1 Technical Requirements

This section comprises several technical requirements, which must be considered when designing or developing e-Government applications in the public cloud.

Confidentiality: Confidentiality in the context of e-Government applications means that, on the one hand, the application itself must work trustworthy and, on the other hand, any processed sensitive or personal data must be treated confidentially. The cloud provider itself or any other unauthorized organization should not get access to sensitive data. This requirement relates to sensitive data, which are intended to be processed within the cloud application or to be transferred into the cloud. [Baun et al., 2011]

Authenticity: Authenticity describes the genuineness, trustworthiness, and reliability of objects and can for example easily be proved by applying electronic signatures. Since many e-Government applications process sensitive or personal data, it is important that the authenticity of the processed data can always be verified when necessary. However, authenticity is not only required for the processed data but also the application itself.

Integrity: In general, integrity defines some kind of guarantee that applications work correctly and data cannot be altered [Cloud Security Alliance, 2011]. For instance, in running applications it must be verifiable that no malicious code has been injected. Referring to Reichstädter [2012], four types of integrity can be distinguished: data integrity, software integrity, configuration integrity, and message integrity. Hence, integrity must be assured in several areas where data are processed.

Dependencies: Within cloud computing, service oriented architectures (SOA) or web services play an important role [Baun et al., 2011]. Services are loosely coupled, distributed, and can be interconnected for new services creation. Due to the distributed architecture, dependencies to other services can also exist in cloud environments. A typical example for dependencies between clouds would be the deployment of a hybrid cloud model. Cloud applications that base on a distributed architecture have to deal carefully with such dependencies and thus must be designed and developed accordingly.

Scalability: In the field of software technology, the term scalability describes the possibility of increasing performance or resources on demand. If an application receives higher access rates within a certain period, then it should be able to handle dynamic load variations. Traditional applications usually have been designed and developed to handle such situations and the load can be shared between different available servers. When applying cloud computing, applications do not need to be especially designed for scalability anymore because scalability is one of the main advantages of cloud computing and is managed by the cloud provider and its infrastructure.

Sustainability: In the special case for e-Government applications, sustainability affects not only the technical, but also the economic, legal, and organizational level. On technical level, it is important to develop the application independent from specific platforms or providers by relying on approved standards. This requirement additionally affects the economical level, as the missing opportunity of a provider change can have economic consequences. If vendor lock-in takes effect, economic advantages of other providers cannot be utilized. E-Government applications must particularly comply with given legislation. Since changes in legislative frameworks are occasionally possible, also the application, which is implementing the law, must be able to easily handle such situations. Additionally, also on organizational level appropriate precautions must be made for a sustainable use of e-Government applications in the cloud. In particular, applications should for instance not be designed for one municipality or public authority only, but instead in such a generic way to be available and re-usable also by other municipalities or public authorities.

Usability: Designing and developing usable applications does not define a requirement tailored to cloud applications only. Nevertheless, usability constitutes an important requirement that has to be considered during developing or designing online applications. Furthermore, every application – especially applications in the e-Government sector – should consider usability with high priority. This relates to the navigation through the application, readability, as well as the design of the entire user interface. Especially for e-Government applications, barrier-free access and WAI (Web Accessibility Initiative) conformity should be considered.

6.3.5.2 Organizational Requirements

In this section, several organizational requirements are listed, which need to be taken into account when designing or developing e-Government applications in the public cloud.

Availability: Availability constitutes an important requirement for e-Government applications since e-Government aims on 24/7 availability, offering citizens open office hours around the clock. For cloud applications, the cloud provider is responsible for general availability. Nevertheless, also cloud application developers must bear in mind certain criteria concerning availability. Cloud applications should be designed and developed in such a way that applications can be deployed and run redundantly.

Reliability: Reliability of software applications concerns the correct functionality of the application over a specific period. This requirement is not cloud computing specific but a more general criterion, which should be taken into account by developers during the complete software development

cycle. The more critical the application, the more reliable the application must work. Especially for e-Government applications, reliability is important because of the processing of sensitive data.

Transparency: Transparency is important for e-Government applications to show citizens that applications are working according to the law and are protecting citizens' rights. Transparency affects the development process of an e-Government cloud application and also their users. The process flows of an e-Government application should be transparent, hence the development of e-Government applications should be based on standardized interfaces. The use of interfaces offers possibilities to exchange implementations and take solutions of other vendors. For users, look and feel should remain unchanged when accessing the application. The functionality of an application should always be comprehensible.

Interoperability: E-Government applications should be developed in such a way that they comply with standards as much as possible to guarantee portability. However, interoperability is not only important within an application, but also when communicating with other applications. Hence, for communication between different clouds or cloud applications well-established standards should be relied on. Moreover, interoperability and portability provide e-Government services greater opportunities for re-use and thus better possibilities for contribution in a distributed and interconnected system or environment.

Governance: In the IT domain, the term governance has a strong relationship to compliance. While compliance rather focuses on adherence of external regulations such as laws (the requirement on compliance will be discussed in the next section), IT governance defines the observance of internal policies or strategies of organizations [Meyer et al., 2003]. This definition rather relates to enterprises than to public authorities, speaking of business goals in the public sector is not optimal though. Nevertheless, also public administrations or authorities define goals or strategies, which must be followed when adopting cloud computing.

6.3.5.3 Legal Requirements

Several legal requirements affecting the design and the development of e-Government applications in the public cloud are explained next.

Auditing and Logging: Logging or auditing refers to the systematic tracing or monitoring of processes or system properties. Basically, information about access or process steps is stored in log files (logging), which facilitates further investigations of a system (auditing). In traditional IT systems, log files are usually stored in the own computing center only and can only be accessed by system administrators. In cloud environments, this requirement cannot be met easily anymore as theoretically a log file could be stored distributed around the world physically located in different countries and on different machines. Additionally to system administrators, who have access to the application and thus to these log files, theoretically also the cloud provider itself has access to these files. Normally, log files should not contain sensitive data. However, in some special cases this might be necessary e.g., for auditing purposes or to achieve compliance with legal regulations. For that reason, e-Government applications in the cloud should be developed in such a way that, on the one hand, critical data are not stored in log files and, on the other hand, only authorized persons can access them.

Compliance: Generally, the term compliance describes the adherence to legal regulations or certain policies. Legal fields that are relevant for cloud computing and e-Government are data protection law, public procurement law, IT contract law, liability and warranty, or criminal trial law [Reichstädter, 2012]. Additionally, cloud applications probably must comply with specific national law in some cases or other international conventions. Since data protection plays a major role in the field of cloud computing it will be described separately next.

Data Protection: Besides security, data protection constitutes currently one of the most discussed topics in the area of cloud computing. Compliance with data protection regulations represents a key factor of e-Government applications. Distributed storage of personal data such as in public cloud environments usually violates existing national data protection regulations, at least in Europe. Usually, the requirement of having data stored in a specific location is just met on contractual level with the cloud provider. For example, it may be agreed that data may only be stored in certain countries [Catteddu and Hogben, 2009]. Such agreements are mostly contracted in so-called SLAs (service level agreements) between the cloud provider and the customer. In general, SLAs additionally may regulate various other things such as availability or support times.

6.3.5.4 Economic Requirements

This section summarizes economic requirements that influence the design and development of e-Government applications in the public cloud.

Profitability: Economic and business criteria play also an important role in e-Government. If old applications are transferred into the cloud or new cloud applications are developed, an according ROI (return on investment) must be given. For example, if existing applications can easily be run in internal infrastructures and own hosted data centers, there is probably no need for a migration into a cloud environment. The same thought is valid for applications that are used with low frequency and where no high load must be expected. This means for e-Government applications that the cost-benefit ratio must be within an acceptable value area. If e-Government applications are rarely used only, the costs for a new development or cloud migration are usually too high for being profitable.

Migration effort: The requirement of migration effort effects both newly developed applications and existing applications that should be transferred into cloud environments. During the development of cloud applications, efforts required for a possible transfer from one cloud provider to another one have to be considered. There are plenty of reasons for a necessary transfer, ranging from changes in price conditions to insolvency of the cloud provider and cohering cessation of service or support. If such scenarios become real, the migration effort must be minimal in order to be able to quickly restore availability of the cloud application. To keep the migration costs for public authorities as low as possible, the migration effort must also be taken into account when developing or transferring e-Government cloud applications. An unacceptable high migration effort can cause e-Government applications to be shut down if the cost-benefit ratio becomes too low.

6.3.6 Implementation Possibilities for E-Government Applications in the Public Cloud

This section introduces possible solutions for meeting the previously defined requirements for e-Government applications in the public cloud on an abstract level. Focus is especially put on technological possibilities. However, also organizational possibilities are discussed. The technologies discussed in this section are mostly state-of-the-art technologies. Additionally, current topics in research are investigated. Legal possibilities have been wittingly not considered as their enforcement usually anyhow requires technical or organizational means. The following matrix opposes the previously defined requirements for e-Government applications with the technical and organizational implementation possibilities. Table 6.2 illustrates which requirements can be addressed by which implementation possibility¹⁴. By listing these possibilities, policy makers, researchers, managers, or developers of the public sector are able

¹⁴The identified requirement of scalability is excluded in this analysis because high scalability and elasticity constitute one of the main advantages of public clouds. If load bottlenecks occur they can easily be resisted by the cloud provider's infrastructure. Hence, during application development the focus does not need to lie on this requirement.

to gain some quick information on how specific requirements can be addressed, when developing or migrating public cloud e-Government applications.

Table 6.2: Opposition of requirements and implementation possibilities

Implementation possibilities / Requirements	Anonymous Credentials	Standardization	Remote Logging	Anonymization / Pseudonymization	Cloud Cryptography	Distributed Storage	Trusted Computing	Metadata	Privacy and Policy Languages	HTML5	Back Ups or Duplication	Hybrid Cloud	Open Government	Open Source
<i>Confidentiality</i>	X			X	X									
<i>Integrity</i>	X				X		X	X						
<i>Availability</i>		X									X	X		
<i>Reliability</i>				X			X						X	
<i>Authenticity</i>	X			X	X		X							
<i>Transparency</i>		X	X					X	X				X	X
<i>Dependencies</i>		X						X				X		
<i>Migration Effort</i>		X	X							X	X			X
<i>Interoperability</i>		X								X				
<i>Scalability</i>														
<i>Auditing/Logging</i>			X	X	X	X								
<i>Sustainability</i>		X											X	X
<i>Compliance</i>	X		X	X	X	X		X	X				X	
<i>Data Protection</i>	X			X	X	X		X	X				X	
<i>Governance</i>		X						X	X		X	X	X	X
<i>Usability</i>										X				
<i>Profitability</i>		X											X	X

As can be seen from this matrix, numerous technical and organizational possibilities for fulfilling the requirements for a more secure cloud computing exist. Nevertheless, not all of these possibilities and solutions are already mature enough to counter all identified issues of cloud computing.

The listed requirements and implementation possibilities do not guarantee completeness. However, they can easily be extended according to specific needs or circumstances. In the following, both technical and organizational possibilities to meet the previously identified requirements are discussed in detail.

6.3.6.1 Technical Implementation Possibilities

The following list describes possibilities to fulfill or meet the previously defined requirements using technical means. It is further described why those technologies are able to fulfill certain requirements.

Anonymous Credentials: Anonymous Credentials have been designed to particularly preserve users' privacy. With the help of this technology it is possible to disclose only single or a sub-set of user attributes without revealing the complete identity. Additionally, user data can be released only for a certain amount of usages. Furthermore, anonymous credentials avoid tracking and linking of user activities. In contrast, such credential systems have the ability to force users to disclose certain attributes in every transaction. Popular representatives of this technology are *U-Prove* [Brands, 2000] and *Idemix* [Camenisch and Lysyanskaya, 2001].

The particular focus of these technologies on minimal disclosure of user attributes and privacy allows for easily meeting the requirements of compliance and data protection. By using anonymous credentials, only the least amount of personal data needs to be disclosed by a user. This feature

also helps in keeping data confidential and of integrity. Due to the special design of such systems, anonymous credentials enable authentication in a privacy-preserving manner.

Standardization: Like in nearly every technical field, standardization constitutes an important topic. This importance holds for cloud computing too. Standardization is key for achieving interoperability between different systems or implementations. Currently, the cloud landscape is still very heterogeneous. Nevertheless, a couple of standardization initiatives and working groups already exist and try to encourage the standardization of interfaces in the field of cloud computing. Heck and Müller [2010] give a good overview on the groups and committees that work on cloud computing interoperability.

Standardization efforts can help in meeting several requirements. For instance, the use of standards allows for making systems interoperable. Due to that, dependencies can be easier managed which in turn lowers migration efforts, when applications need to be ported. If applications are interoperable and can be migrated with low efforts, this may ensure sustainability and availability as e.g., applications can be easier deployed redundant.

Remote Logging: Log messages or log files are an integral part of every application because they provide information on the current system state and thus help finding errors in case of malfunction or unexpected behavior. In a distributed architecture such as clouds it can be reasonable not to store log files on the same system or in the same domain, which the application itself is running on or in, but rather send them to a remote and trusted server. This server stores the log information and can provide details on demand. The use of remote logging capabilities may also increase transparency and ensure compliance, as it might be forbidden to store sensitive log data in cloud environments.

Anonymization and Pseudonymization: When using anonymization, personal data are modified in such a way that it cannot be linked to a specific person anymore. This way, data can easily be processed anonymously. In contrast to anonymization, pseudonymization substitutes specific personal attributes that can be linked to a person with other attributes. This way, linkage can be avoided or at least aggravated. At this point, it is important to mention that data are not faked or falsified, but only the link to these data is substituted with another attribute. Data itself or the relation between data sets can be processed in the same way as if the original data was used. This further means that data can still be reliable or authentic. However, the main advantage of anonymization or pseudonymization is the possibility of treating users compliant to data protection regulations.

Cloud Cryptography: At the moment, it is impossible to securely store private data in the cloud if the cloud provider is not trusted, unless the data has been encrypted outside the cloud provider's environment. Current research on cryptography aims on overcoming this drawback by developing technologies that allow the storage and processing of sensitive data in the cloud. A typical example for such a technology is homomorphic encryption [Gentry, 2009] (cf. Section 7.3.2.7). With the help of this technology, mathematical operations such as addition or multiplication can be simply carried out on encrypted data. Another cryptographic possibility for processing sensitive data confidentially in the cloud is proxy re-encryption [Ateniese et al., 2006] (cf. Section 7.3.2.6). By applying proxy re-encryption, a semi-trusted proxy can alter a ciphertext, which has been encrypted for one party, so that it may be decrypted by another party. Thereby, the proxy neither gains access to the plaintext of the data nor to the decryption key.

Distributed Storage: If data are processed in the cloud, data are usually stored in the cloud provider's environment. In principal, the cloud provider has always access to the stored data, which is mostly not acceptable due to data protection regulations. Therefore, research approaches focus on distribution of the data to be stored, either distributing the data between different systems or even between different cloud providers. This way, access to the data or reconstruction becomes much more difficult since one cloud provider can only see parts of the data. Examples of distributed file systems are given in Zhang et al. [2010]. Another approach was published by Buyya et al. [2010].

Trusted Computing: The general idea behind trusted computing is that computers work and behave as expected or as usual Müller [2008]. Such a behavior is assured by special software or hardware. The core component of trusted computing systems defines the so called trusted platform module (TPM). This module is responsible for assuring and verifying the integrity of a system component or software using cryptographic methods. Since cloud computing is heavily based on virtualization, traditional trusted computing concepts for assuring integrity, reliability, or authenticity of software cannot be used. A solution for this problem are virtualized TPMs which are introduced in Blum and Krikken [2010] for example. This implementation possibility has also been mentioned in Zhang et al. [2010].

Metadata: In general, the term metadata specifies data containing information about other data. Metadata can also be useful in cloud computing, especially to check what happens to the data in the cloud. An example of metadata in the cloud could be positioning data to guarantee or verify that data are not stored in another country according to data protection regulations. Metadata can also be used to model a certain trust framework, which can meet governance requirements. An approach for a location control model in the cloud can be found in Fatema et al. [2014].

Another example for metadata is the use of so-called sticky policies Pearson and Mont [2011]. Sticky policies define who is allowed to access the data or how the data can be processed. These policies are attached transparent to the data and only appear together with the data in the system. Hence, sticky policies can also be an interesting approach for assuring compliance with data protection rules.

Privacy and Policy Languages: Privacy or policy languages are especially constructed for the modeling of general policies or specific privacy and data protection policies for automatic processing. The use of such kind of markup languages can also be useful for cloud applications, as data protection policies can be checked automatically and SLAs on organizational level can be omitted. An example for a policy language is XACML¹⁵ (eXtensible Access Control Markup Language), a representative for a privacy language is EPAL¹⁶ (Enterprise Privacy Authorization Language).

HTML5: HTML5 [Berjon et al., 2014] is currently the latest version of HTML. Although HTML5 is still in its development phase, it offers much more functionality compared to its predecessors. The enhanced functionality of HTML5 renders the use of various browser plugins unnecessary. Ingthorsson [2010] sees HTML5 as an emerging technology for cloud computing. While most applications on mobile gadgets (e.g., smartphones, etc.) are downloaded to the device, HTML5 offers the possibility to run the application directly in the cloud. This lowers migration efforts to other platforms. Moreover, especially usability can be increased since HTML5 supports the developer in creating usable solutions.

6.3.6.2 Organizational Implementation Possibilities

The following list describes possibilities to fulfill or meet the previously defined requirements using organizational means. It is further described why those organizational possibilities are able to fulfill certain requirements.

Back Ups or Duplication: Relevant cloud computing literature frequently addresses the vendor lock-in issue. Avoiding vendor lock-in would be a reason to additionally deploy and run a cloud application at a second cloud provider using redundancy. Another reason to run the same application at different providers would be availability. Although cloud providers offer and guarantee high availability of their services using SLAs, in case of a breakdown of the provider's systems only penalty

¹⁵<http://www.oasis-open.org/committees/xacml>

¹⁶<http://www.zurich.ibm.com/pri/projects/epal.html>

fees can be claimed by the customer but the application still remains offline. To overcome such an issue, installing a back-up application at another cloud provider would be an adequate mean.

Hybrid Cloud: Concerning requirements related to security and privacy, the use of private or community clouds has been identified to be a proper choice for cloud based solutions in the public sector. However, with respect to economic aspects and organizational efforts public clouds are advantageous. Since cloud computing is based on a distributed architecture, advantages of individual cloud models can be combined. Hence, the setup of a hybrid cloud defines a proper model for fulfilling certain e-Government cloud application requirements, such as governance, availability, or dependency management.

Open Government: In open government, public authorities or the government itself make data publicly available Lathrop and Ruma [2010]. The idea behind this offering is to increase transparency for citizens on the one hand and to boost innovation on the other hand. For example, the private sector can take up the data to offer innovative applications based on these open data. In contrast to that, in the past such data was mostly especially protected and secured from unauthorized access. The simple release of data weakens a couple of requirements for cloud computing and additionally offers possibilities to create and develop new applications based on these data. This means, before putting efforts in meeting certain e-Government cloud application requirements, it should be analyzed and balanced whether the data to be processed in the application are really worth to be strictly protected or not. The public release of open government data can also help in developing sustainable solutions.

Open Source: Usually, the source code of software issued under an open source license is freely accessible and can be easily amended or altered without paying license fees Koper [2008]. This type of software distribution model is properly applicable for e-Government applications [Posch et al., 2010]. Due to free software access, citizens can evaluate the software and decide for themselves whether it is secure enough to process their sensitive data. Taking this software release approach also for governmental cloud applications, certain requirements such as transparency or sustainability could be met by this organizational possibility.

6.4 Cloud Computing in E-Government in Europe

The adoption of cloud computing in e-Government is not only a vision, it already became reality. Many countries or cities, especially across Europe, have already adopted cloud computing solutions in the public sector or are planning to do so [Wyld, 2009]. In the next subsections, based on the work of Zwattendorfer et al. [2013b] some details on governmental cloud computing adoption within eight European countries, which currently also have a well-established and successful e-Government infrastructure in place, are given.

6.4.1 Austria

Austria or Austrian cities have not adopted cloud computing in their public services yet. However, the *Platform Digital Austria* of the Austrian federal chancellery (cf. Section 2.2.2.1) has published a position paper for the use of cloud computing in the public sector in 2012 [Reichstädter, 2012]. This position paper especially covers legal, organizational, economic, and technical aspects, as well as opportunities and risks of cloud computing for public sector use. According to this paper, Austrian e-Government applications might be deployed in a private, community, or public cloud in the future. Moreover, Reichstädter [2012] sees all service levels applicable. IaaS could be used for archiving or backup purposes. By relying on PaaS, a particular platform supporting an easy applicable framework for developing e-Government

cloud services is imaginable. On software level, future cloud services might include specific collaboration suites for public authorities or more security related services such as Identity as a Service [Roessler, 2010].

6.4.2 Denmark

The local government of Denmark started discussions on using cloud computing in the public sector already in early 2009 [Epractice.eu, 2009]. Moreover, according to KPMG [2012] Denmark is one of the leading countries regarding the adoption of cloud computing in the public sector. For instance, in 2011 a Danish municipality planned to use Google Apps Services such as calendar or e-mail in their school systems [Datatilsynet, 2011]. In addition, a Danish procurement organization of a Danish municipality moved procurement services into the cloud in 2011 [Datacentres.com, 2011]. Although Denmark still struggles with security and privacy issues [KPMG, 2012], the Danish data protection agency still judged the cloud service of Microsoft – Office 365¹⁷ – to be compliant with the EU and Danish legislation [Albertazzie, 2012]. In addition, *cloud.dk* offers public cloud services fully compliant with the Danish data legislation.

6.4.3 Finland

According to Yläupa [2011], Finland currently has no common strategy on cloud computing in the governmental sector. The government has only started an explanatory research for centralizing ICT services where cloud computing could play a major role. Particularly, the aim of such centralized ICT infrastructure is bundling maintenance and support tasks as well as monitoring and help-desk services. Referring to Yläupa [2011], no statistics exist which public authorities eventually use cloud computing services already. However, the Finnish government particularly emphasizes cloud computing in its report "Productive and Innovative Finland – Digital agenda for the years 2011-2020" [Frelle-Petersen et al., 2011].

6.4.4 France

France is currently one of those countries that favor the development and installation of a nation-wide cloud for governments, a so-called G-Cloud (Governmental Cloud). France started its development of the G-Cloud named "Andromeda" in 2011 [Pérez San-José et al., 2012]. This G-Cloud, which is - in this particular case - a IaaS platform for governments, is currently set up and implemented by the two companies Orange¹⁸ and Thales¹⁹ [Auffray, 2012]. The main aim for developing an own G-Cloud in France are data protection and legislative issues. A cloud especially developed for France can guarantee full compliance with national law in terms of data protection and security [Pérez San-José et al., 2012]. Such compliance may not be achieved e.g., by adopting US-based services. Furthermore, Accenture is currently building up some kind of G-Cloud for the French *Directorate of Legal and Administrative Information* (DILA). This cloud shall offer French citizens fast and performing access to French public services [Zacks Equity Research, 2012].

6.4.5 Germany

Cloud computing is one of the main pillars of the ICT strategy of the German federal government [Federal Ministry of Economics and Technology (BMWi), 2010]. This strategy has been published by the *Federal Ministry of Economics and Technology* in 2010 and aims on the digital future in Germany until 2015.

¹⁷<http://www.office365.com>

¹⁸<http://www.orange.fr>

¹⁹<http://www.thalesgroup.com>

Focusing on cloud computing, the objective is to facilitate and foster the development and installation of cloud computing services. In particular, both small- and medium-sized enterprises and the public sector should take advantage of cloud computing as fast as possible. The challenges (e.g., data security, quality assurance, easy integration, open standards, etc.), which need to be addressed for adopting cloud computing in Germany, are targeted in the so-called "Cloud Computing Action Programme" within this ICT strategy. These challenges particularly arise when adapting existing IT concepts to the specific requirements of cloud computing.

6.4.6 Ireland

Ireland anchored cloud computing in their national governmental strategy. This strategy of the Irish government with the name "Technology Actions to Support the Smart Economy" was introduced by the *Ministry of Energy and Communications* and the *Ministry of State* in 2009 [Irish Government, 2009]. In more detail, Ireland sees cloud computing as one of the key drivers for economic growth in Ireland. They estimate high reductions in server and energy costs by expecting high value job generation at the same time [Robinson et al., 2010]. Therefore, they released a separate "Cloud Computing Strategy" paper in 2012 [Robinson et al., 2010]. They plan several governmental services based on cloud computing offered to their citizens, aiming on increased productivity by decreasing public expenditures at the same time [Robinson et al., 2010]. Finally, the Irish government provided some kind of guidance for businesses when adopting cloud computing. This guidance entitled "SWiFT 10: Adopting the Cloud – Decision Support for Cloud Computing" consists of a set of standards which shall help businesses to lower obstacles when moving services into the cloud [Robinson et al., 2010].

6.4.7 Spain

Pérez San-José et al. [2012] did a thorough analysis on cloud computing in the Spanish public sector. This study concludes that there is still limited adoption of cloud computing in the public sector in Spain. Reasons are information integrity, privacy, and legal concerns. The central government is not the driving force behind cloud computing adoption but moreover local governments are. Local governments have a limited financial capacity in contrast to the central government and here cloud computing can tremendously help in saving costs. However, a lot of governments have adopted cloud computing already since more than three years. According to Pérez San-José et al. [2012], the favored deployment model in Spain is the private cloud (app. 58%), followed by the public cloud (app. 31%), and the hybrid cloud (app. 17%). The private cloud is favored because of higher control in terms of security and privacy. The community cloud model is generally seldom in Spain because it targets a fusion of specific sector applications (e.g., health), which seems to be undesired. [Pérez San-José et al., 2012]

6.4.8 United Kingdom

In 2011 the UK government published an ICT strategy, which also covers the topic on cloud computing [UK Cabinet Office, 2013]. This strategy particularly involves the implementation and installation of a G-Cloud in the UK. The main objectives of this G-Cloud are reducing ICT costs for governments, optimizing the use of data center infrastructure, and increasing public sector agility [UK Cabinet Office, 2013]. In fact, the installation of this G-Cloud is an iterative process. The first step, the realization of the so-called *CloudStore*²⁰, has been achieved in 2012. This CloudStore offers infrastructure, software, platform, and specialist services which can be bought online. [UK Cabinet Office, 2013]

²⁰<http://gcloud.civilservice.gov.uk/cloudstore>

6.4.9 Comparison across Europe

In this subsection, between the eight European countries it is compared whether cloud computing has been anchored in a national governmental strategy or not. Moreover, it is elaborated whether cloud computing has been adopted more on national, regional, or municipality level. It is further listed, which cloud computing deployment models (public, private, community, or hybrid cloud) or service models (IaaS, PaaS, SaaS) are applied in the public sector. However, it is not distinguished whether those models are already in place or it is just planned by the individual country to adopt them. Finally, a sample on which government-related services were or are planned to be moved into the cloud are listed.

The comparison is based on a thorough literature review and web research, involving the countries Austria, Denmark, Finland, France, Germany, Ireland, Spain, and the UK. Table 6.3 shows the comparison of governmental cloud computing between these countries.

As can be seen, five of the eight investigated countries have anchored the adoption of cloud computing in the public sector in some kind of national strategy. For the remaining three countries, cloud computing is individually applied by local governments such as municipalities or cities.

Two of the evaluated countries have already adopted cloud computing and hence are in an executional stage. The other countries are still in the developing or planning phase. All countries, which have manifested cloud computing in some national strategy, are mostly still in the planning phase. However, the UK has already some governmental cloud services running. Nevertheless, the full implementation of their national cloud computing strategy will still take another few years.

Most countries plan the adoption of cloud computing in the public sector on national level. The reason for this is probably that security and privacy issues can be easier faced. In particular, Austria, France, Spain, and the UK are planning or are already developing a so-called G-Cloud (Governmental Cloud), a nation-wide private or community cloud. For Finland and Germany no further information was available to compare them against the other countries.

The most frequently planned and developed cloud computing deployment models amongst the evaluated countries are the private and the community cloud. This is because many of those countries tend to implement a national G-Cloud. The use of public clouds is also common across those countries. However, public clouds are and will be only applied if certain security and privacy requirements can be met or even be neglected.

When comparing cloud computing service models, 50% of the evaluated countries rely on the most common service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). France will set up a G-Cloud and focuses on IaaS. However, public authorities, which will take advantage of the offerings of this G-Cloud, will still be able to provide cloud computing services on other levels, i.e., PaaS or SaaS. For Denmark, information could only be found on the application of SaaS services.

Finally, in Table 6.3 it was compared which services might be or are already moved to the cloud. The list is not exhaustive, so only the most important services are named. Applying IaaS, many countries think about cost-effective backup and archiving solutions. Additionally, IaaS can also play a major role for open data initiatives. For PaaS, the evaluated countries tend to offer some kind of cloud framework for e-Government solutions. This framework can be further taken as a basis for local governments or cities, where individual e-Government applications could be developed to. Finally, the most frequent SaaS services to be moved to the cloud are e-mail services. In addition, many countries think about the use of collaboration services or office suites in the cloud.

Table 6.3: Comparison of cloud computing in e-Government across eight European countries [Zwattendorfer et al., 2013b]

Country	Cloud Computing anchored in a National Strategy	Cloud Adoption	Cloud Adoption Level	Cloud Deployment Models	Cloud Service Models	e-Government Sample Services
<i>Austria</i>	Yes	Planned	National Regional City	Public Cloud Private Cloud Community Cloud	IaaS PaaS SaaS	- Backup/Archiving - Cloud Framework for e-Government applications - Collaboration Suites - Identity as a Service
<i>Denmark</i>	No	Planned Executional	Municipality	Public Cloud Private Cloud Community Cloud	SaaS	- E-Mail - Procurement
<i>Finland</i>	No	Planned				
<i>France</i>	Yes	Development	National	Community Cloud	IaaS	
<i>Germany</i>	Yes	Planned				
<i>Ireland</i>	Yes	Planned	National	Public Cloud Private Cloud Community Cloud	IaaS PaaS SaaS	- Open Data - Public Information Repositories - Collaboration Suites - E-Mail
<i>Spain</i>	No	Planned Executional	National Regional City	Public Cloud Private Cloud Community Cloud Hybrid Cloud	IaaS PaaS SaaS	- E-Government Services - Open Government - Citizen participation - E-Mail - Storage/Backup - Office and Collaboration
<i>UK</i>	Yes	Development Executional	National	Private Cloud Community Cloud	IaaS PaaS SaaS	- E-Mail - Office - Customer Relationship Management

6.5 Cloud Computing in E-Government beyond Europe

The following subsections – based on the work of Zwattendorfer and Tauber [2012c, 2013] – briefly explain national strategies and cloud adoptions of various countries beyond Europe. These explanations will show that most countries stick to the highly controlled and less economical private cloud model for their governmental applications.

6.5.1 America

In the following, two American countries are elaborated.

6.5.1.1 Canada

In 2009 the CTO at *Public Works Government Services Canada* published the document "Cloud Computing and the Canadian Environment" [Danek, 2009] dealing with Canada's cloud adoption strategy and balancing cloud benefits (e.g., reduction of operating costs and improved maintainability) with cloud risks (e.g., privacy and personal data protection). Based on that, the Canadian government was offering a community cloud for certain services (payment, pension, etc.) in 2010. The idea was to use IaaS for virtual storage, PaaS for commoditized hosting of cloud applications, and SaaS for virtual office provision and internal collaboration [Robinson et al., 2010].

6.5.1.2 USA

Currently, the USA is one of the leading countries in cloud computing adoption. Several services, especially e-mail services, have already been moved to the cloud. For instance, the cities of Los Angeles, Washington, and Carlsbad shifted the e-mail services of their employees to the cloud [West, 2010]. Another popular example for US governmental cloud services is *Apps.gov*, where cloud solutions are offered by the US general service administration (GSA) for public sector customers. In general, the US government forecasts in its "Federal Cloud Computing Strategy" enormous cost savings potential [Kundra, 2011]. Therefore, 40% of the existing data centers should be closed and substituted by modern cloud computing technologies. The general aim of the US cloud computing strategy is taking advantage of cloud computing and drive forth its adoption in the public sector. [Kundra, 2011]

6.5.2 Australia

The Australian government published a strategic paper on cloud computing in 2011 [Australian Government, 2011]. The main policy of this paper is that "*agencies may choose cloud-based services where they demonstrate value for money and adequate security*" [Australian Government, 2011]. Basically, the hosting of cloud computing services should decrease the need of separate data centers for Australian agencies. Some agencies have already piloted cloud computing applications (eTax, electronic lodgement system, etc.) [Australian Government, 2011]. However, the cloud computing strategic paper foresees more mature cloud adoptions based on a risk-managed approach. Depending on the classified risk level of a particular service or application, the services may be deployed in a public, private, or community cloud. From 2011 onwards, low risk services should be deployed in a public cloud, medium risk services in outsourced private clouds, and high risk services in community clouds for the government. [Australian Government, 2011]

6.5.3 Asia

In the following, eight Asian countries are briefly elaborated.

6.5.3.1 China

China does not follow a particular and nation-wide cloud computing strategy. Only some cities such as Dongying or Wuxi have started some cloud computing initiatives. These initiatives do not especially aim on e-Government adoption. They furthermore should help less financially strong start-ups to set up their businesses and thereby strengthen the economic growth of China. [Wyld, 2009]

6.5.3.2 India

India currently has a limited adoption on cloud computing. The Indian states Jammu and Kashmir offer governmental services such as the issuance of birth certificates through the cloud. Although cloud computing adoption is currently low, significant interest on further adoption is given across the country. Before achieving that, security and privacy issues as hindering factors must be met. [Chandrasekaran and Kapoor, 2011]

6.5.3.3 Japan

In contrast to China and India, Japan has already started a big governmental cloud initiative. Within this initiative, a private cloud hosting all Japanese public services should be developed. The cloud is named "Kasumigaseki" and is part of the governmental *Digital Japan Creation Project*. The aim of this cloud is to decrease development and operational costs for services and to increase performance of applications. Deployment of this cloud should happen step-by-step and should be completed in 2015. [Ng, 2009]

6.5.3.4 Malaysia

In 2009 Malaysia joined an open source cloud computing test platform. The aim of this join was to gain experience for establishing such a platform for the whole country in future. Currently, cloud adoption in Malaysia is low. The Malaysian e-Government portal and some national archive databases rely on private cloud elements. Nevertheless, cloud computing can be seen as one of the driving technologies in the Malaysian national ICT initiative. The aim is being more efficient by decreasing costs and increasing transparency at the same time. [Chandrasekaran and Kapoor, 2011]

6.5.3.5 Singapore

At the end of 2011 Singapore started an auction for the development and set-up of a private cloud. Like for the UK (cf. Section 6.4.8), this cloud should form a G-Cloud to map the current governmental infrastructure as a cloud model and thus to take advantage of all cloud computing benefits. In addition, this cloud should offer central public services of Singapore. Nevertheless, during the development security and public services requirements must be taken into account. [Guo, 2011]

6.5.3.6 South Korea

Referring to Chandrasekaran and Kapoor [2011], the communication commission of South Korea is going to budget hundred millions of dollars for cloud-based infrastructures in Korea. The cloud-based infrastructures should support both the government and the private sector. On the one hand, the aim of building such infrastructures is to support smaller businesses to enter the global market. On the other hand, ICT costs of the public sector shall be decreased about 50%. [Chandrasekaran and Kapoor, 2011]

6.5.3.7 Thailand

Also Thailand has ambitions to build and set up a private cloud for public services. By the help of this private cloud, small- and medium-sized public authorities with limited budget should get facilitated access to e-Government. The cloud should be deployed and operated by Thailand's *Government Information Technology Service (GITS)*. [Hicks, 2009]

6.5.3.8 United Arab Emirates

According to Elbadawi [2011], also the United Arab Emirates (UAE) plan to launch a governmental cloud especially for federal and local governmental entities. This cloud should be built as a community cloud model, bundling also existing services. In particular, infrastructure and software shall be provided as a service. The use of cloud computing also fits the strategic plan and vision of the UAE. In there, collaboration between government entities should be fostered, public services should be improved, and the costs of public services should be cut down. [Elbadawi, 2011]

6.6 Chapter Conclusions

Cloud computing and its flexible business model of consuming IT resources such as computing power or data storage just on demand promises a lot of benefits and advantages. These advantages also the public sector and governments can benefit from. Hence, cloud computing is already on the agenda of governmental policy and decision makers. Additionally, various countries have already adapted their IT strategies to support cloud computing for their governmental and public services. However, within the public sector the private cloud model currently constitutes the dominant deployed approach. Although this model offers high control it does not take full advantage of the economic benefits of cloud computing. Therefore, it was shown that public clouds are worth more than a peek for e-Government because of their tremendous cost savings potential. By now, the reader should have a basic understanding of the cloud computing concepts and its benefits, which can help governments to save costs by providing more flexible and mature services and applications at the same time.

However, the move of e-Government services – if sensitive data are processed – into the cloud is not trivial, in particular when aiming on migrating or developing applications for the public cloud. Although the public cloud has the highest cost savings potential it can bring up new obstacles since the public cloud cannot be considered completely trustworthy. In the next chapters, the areas of cloud computing and electronic identity are combined. Focus is put on the migration of existing e-Government concepts such as identity management systems from trusted environments into semi-trusted environments e.g., the public cloud. By applying such a migration, the complete bandwidth of cloud computing benefits can be brought into the electronic identity and thus into the e-Government domain.

Chapter 7

Electronic Identity and Cloud Computing

Unique identification and secure authentication are essential processes in various areas of application e.g., in e-Government, e-Health, or e-Business. During the past years several identity management-systems and models have evolved. Many organizations and enterprises or even countries for their national eID solutions rely on identity management-systems for securing their applications. Since more and more applications are migrated into the cloud, secure identification and authentication are also vital in the cloud domain. However, most cloud service providers rely on weak authentication mechanisms such as username/password schemes only.

In this chapter, the topics of cloud computing and electronic identity are combined. First, it is discussed how highly secure national eID solutions can be used for unique qualified identification and authentication at different cloud service providers. This offers cloud service providers the possibility to penetrate market areas where higher security requirements for identification and authentication must be met (e.g., the e-Government or e-Health sector). Second, it is illustrated how existing identity management-systems could be moved into the public cloud by still preserving citizens' privacy. This is illustrated by showing three distinct approaches using different cryptographic technologies. The best approach is applied to the Austrian eID system, thus moving MOA-ID and several other relevant components into the public cloud as a sample use case. Finally, a new user-centric identification and authentication model is proposed, which is particularly applicable for semi-trusted environments (in terms of data protection and privacy) such as the public cloud. The model allows the usage of both server-side and client-side approaches for eID solutions by still putting users under full control of their data, i.e., providing selective disclosure in both approaches.

This chapter is structured as follows. In Section 7.1 different cloud identity models are discussed that have already evolved over time. In Section 7.2 the *Identity to the Cloud-Model* is applied by showing how various national eID solutions can be used for secure cloud authentication at SaaS applications. How existing identity management solutions and systems using eIDs can be ported into the public cloud is shown in Section 7.3. Thereby, the complete Austrian eID system is migrated into the public cloud by keeping the same level of security and privacy for Austrian citizens as in the current system. Finally, a user-centric *Identity as a Service*-architecture for eIDs enabling selective attribute disclosure is proposed.

7.1 Cloud Identity Models

Given the increasing number of cloud applications, also in the field of e-Government, identification of users gains also more and more importance in the field of cloud computing. Hence – similar to the conventional identity models discussed in Section 3.3 – different cloud identity models have already been defined to cover new requirements particularly relating to cloud computing. The main distinctive criterion between these cloud identity models is the entity, which operates the identity provider in relation to the cloud application. Gopalakrishnan [2009]; Cox [2012]; Goulding [2010]; Cloud Security Alliance [2011] classify such cloud identity models in their publications. Classification criteria are mainly how and where identities are managed.

Gopalakrishnan [2009] concludes that three different identity management patterns in the cloud can be distinguished. Within the first identity management pattern (*Trusted IdM Pattern*), the identity management system is running within the trusted domain of the cloud provider, which is also hosting the application to be secured by the identity management system. According to Gopalakrishnan [2009], this pattern is intended for smaller and less scalable cloud models such as private clouds. In contrast to that, the second identity management pattern (*External IdM Pattern*) is intended for public clouds, which have high scalability. In this pattern, the identity management system is external to the cloud provider's domain. Identity data and attributes are provisioned through a well-defined protocol such as SAML (cf. Section 3.5.2). The last and most flexible proposed identity management pattern is the so-called *Interoperable IdM Pattern*. In this pattern, a central identity management system is capable of various authentication technologies and is serving multiple identity consuming service providers.

Cox [2012] focuses on public clouds in his identity model classification. In his opinion, identity management in private clouds is obvious, as the identities are managed by the private cloud's organization on their own and no trust relationship to external providers is required. Cox [2012] actually defines four different models and particularly pays attention for provisioning and de-provisioning of users or identities respectively. In the first model, the cloud service provider generates and manages the identities for the enterprise. There is no external connection to e.g., an enterprise data source. The second model of Cox [2012] deals with synchronization. Thereby, the identity management system of an enterprise is synchronized with the user management of the cloud service provider. In the third model, identities are federated. This means that identities are still managed by the enterprise but are consumed by the cloud service provider. Similar to the *Interoperable IdM pattern* of Gopalakrishnan [2009], Cox [2012] proposes a unified model implementing features of the three other described models as a fourth identity model for the cloud.

Also Goulding [2010] classifies such cloud identity models in his whitepaper. The models are based on three use cases. The first model serves the use case of extending the enterprise identity management system up to the cloud. The second model deals with the use case of securing cloud services with an enterprise identity management system. In the third model, identity services are delivered to various applications down from the cloud.

In addition to those classifications, also the Cloud Security Alliance [2011] discusses three identity architectures for the cloud. In the so-called *hub-and-spoke* model identities are managed by a central broker or proxy, which serves multiple identity and service providers. In the *free-form* model, the service provider itself is responsible for managing several and disparate identity providers. The third model described by the CSA constitutes a hybrid model, which synthesizes advantages of the *hub-and-spoke* model and the *free-form* model.

In the following, the different identity models described before are taken as a basis to classify cloud identity models, which have already been deployed in several cloud computing environments. In addition, advantages and disadvantages of the individual models are listed. A detailed overview of cloud identity management-models is given in Zwattendorfer et al. [2014].

7.1.1 Identity in the Cloud-Model

The *Identity in the Cloud-Model* constitutes the simplest cloud identity model. In this model, the cloud service provider, which hosts the cloud application, also acts as identity provider. This means that the cloud service provider has its own user management, which is used for identification and authentication at its cloud applications. Hence, identity data are stored *in the cloud*. Figure 7.1 illustrates the *Identity in the Cloud-* model.

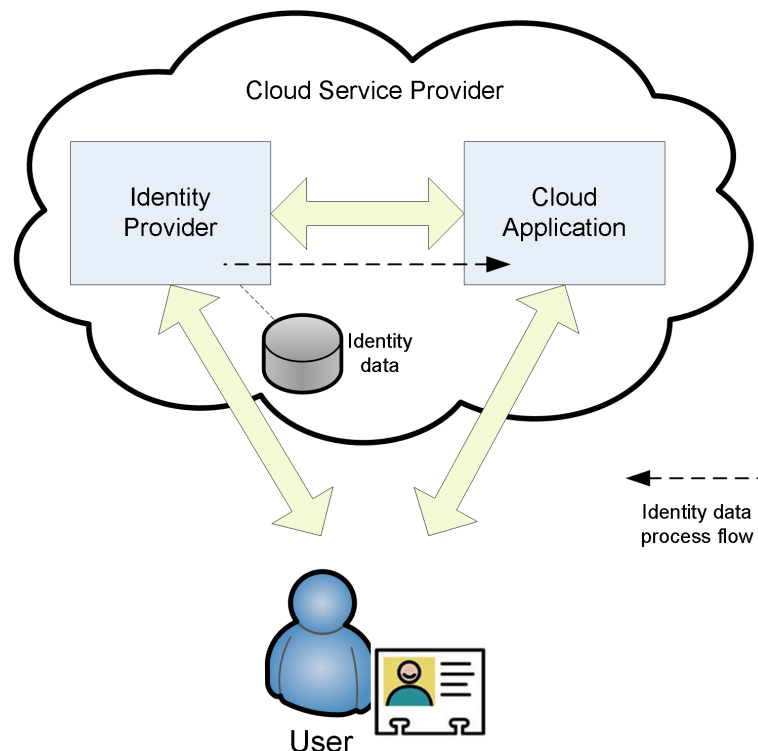


Figure 7.1: Identity in the Cloud-Model [Zwattendorfer et al., 2014]

This model can be seen as a special case of the traditional isolated identity model described in Section 3.3.1, where the identity provider and service provider define the same entity for this cloud case. This model has been also discussed by Gopalakrishnan [2009] or Cox [2012]. Typical practical and already deployed examples of this model are the cloud service providers *Google* or *Salesforce.com*. Both cloud service providers host, maintain, and offer their own user management for their Software as a Service (SaaS) applications.

The advantage of this cloud identity model is that organizations can just rely on the existing user management of the cloud service provider. This saves costs and maintenance efforts as no separate user management is required and accounts are created and maintained directly at the cloud service provider, which also hosts the organization's applications. However, this transfer of responsibility to the cloud service provider means also less control for the organization on identity and user data. Additionally, transfer of identity data to the cloud service provider or synchronization (e.g., as discussed by Cox [2012]) cannot be easily achieved because the cloud service provider might rely on different data models in its storage systems.

7.1.2 Identity to the Cloud-Model

The *Identity to the Cloud-Model* actually puts the traditional central identity model of Section 3.3.2 into the cloud domain. In the traditional case, the user management is outsourced by the service provider to an external identity provider. The only difference in the cloud identity model is that the service provider

is cloud-based and not only simply web-based. In addition, it is assumed that the identity provider is not cloud-based equally as in the traditional model. The scenario of a fully cloud-based identity provider will be considered in the next Section 7.1.3. However, Figure 7.2 illustrates the *Identity to the Cloud-Model*.

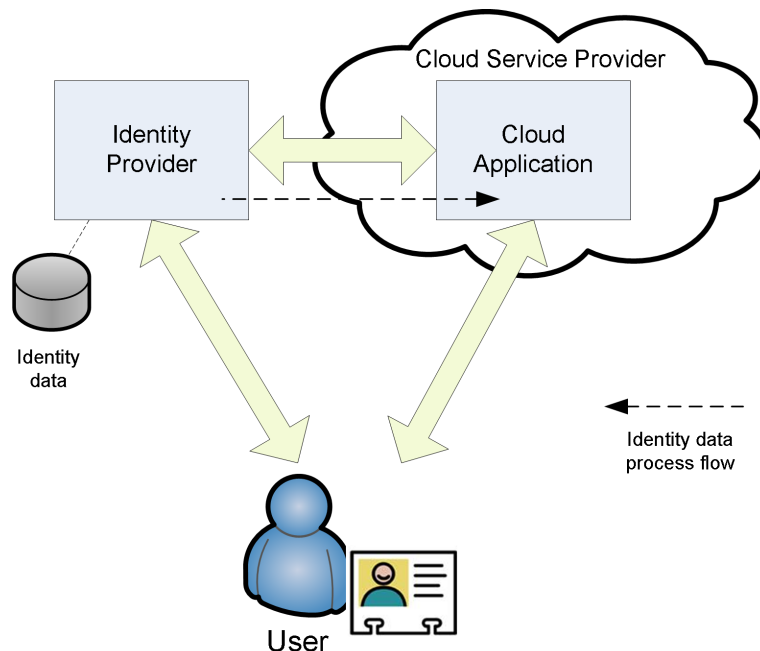


Figure 7.2: Identity to the Cloud-Model [Zwattendorfer et al., 2014]

The identity provider is responsible for the complete user management, such as provisioning or de-provisioning of identities, user authentication, etc. The cloud service provider is responsible for the cloud application only and just consumes identity data or information respectively from the identity provider. In other words, identity data are transferred *to the cloud*. Transfer of identity data between the identity and the cloud service provider is usually carried out based on well-defined interfaces and standardized protocols. Such protocols dealing with the secure exchange of identity and authentication data are e.g., SAML, OpenID, or OAuth (cf. Section 3.5).

Many existing cloud service providers, in particular public cloud providers such as *Google* or *Salesforce.com*, rely on such interfaces or protocols for external identity provisioning. For instance, both mentioned cloud service providers rely on SAML and OpenID for their identity provisioning or so-called single sign-on (SSO) interfaces. In contrast to *Salesforce.com*, *Google* additionally allows external authentications via OAuth. The use of such interfaces does not only allow the implementation of the traditional central identity model but moreover enables the application of the federated identity model described in Chapter 8.

When applying this model, advantageous is the possibility to re-use existing identity management systems (e.g., an internal identity management system of an organization or enterprise) for external identification and authentication at cloud providers and cloud services. In contrast to the previously described *Identity in the Cloud-Model*, no new user management at the cloud service provider or any migration to the cloud service provider is required. While the application or service is operated in the cloud, the user management stays under full control of the individual organization. In contrast to that, an issue might be interoperability (e.g., technical or semantic interoperability). Many cloud service providers, which offer SSO interfaces for external identification or identity federation, rely on standardized protocols. Although standardized protocols should actually guarantee technical interoperability, the implementations of such protocols may have a different behavior as shown in Zwattendorfer and Tauber [2012a]. In addition, the respective cloud service provider might not support the desired identity protocol for external authentication, which could cause additional implementation efforts and costs at the organization's or

enterprise's site. Semantic interoperability constitutes another issue, as user attributes of the external identity provider might not be understood by the cloud service provider. Hence, a thorough attribute mapping between the identity provider and the cloud service provider is required.

7.1.3 Identity from the Cloud-Model

Within the third introduced cloud identity model identities are provided from an identity provider, which fully resides in the cloud. In fact, identities are provided as a service *from the cloud*. Therefore, the proposed model can also be seen as an *Identity as a Service-Model* [Emig et al., 2007]. Figure 7.3 illustrates the so-called *Identity from the Cloud-* model.

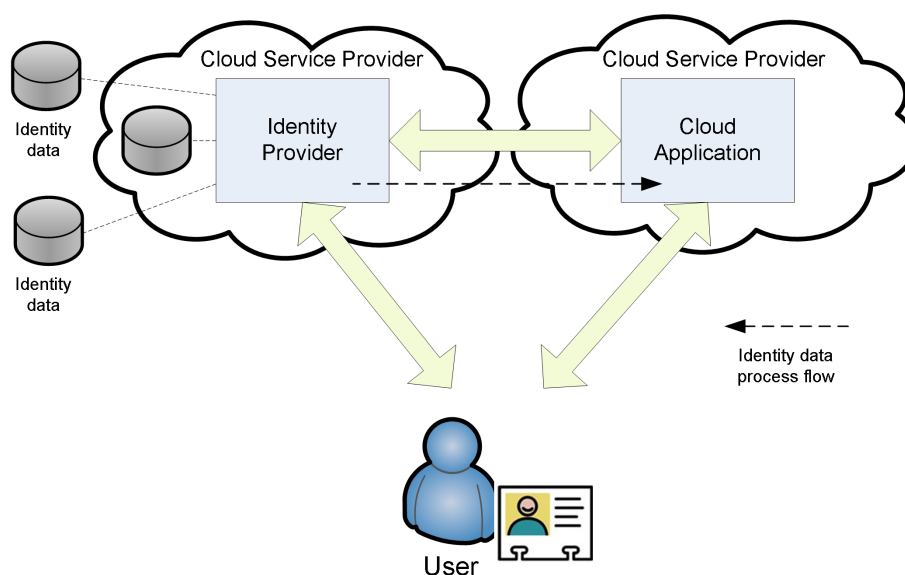


Figure 7.3: Identity from the Cloud-Model [Zwattendorfer et al., 2014]

In this model, both the identity provider and the application are operated in the cloud. Contrary to the *Identity in the Cloud-Model* of Section 7.1.1, the identity provider need not necessarily be operated by the same cloud service provider that also hosts the application. Needless to say that still just one cloud service provider can operate both, the identity provider and the application. However, the precondition is that the user management of the identity provider is separated from the application's cloud service provider.

Basically, this cloud identity model is independent of the underlying cloud deployment or operational model. In fact, this *Identity as a Service-Model* can be operated in a public, private, or community cloud. Due to the interconnection of different cloud deployment models (the cloud model used for operating the identity provider might be different than the cloud model for hosting the application), this cloud identity model can also be seen as hybrid cloud model. However, although within the illustrating Figure 7.3 only cloud applications are shown acting as identity consuming services, this *Identity as a Service-Model* can also be applied to traditional web- based applications of service providers.

Besides cost advantages and less maintenance efforts due to the outsourcing of identity management tasks into the cloud, the main advantage of this model is the separation of the cloud service providers. I.e., the cloud service provider for the application is usually different to the cloud service provider acting as identity provider. This allows organizations or enterprises an individual selection, which service provider they are going to trust to host and maintain their user management. A requirement for selecting a particular cloud service provider to act as identity provider might be, for instance, specific data protection regulations, such as enforcement that sensitive data are only allowed to be stored in selected or specific countries. Disadvantages of this model are, however, the need to move identity data into the cloud and

thus trust a third party (the cloud service provider) for the user management. Furthermore, although complexity is decreased due to the take up of management tasks through the cloud service provider, organizations or enterprises need to think about how identity data can be easily transferred to this cloud service provider.

7.1.3.1 Cloud Identity Broker-Model

The *Identity as a Service-Model* seems to be a promising concept for identity management in the cloud. In the previous section, the author provided a more general view on this model, just illustrating the basic idea that identities are provided from the cloud. However, according to the [Cloud Security Alliance \[2011\]](#) or [Huang et al. \[2010\]](#) this *Identity as a Service-Model* can be more seen as an identity broker model. This means that the identity provider in the cloud, which provides identities as a service, acts as central identity broker between various other identity providers and several service providers. In other words, the cloud identity provider plays some kind of hub between multiple service and identity providers [[Cloud Security Alliance, 2011](#)]. [Figure 7.4](#) gives a more detailed view on the *Identity as a Service-Model* with central identity broker functionality.

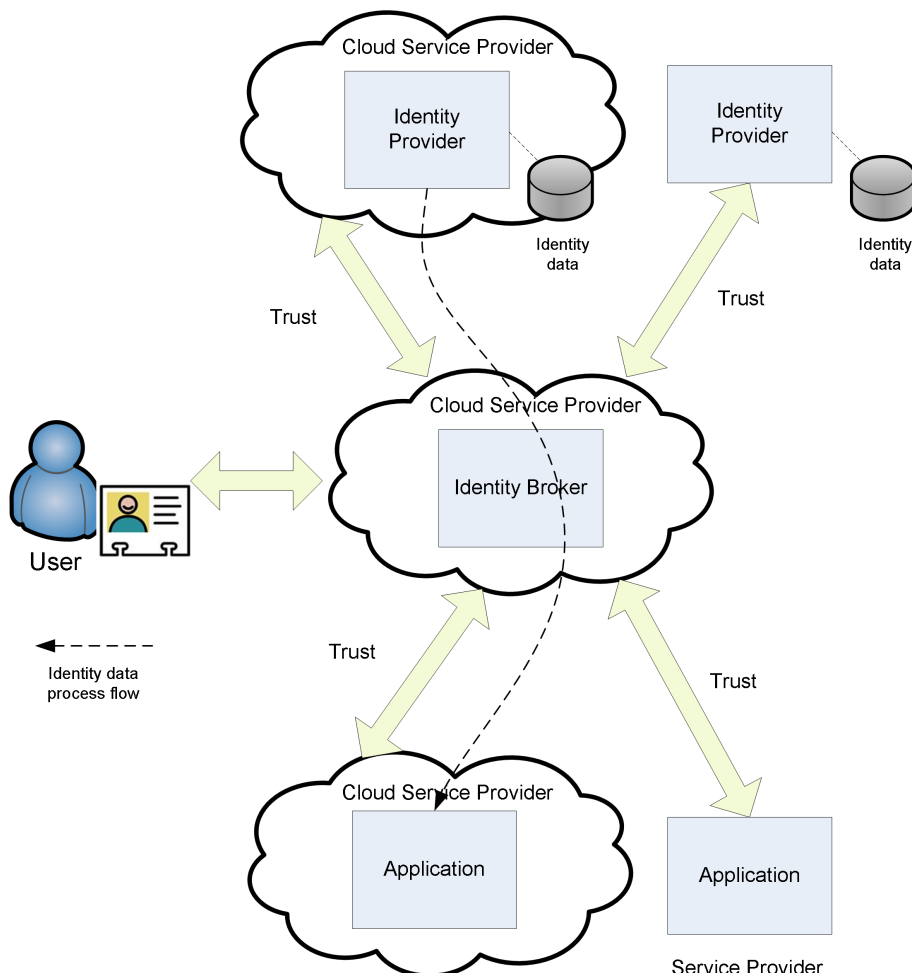


Figure 7.4: Cloud Identity Broker-Model [[Zwattendorfer et al., 2014](#)]

The main idea of this model is to decouple the service provider from multiple identity providers. This means for the service provider that instead of having multiple dependencies to various identity providers, only one strong dependency to the identity broker is given. This has further advantages, both on technical and organizational level. On technical level, the service provider only needs to implement

the communication protocol to the identity broker and thus can ignore specific protocols of the individual identity providers. To lower the implementation efforts for service providers, the identity broker can offer standardized and well-established interfaces and protocols for secure data exchange (e.g., SAML, OpenID, etc.), where service providers can easily connect to. On organizational level, the strength of this model is aggregating multiple different trust relationships between service and identity providers to just one, namely between the service provider and the identity broker. The identity broker now takes over these various trust relationships with the individual identity providers. In other words, the trust relationship between the service provider and the identity provider is brokered through the cloud identity broker. Having just one trust relationship simplifies the contractual model for the service provider. Needless to say that this centralized model has one general drawback. If the identity broker breaks down, users are cut off service provisioning. Nevertheless, this risk is not specific to this model and can be found in several other identity models, where identification and authentication are outsourced to an external entity.

The identity broker model is not new and has already been implemented and deployed by several organizations. For instance, the *Cloud SSO*¹ product of *McAfee*² constitutes a ready implementation. *McAfee Cloud SSO* offers strong user authentication and connectivity to different identity stores and more than 100 external Software as a Service (SaaS) applications. For achieving that, *McAfee Cloud SSO* relies on existing federation interfaces provided by the different SaaS vendors. Another implementation of the identity broker model constitutes the results of the *SkIdentity* project³. *SkIdentity* especially focuses on eIDs, providing secure access to cloud services by supporting various types of eIDs. Hence, the *SkIdentity* implementation might also be interesting for e-Government adoption. In contrast to *McAfee Cloud SSO*, for identity provisioning *SkIdentity* requires a special connector module to be installed at the cloud service provider. Other products implementing the identity broker model are e.g., RadiantOne's *Cloud Federation Service*⁴, or Fugen's *Cloud ID Broker*⁵.

Although several benefits of this model can be identified, still some drawbacks can be found. One major drawback is that users and service providers must rely on the same central service, the cloud identity broker. This means that both the service provider and the user must have a trust relationship with the same authenticating authority. In terms of trust, this model is similar to the traditional central identity model (cf. Section 3.3.2), which uses a pairwise trust model as described in Section 3.1.6. Brokered trust only comes into play between the service providers and the different identity providers.

In addition, another disadvantage is that both the service provider and the user are more or less dependent on the functionality and features of the cloud identity broker. For instance, on the one hand service providers are dependent on the interfaces the identity broker supports. If the cloud identity broker suddenly quits the support of a particular interface, the service provider is cut off of any identity service and requires much effort for implementing another supported interface. On the other hand, users are dependent on the type and number of identity providers the identity broker supports. If a user wants to authenticate at a specific identity provider, which has no affiliation with the identity broker, or if a user wants to use a particular authentication mechanism, which is not supported by the identity broker, accessing the service provider becomes impossible. In other words, the user has actually no real free choice which identity provider to use and is dependent on the support of the identity broker.

To bypass these disadvantages, in this thesis the author proposes a new identity model for the cloud. This new model relies on a federated approach between multiple cloud identity brokers. This *Federated Cloud Identity Broker-Model* or *Federated Identity as a Service-Model* will be discussed in more detail in the next Chapter 8.

¹<http://www.mcafee.com/us/products/cloud-single-sign-on.aspx>

²<http://www.mcafee.com>

³<http://www.skidentity.com>

⁴<http://www.radiantlogic.com/products/radiantone-cfs>

⁵<http://fugensolutions.com/cloud-id-broker.html>

7.1.3.2 BlindIdM Model

The *BlindIdM-Model* has been introduced by Nuñez and Agudo [2014]⁶ and can also be seen as an extension and alteration of the *Identity from the Cloud-Model*. The basic idea is principally the same, however, this model enables identity data storage and data processing also by semi-trusted identity providers⁷ in the cloud. In fact, the identity provider in the cloud can provide identity data to service providers without actually knowing the contents of these data. Hence, the identity provider provides these data in a blind manner [Nuñez and Agudo, 2014]. This particularly preserves users' privacy, as only blinded data are transferred through the cloud identity provider and the cloud provider has no possibility to inspect these data.

The identity data being transferred are actually blinded by using a proxy re-encryption scheme⁸ [Green and Ateniese, 2007; Ateniese et al., 2006]. In more detail, during identity management setup and user registration a home organization⁹ stores the users' identity data in encrypted format at the cloud identity provider. Thereby, the private key is kept confidential by the organization, hence the cloud provider is not able to decrypt the stored identity data. In addition, the organization generates a re-encryption key for the identity provider¹⁰, which allows the re-encryption from the stored data encrypted for the cloud identity provider into other encrypted data, which however can be decrypted by the service provider. During an authentication process, the cloud identity provider then just re-encrypts the desired identity data of the user for the service provider. The practical applicability of the *BlindIdM-Model* has been shown by an implementation in connection with OpenID [Nuñez and Agudo, 2014].

7.2 Electronic Identity to the Cloud

According to the *Identity to the Cloud-Model* of Section 7.1.2, an external identity provider is queried for user identification and authentication at cloud applications. Current cloud applications usually rely on weak authentication mechanisms such as username/password schemes only. In this section, solutions are proposed to be able to use also qualified eIDs such as the Austrian citizen card for cloud authentication [Zwattendorfer et al., 2012a; Zwattendorfer and Tauber, 2012a,b].

7.2.1 Problem Statement

Software as a Service (SaaS) providers offer customers ready-made applications developed and provided by the cloud service provider. Prominent examples of such SaaS cloud service providers are *Google Apps*¹¹ or *Salesforce.com*. However, a lot of other cloud service providers providing SaaS have already emerged and do exist.

Most of the SaaS applications are usually protected by some authentication mechanism. Currently, the dominant authentication approach used by cloud service providers depicts username/password schemes. Therefore, each cloud service provider also hosts its own and separate user management. This has several disadvantages. First, username/password authentication mechanisms early turned out to be weak [Kessler, 1997], which makes such SaaS applications inapplicable for sensitive sectors like e-Government or e-Health. Second, users require and have to manage individual username/password pairs

⁶A similar approach has been introduced by Zwattendorfer and Slamanig [2013a] and will be described in Section 7.3.3.1.

⁷A semi-trusted identity provider is an identity provider that works correctly but may be interested in inspecting private data. In other words, the identity provider acts *honest but curious* [Chen and Sion, 2010; Nuñez and Agudo, 2014].

⁸By using proxy re-encryption a semi-trusted proxy can alter a ciphertext, which has been encrypted for person A, in such a way that it can be decrypted by person B. Thereby, the proxy gains no access to the plaintext of the data. Proxy re-encryption will be explained in more detail in Section 7.3.2.6.

⁹According to Nuñez and Agudo [2014], a home organization is responsible and in control of the organization's identity management. This includes identity data storage, authentication, etc.

¹⁰For generating a re-encryption key, the organization requires its private key and the public key of the service provider.

¹¹<http://www.google.com/enterprise/apps/business/>

for each cloud service provider. I.e., for accessing services of different cloud providers the user first has to register at each provider and second has to authenticate separately. As an example, if a user wants to access CRM cloud services of Salesforce.com and the e-mail services (Gmail) of Google at the same time, she has to run through the complete authentication process for each cloud service provider separately. Figure 7.5 illustrates this current sample situation for cloud authentication where different username/password pairs need to be provided at each cloud provider.

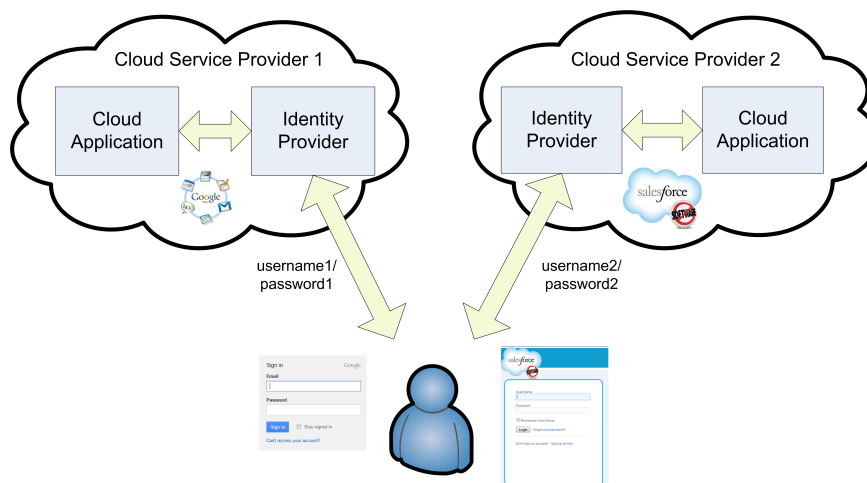


Figure 7.5: Current Situation for Cloud Authentication [Zwattendorfer and Tauber, 2012b]

In the following subsections, solutions are proposed to increase security by using eIDs, which allow for unique identification and which are usually based on strong two-factor authentication instead of simple and insecure username/password mechanisms. Electronic identities are usually user-centric, which puts users into maximum control of their personal data. In addition, users only need to mind just one secure token – and one secure PIN code – instead of managing an overwhelming mass of different passwords. Moreover, the use of eIDs enables fulfillment of certain legal requirements, which helps to facilitate penetration of the cloud market also for sensitive areas such as e-Government or e-Health.

7.2.2 Secure Cloud Authentication using the Austrian Citizen Card

The Austrian citizen card is suited for secure and unique identification and authentication of Austrian citizens at online applications. In this subsection, the Austrian citizen card is used also for identification and authentication at cloud applications. In particular, it is described how the *Identity to the Cloud-Model* of Section 7.1.2 has been realized by using MOA-ID as identity provider and the Austrian citizen card for authentication at selected public cloud service providers [Zwattendorfer et al., 2012a]. For the proof of concept-implementation the cloud service providers Google and Salesforce.com and their SaaS applications were used as identity data consumers. Figure 7.6 illustrates the corresponding architecture.

For the proof of concept applying this identity model, two public cloud service providers (Google and Salesforce.com) were selected for demonstrating secure eID identification and authentication at their SaaS applications. Both providers provide single sign-on interfaces for external eID federation. One protocol they both rely on is SAML. Although both rely on SAML, the individual specifications and implementations are different. Google offers the SSO interface based on SAML 2.0, Salesforce.com provides external authentication capabilities for the SAML versions 2.0 and 1.1. Google supports the SAML *AuthnRequest/Response protocol* [Cantor et al., 2009b] whereas Salesforce.com does not require the use of a specified SAML protocol, which allows the reception of unsolicited response messages. However, both providers rely on the SAML *HTTP Post Binding* [Cantor et al., 2009a] for SAML message transfer. Besides SAML, both providers also offer other external authentication possibilities such as OAuth or OpenID. The latter is only supported by Google.

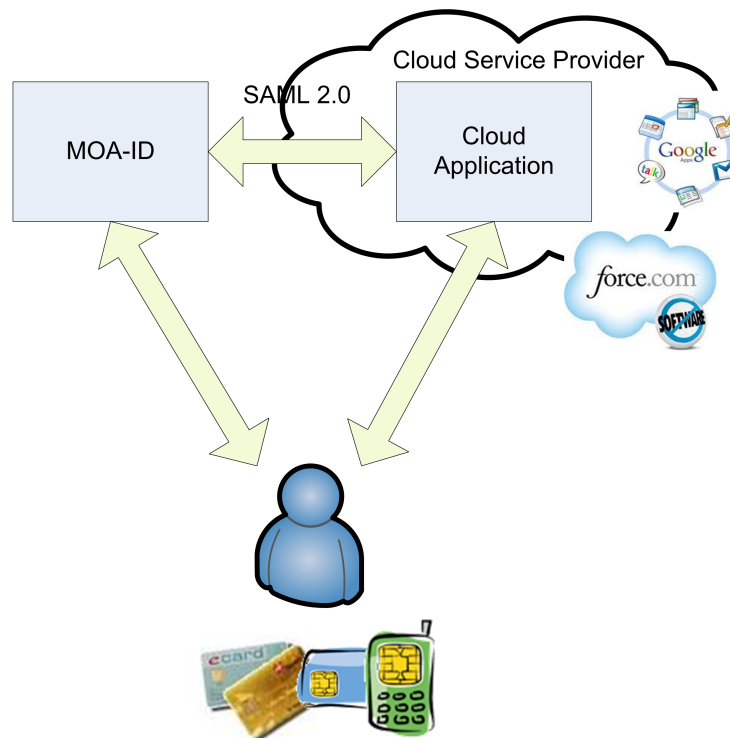


Figure 7.6: Authentication at Google and Salesforce.com using the Austrian citizen card [Zwattendorfer et al., 2012a]

To achieve citizen card authentication at these two cloud service providers, MOA-ID was enhanced by appropriate cloud connectors. These cloud connectors implement the respective SAML 2.0 interface according to the requirements of the cloud service provider. On the one hand, these interfaces enable the reception of SAML 2.0 authentication request messages and, on the other hand, also the sending of SAML 2.0 response messages to the requesting cloud service provider after a successful authentication attempt. The interfaces were implemented according to the requirements offered by Google and Salesforce.com. The modular extension of MOA-ID based on connectors allows easy coupling and decoupling of connector modules. Thereby, the connectors implement an authentication interface to a cloud service provider.

Due to data protection reasons, for electronic identification in Austria the unique identifier (sourcePIN) is derived according to a sector-specific model and a sector-specific PIN (ssPIN) is created (for details see Section 3.6.1). To give citizens the same level of security and privacy also for cloud authentication, the sourcePIN is also derived for cloud service providers according to the Austrian e-Government Act [Federal Chancellery, 2008]. Hence, MOA-ID calculates separate identifiers (ssPINs) for Google and Salesforce.com respectively. This identifier is further used for identity and account federation at the cloud service provider, i.e., linking an existing user account at the cloud service provider with the derived ssPIN for the according cloud service provider.

In more detail, the identifier to be used for authentication at Google must follow the format of an e-mail address. Hence, the derived identifier was transformed into the format $\dots@xyz.com$, where $xyz.com$ denotes the custom domain used for Google Apps. For successful authentication at Google Apps, this identifier must be registered before. Thus no authentication without prior registration is possible. In contrast to that, Salesforce.com allows seamless and on-the-fly user registration. For identification either the username internally used by Salesforce.com or an identifier to be federated with the Salesforce.com account can be used. In the implementation the author favored the second approach as no format changes of the generated derived identifier were required.

Figure 7.7 illustrates the authentication process by using the Austrian citizen card at Google Apps.



Figure 7.7: Citizen card authentication to Google Apps [Zwattendorfer et al., 2012a]

In this scenario, a citizen wants to access a SaaS application of Google (e.g., Google Apps or `https://docs.google.com/a/xyz.com/`). Since in the Google Apps configuration an external identity provider (in this case MOA-ID) was configured, by accessing the Google site and having not previously successfully authenticated the user is automatically forwarded to MOA-ID for authentication. The forward is based on the SAML 2.0 HTTP Post binding and includes a SAML authentication request message. This SAML authentication request message is verified by MOA-ID and – if valid – subsequently a citizen card authentication process is triggered. Thereby, in a first step the identity link is read out from the citizen card and, in a second step, a qualified electronic signature is created (for details of the authentication process to Section 3.6.4 is referred). If both processes were successful, MOA-ID assembles a SAML 2.0 assertion which includes the sSPIN for identity and account federation for the cloud service provider. The assertion is wrapped into a SAML response and the response is transmitted using the SAML HTTP Post binding to the receiving SSO endpoint of Google again. Google validates the SAML message and – if valid – the user is authenticated at the Google application using her citizen card.

Further details on this approach and its implementation can be found in Zwattendorfer et al. [2012a].

7.2.3 Secure Cloud Authentication using the STORK Middleware

This section explains – by relying on the STORK MW approach – how further sophisticated authentication mechanism based on eIDs of other countries can be used for more secure and reliable identification and authentication at applications offered by cloud service providers. For achieving that, again the *Identity to the Cloud-Model* as described in Section 7.1.2 was considered. This model allows for more control and privacy protection than the other models and thus facilitates compliance with most national regulations and laws. In the following, based on the work of Zwattendorfer and Tauber [2012a,b] it is explained how the STORK MW architecture was extended to achieve eID authentication of various countries at two cloud service providers.

7.2.3.1 Extension to the STORK Middleware

To demonstrate the applicability of eID authentication at public clouds using the STORK framework, a prototype was implemented. For the prototypical implementation the two cloud service providers Google and Salesforce.com were chosen again. The reasons why the author chose those two providers were the support of an external interface for identification and authentication on the one side, and the support of SAML for these interfaces on the other side. The author focused on SAML because SAML has been

especially designed for cross-domain identity and authentication data transfer and because the STORK infrastructure already provides some basic SAML functionality.

As identity provider for authentication at these public cloud service providers the author took the VIDP from STORK because of its flexible and modular architecture. On the one hand, various national eID systems are already supported and covered by this architecture. On the other hand, the plug-able design allows for easy integration of new service provider authentication interfaces as required for the communication with Google and Salesforce.com. The modular VIDP architecture allows easy extensibility, hence also other cloud service providers offering different interfaces could be supported.

To allow for secure eID authentication at Google Apps and Salesforce.com, the VIDP architecture was enhanced by adding two new service provider modules: one interface for secure authentication at Google Apps and the other one for secure authentication at Salesforce.com. Both interfaces are SAML-based. Two additional modules supporting the SSO interface of the individual cloud service provider were implemented. Those modules furthermore implement the *Service Provider Interface* (cf. Figure 7.8) and are plugged on the VIDP. Both modules are capable of receiving SAML-based authentication request and sending response messages carrying identity and authentication information. The author decided to use SAML 2.0 as cloud authentication protocol for both providers because basic SAML functionality was already available by the VIDP implementation. Although STORK already provides SAML functionality, the STORK protocol could not be used out-of-the-box for SSO authentication at these cloud service providers. The reason is that the SAML interfaces of STORK, Google, and Salesforce.com all behave differently. Therefore, only some basic SAML functionality of the STORK framework could be re-used for the implementation of the respective cloud service provider interfaces. In fact, two STORK extensions for cloud service provider interfaces were implemented, both supporting SAML, but one the SAML "profile" of Google and one the SAML "profile" of Salesforce.com. However, both interfaces rely on the SAML 2.0 *Web SSO Profile* [Hughes et al., 2009] and the *HTTP Post Binding* [Cantor et al., 2009a] for SAML message transfer. Figure 7.8 illustrates this extended VIDP architecture.

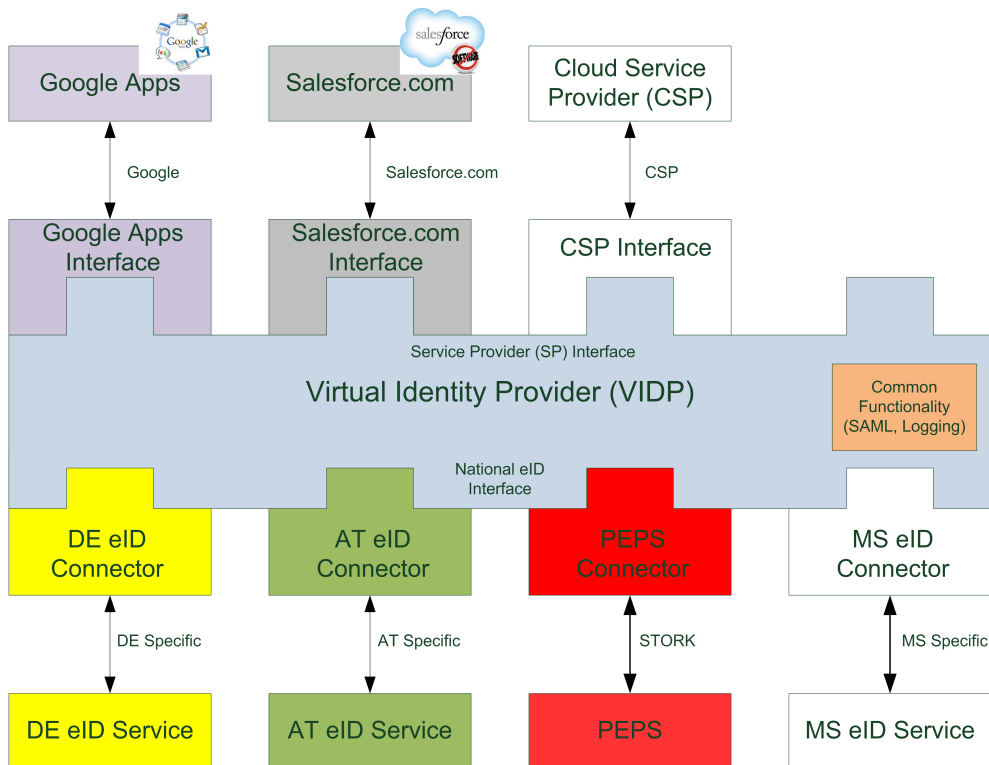


Figure 7.8: Extended VIDP architecture supporting eID- based cloud authentication [Zwattendorfer and Tauber, 2012a]

7.2.3.2 Extensions for enabling Single Sign-On

In the previous described scenario, the user has to authenticate at the STORK VIDP for each cloud service provider one after another. First, the user has to authenticate at Google using appropriate credentials. Second, the user must provide the same credentials a second time for authentication at Salesforce.com. Needless to say, the sequence of authentications could also be vice versa. While two subsequent authentication processes do not extremely decrease comfort, a higher number of authentication sequences could become burdensome for users. To overcome this issue, the author introduced a secure and privacy-preserving SSO architecture for cross-cloud authentication. By applying this architecture, users need to authenticate only once but still get access to applications of multiple cloud service providers. According to Figure 7.5, users already authenticated at cloud service provider 1 (Google) are seamlessly authenticated at cloud service provider 2 (Salesforce.com) without re-authentication.

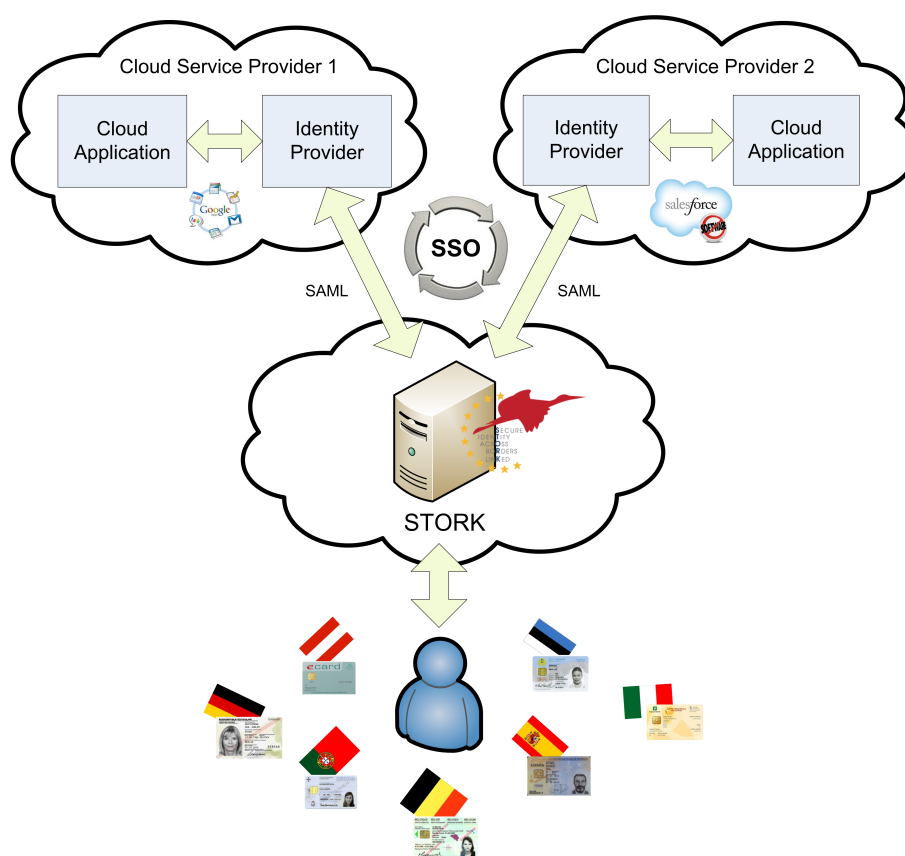


Figure 7.9: Extended STORK MW Architecture for Cross-Cloud SSO [Zwattendorfer and Tauber, 2012b]

The extended STORK MW architecture shown in Figure 7.9 supports strong eID authentication at different SaaS cloud service providers, providing single sign-on between those providers at the same time. This means, by using her national eID a European citizen just needs to authenticate once via STORK at one cloud service provider. After that, the citizen is automatically and seamlessly authenticated at other cloud service providers protected by STORK without re-authentication. STORK supports 18 country-specific eID approaches, hence citizens of 18 EU member states are capable of using this solution (cf. Section 5.5). In this figure, only two sample SaaS cloud service providers, namely Google and Salesforce.com, are shown. This is because those two providers were also chosen in the implementation, demonstrating SSO between different SaaS cloud service providers. The proposed architecture can be extended to support SSO between multiple cloud service providers. Although in this demonstrator SAML is used as external SSO interface for both cloud service providers, other SSO protocols (e.g.,

OpenID) offered by cloud service providers may be supported, as the STORK architecture allows for easy extension due to its modular design (cf. Section 5.5.5.2).

Nevertheless, the previously described status of the implementation still reflects just single, but strong authentication at the individual cloud service providers. Hence, if users want to simultaneously access SaaS applications of both cloud service providers, they still have to login twice by using their respective national eID. To achieve single sign-on between both providers, the author had to further amend the STORK architecture to manage authentication sessions for a certain time period. Within this period, seamless SSO authentications between both providers are possible without re-authentication. In addition, some identity broker functionality was added because the national electronic identifier provided by STORK cannot be directly used for cloud service provider authentication in some situations. This especially has legal reasons as some countries do not allow direct processing of the national identifier due to data protection restrictions (e.g., Austria). Moreover, instead of using the identifier directly, some context-specific derivation is required. Therefore, in the proposed solution the identifier provided by STORK is securely derived separately for Google and Salesforce.com using one-way cryptographic hash functions (similar to the Austrian approach used in Section 7.2.2). For derivation, the combination of the STORK identifier and a provider-specific identifier of the respective cloud service provider was used as a basis. Hence, two provider-specific identifiers were created that can be further used for identification at the respective cloud service provider. The use of hash functions for derivation has two advantages. First, hash functions still guarantee uniqueness of the newly created identifier. Second, hash function derivations do not allow recalculation to the actual given STORK identifier. This especially preserves citizens' privacy as never the very same identifier is used for identification at different cloud service providers.

Further details on these extensions enabling single sign-on can be found in Zwattendorfer and Tauber [2012b].

7.2.4 Lessons Learned

One of the main lessons learned is that one SAML implementation is not like another. Even if the same SAML version, the same SAML profile, or the same SAML binding is used, the behavior is different between clients and providers respectively. This implies for the prototypical implementation, that although both for demonstration selected public cloud service providers (Google and Salesforce.com) rely on SAML 2.0, a different behavior of the provided SAML interfaces could be determined during the implementation. Hence, instead of one single SAML interface provided by STORK, the STORK framework had to be extended by two additional SAML interfaces. One interface supporting the SAML "profile" of Google, and the other one supporting the SAML "profile" of Salesforce.com. In fact, the SAML messages sent to the providers had to perfectly match their desired standard. SAML messages containing additional elements or attributes – even if they were valid according to the SAML 2.0 specifications – were simply declined. This actually should not define a severe issue, but the documentation for implementing the SAML-based cloud service provider interfaces was rather weak. Google, for example, provides some out-dated reference code for demonstrating access to the SAML interface¹². In contrast to that, Salesforce.com is more developer-friendly. They actually provide some online validation service for testing the SAML messages. Verification of SAML messages, of course except security related functions, is not that strict compared to Google.

Concerning the identifier to be used for external identification at the cloud service providers, also no common format can be used for both providers. The unique identifier provided by STORK is provider-specific derived due to privacy reasons. Thereby, Google only accepts identifiers following the e-mail format. This identifier must also match a username which must have been previously registered in the internal user database of Google Apps. As opposed to this, in Salesforce.com applications real identity

¹²https://developers.google.com/google-apps/sso/saml_reference_implementation_web?csw=1

federation is supported. This means that the identifier used for external authentication just needs to be linked to an existing username of the internal Salesforce.com user management. Moreover, this does not define a strict requirement as Salesforce.com also supports on-the-fly registrations, which constitute seamless registrations during the very first successful authentication process.

7.2.4.1 Further Implementation Details

After successful implementation of the *Identity to the Cloud-Model*, it was decided to further try moving the extended VIDP architecture also into the cloud for applying the *Identity from the Cloud-Model*. Thereby, the cloud paradigm of an *Identity as a Service-Model* using eIDs could be fully supported.

For deploying the VIDP in the cloud *Jelastic*¹³ and the *Google App Engine*¹⁴ PaaS offerings were selected as underlying Java-based cloud platforms. The author early succeeded of the deployment on Jelastic as no code modifications were required. Jelastic supports a complete Java virtual machine (JVM) and various application servers in its provisioned cloud platforms, where the VIDP could be deployed to. The deployment of the VIDP on the Google App Engine was even more difficult as the provided JVM of the Google cloud platform provides a limited subset of functionality only. Hence, several changes on the code were necessary. For instance, code snippets writing to the file system, running threads, or raw network sockets, which are all not supported by the Google App Engine, had to be exchanged and rewritten to use only functionality supported by this platform. Nevertheless, the author also succeeded in deploying the extended VIDP on this cloud platform to apply a fully-fledged *Identity as a Service-Model*.

While the implementation of this model was technically feasible, it has several implications and brings up new obstacles as identity data are processed directly in the cloud. As mentioned in Section 6.3.2, privacy and data protection are severe issues when storing or processing sensitive data in the cloud. To bypass these issues, the author proposes privacy-enhanced versions of the *Identity from the Cloud-Model* in the next section.

7.3 Electronic Identity from the Cloud

The last cloud identity management-model (*Identity from the Cloud-Model*) of Section 7.1 fully utilizes the cloud computing paradigm as identities are provided from the cloud. In this concept or model respectively, an identity provider or identity broker is operated in the cloud. However, when applying this model in the public cloud, several privacy issues may occur as the cloud service provider operating the identity provider/identity broker might be able to inspect stored or processed identity data. To bypass this issue, the author proposes different solutions for deploying identity providers (or identity brokers) in the public cloud by still preserving citizens' privacy. In particular, the author focuses on eID solutions to be applied in the public cloud in a privacy-preserving manner, since eIDs are the identification means to be used in e-Government scenarios which can include sensitive citizen data. The work has been published in Zwattendorfer and Slamanig [2013a,c]; Slamanig et al. [2014]

First, the author proposes three different possibilities using different underlying cryptographic technologies for deploying an identity provider in a public cloud. More precisely, the author applies these three possibilities to the basic Austrian eID system, involving a citizen, MOA-ID as identity provider, and a service provider. Discussing and evaluating all three possibilities, the author takes the best approach (using proxy re-encryption and redactable signatures – cf. Section 7.3.3.1) and applies it to the whole Austrian eID system, involving identification and authentication of legal persons as well as identification and authentication of foreign EU citizens. Finally, the author proposes an enhanced version of the proxy re-encryption approach by increasing privacy through additional user control.

¹³<http://jelastic.com>

¹⁴<https://appengine.google.com>

This section is structured as follows. First, the general problem statement taking the MOA-ID architecture as an example is described (Section 7.2.1). After that, basic cryptographic building blocks are explained and defined in Section 7.3.2. Adopting these cryptographic technologies, Section 7.3.3 elaborates on the three different approaches for deploying an identity provider (more exactly MOA-ID) in a public cloud. Based on that, Section 7.3.4 explains in detail how the whole Austrian eID system could be migrated into a public cloud using approach 1 (proxy re-encryption and redactable signatures – cf. Section 7.3.3.1). Finally, a general and more enhanced eID model using proxy re-encryption and redactable signatures and additionally enabling privacy features such as user-centricity and selective disclosure is described in Section 7.3.5. This model is named *Identity as a Service-Model for Electronic Identities*.

7.3.1 Problem Statement

The current Austrian eID system relies on a local deployment model¹⁵, where MOA-ID is deployed and operated in basically every service provider's domain. Due to that fact, MOA-ID is assumed to be trusted, i.e., it will not leak sensitive information such as the citizen's sourcePIN. While this local deployment model has some benefits in terms of end-to-end security or scalability, still some issues can be identified compared to a centralized deployment model of MOA-ID. The adoption of a centralized model may have the following advantages:

On the one hand, the use of one single and central instance of MOA-ID has a clear advantage for citizens as they only need to trust one specific identity provider. In addition, users could benefit from comfortable single sign-on (SSO) authentications. On the other hand, especially service providers can save a lot of costs because they do not need to operate and maintain a separate MOA-ID installation. In addition, several different identity protocols can be supported and hence the service provider could select its favorite protocol.

Nevertheless, still some disadvantages can be identified. For instance, a single instance of MOA-ID constitutes a single point of failure or attack. Additionally, a centralized MOA-ID relies on an indirect trust model and the service provider has no direct trust relationship with the citizen anymore as it is in the local model (cf. Section 3.1.6). Finally, scalability may be an issue as all citizen authentications will run through this centralized system. This is probably the main issue, as theoretically the whole Austrian population could use this service for identification and authentication at service providers. However, the issue on scalability can be tackled by moving MOA-ID into a public cloud, which is able to theoretically provide unlimited computing resources (cf. Section 6.3.3.2). Needless to say, a move of a trusted service into the public cloud brings up some new obstacles. For instance, assuming that MOA-ID in the cloud works correctly, it still has to be ensured that the cloud provider has no access to private citizen data during the authentication process. In general, MOA-ID in the cloud must still work equivalent to the current Austrian eID system and must still be compliant to Austrian national law.

In the following subsections, three different approaches are explained which are able to deal with these cloud obstacles by applying and integrating appropriate cryptographic technologies into the Austrian eID system. Before, the applied cryptographic technologies are briefly discussed.

7.3.2 Cryptographic Building Blocks

In this section, cryptographic building blocks that are required by the presented approaches are introduced. In detail, digital signatures, redactable signatures, and anonymous signatures are described. In addition, anonymous credentials are briefly explained. Finally, different encryption techniques such as public key encryption, proxy re-encryption, and fully homomorphic encryption are discussed.

¹⁵The local deployment model is applied for MOA-ID only. Other components such as the mandate issuing service (MIS) are deployed centrally. For details, the author refers back to Section 3.6.3

Note that in practice in all discussed schemes the public key pk_A of a user A is bound to the user's identity. This is typically realized by the means of digital certificates within some public key infrastructure (PKI). Thus, it is assumed that public keys are always publicly available in an authentic fashion. If an entity A is in possession of an encryption (PKE) and signature (DSS) key pair, they are denoted by (sk_A, pk_A) and (sk'_A, pk'_A) respectively. Moreover, it is assumed that if bitstrings a and b are concatenated $a||b$, this happens in a way such that all individual components are uniquely recoverable.

7.3.2.1 Digital Signatures

A digital signature scheme (DSS) [Kaliski, 2011] is a triple $(DSS.KeyGen, DSS.Sign, DSS.Verify)$ of poly-time algorithms, whereas $DSS.KeyGen$ is a probabilistic key generation algorithm that takes a security parameter κ and outputs a private and public key pair (sk, pk) . The probabilistic signing algorithm $DSS.Sign$ takes as input a message $M \in \{0, 1\}^*$ and a private key sk , and outputs a signature σ . The verification algorithm $DSS.Verify$ takes as input a signature σ , a message $M \in \{0, 1\}^*$ and a public key pk , and outputs a single bit $b \in \{\text{true}, \text{false}\}$ indicating whether σ is a valid signature for M . Furthermore, the DSS is required to be correct, i.e., for all $(sk, pk) \in DSS.KeyGen(\kappa)$ and all $M \in \{0, 1\}^*$ then $DSS.Verify(DSS.Sign(M, sk), M, pk) = \text{true}$. A DSS is secure if it is existentially unforgeable under adaptively chosen-message attacks (UF-CMA). Note that in practice one typically employs the hash-then-sign paradigm, i.e., instead of inputting M into $DSS.Sign$ and $DSS.Verify$, one inputs $H(M)$ where H is a suitable cryptographic hash function.

7.3.2.2 Redactable Signatures

A conventional digital signature does not allow for alterations of a signed document without invalidating the signature. However, there are scenarios where it would be valuable to have the possibility to replace or remove (specified) parts of a message after signature creation such that the original signature stays valid (and no interaction with the original signer is required). Signature schemes which allow *removal* of content (replacement by some special symbol \perp) by *any* party are called redactable [Johnson et al., 2002], while signature schemes which allow (arbitrary) *replacements* of *admissible* parts by a *designated* party are called sanitizable signature schemes [Ateniese et al., 2005]. An introduction to redactable signatures and their applicability in e-Business applications is given in Stranacher and Zwattendorfer [2013]; Stranacher et al. [2013a]. Below, an abstract definition of redactable signatures are presented [Zwattendorfer and Slamanig, 2013a]:

RS.KeyGen: This probabilistic key generation algorithm takes a security parameter and produces and outputs a public (verification) key pk and a private (signing) key sk .

RS.Sign: This (probabilistic) signing algorithm gets as input the signing key sk and a message $m = (m[1], \dots, m[\ell])$, $m[i] \in \{0, 1\}^*$ and outputs a signature $\sigma = \text{RS.Sign}(sk, m)$.

RS.Verify: This deterministic signature verification algorithm gets as input a public key pk , a message $m = (m[1], \dots, m[\ell])$, $m[i] \in \{0, 1\}^*$, and a signature σ and outputs a single bit $b = \text{RS.Verify}(pk, m, \sigma)$, $b \in \{\text{true}, \text{false}\}$, indicating whether σ is a valid signature for m .

RS.Redact: This (probabilistic) redaction algorithm takes as input a message $m = (m[1], \dots, m[\ell])$, $m[i] \in \{0, 1\}^*$, the public key pk , a signature σ , and a list MOD of indices of blocks to be redacted. It returns a modified message and signature pair $(\hat{m}, \hat{\sigma}) = \text{RS.Redact}(m, pk, \sigma, \text{MOD})$ or an error. Note that for any such signature $(\hat{m}, \hat{\sigma})$ it is $\text{RS.Verify}(pk, \hat{m}, \hat{\sigma}) = \text{true}$.

Scheme 7.1: Redactable Signatures [Zwattendorfer and Slamanig, 2013a]

7.3.2.3 Anonymous Signatures

Anonymous signature schemes allow group members to issue signatures on behalf of a group, while hiding for each signature which group member actually produced it. There are several flavors of anonymous signatures: *Group signatures* [Ateniese et al., 2000] involve a dedicated entity (the group manager), who runs a setup and an explicit join protocol for every group member to create the respective members signing key. Furthermore, the group manager is able to open signatures issued by group members to identify the respective signer.

Ring signatures [Rivest et al., 2006] are conceptually similar to group signatures, but there is no group manager and the anonymity provided is unconditional. They are "ad-hoc", meaning that a user may take an arbitrary set (ring) of valid public keys to construct a ring signature and the ring represents the anonymity set. The use of ring signatures was chosen for one of the three approaches. An abstract definition of this signature scheme is presented below, where the key generation is that of a standard digital signature scheme (DSS) and hence omitted here [Zwattendorfer and Slamanig, 2013a]:

AS.Sign: This (probabilistic) signing algorithm gets as input the signing key sk_i s.t. $pk_i \in R$, a ring of public keys $R = (pk_1, \dots, pk_n)$, a message m and outputs a signature $\sigma = \text{AS.Sign}(sk_i, R, m)$.

AS.Verify: This deterministic signature verification algorithm gets as input a ring of public keys $R = (pk_1, \dots, pk_n)$, a message m , and a signature σ and outputs a single bit $b = \text{AS.Verify}(R, m, \sigma)$, $b \in \{\text{true}, \text{false}\}$, indicating whether σ is a valid signature for m under R .

Scheme 7.2: Anonymous Signatures [Zwattendorfer and Slamanig, 2013a]

7.3.2.4 Anonymous Credentials

Anonymous credential (AC) systems [Brands, 2000; Camenisch and Lysyanskaya, 2001] enable anonymous attribute-based authentication, i.e., they hide the identity of the credential's owner. Multi-show approaches support unlinkability, i.e., different showings of a credential remain unlinkable and are unlinkable to the issuing [Camenisch and Lysyanskaya, 2001], while others are one-show [Brands, 2000]. Anonymous credentials are very expressive since they allow to encode arbitrary attributes into the credential. Additionally, during the proof of possession of a credential a user can selectively reveal values of attributes or prove that certain relations among attributes hold, without revealing the attribute values. An abstract definition of an AC system can be used as follows [Zwattendorfer and Slamanig, 2013a]:

AC.KeyGen: This probabilistic key generation algorithm is run by an authority and takes a security parameter and produces and outputs a public key pk and a private key sk .

AC.Issue: This interactive algorithm is run between a user U and an authority A . U has as input a list of attributes with corresponding values attr and wants to obtain a credential for attr (U may also have as input a long term secret). U executes the credential issuing protocol for attr with A by using U 's input attr and A has as input its private key sk . Both algorithms have as input pk and at the end of this interaction U obtains a credential Cred corresponding to attr .

AC.Prove: This interactive algorithm is run between a user U and a verifier V . U proves the possession of Cred for attr' , which represents some subset of attr , to a verifier V . At the end of the protocol, V outputs accept if U has a valid credential Cred for attr' , otherwise V outputs reject .

Scheme 7.3: Anonymous Credentials [Zwattendorfer and Slamanig, 2013a]

Note that the Prove algorithm may also be non-interactive, i.e., the credential holder produces a signature of knowledge which can then be given to the verifier to check the validity of the proof locally.

7.3.2.5 Public Key Encryption

A public key encryption (PKE) scheme [Pointcheval, 2011] is a triple (PKE.KeyGen, PKE.Enc, PKE.Dec) of poly-time algorithms, whereas PKE.KeyGen is a probabilistic key generation algorithm that takes a security parameter κ and outputs a private and public key pair (sk, pk). The probabilistic encryption algorithm PKE.Enc takes as input a public key pk and a message $M \in \{0, 1\}^*$ and returns a ciphertext $c = \text{PKE.Enc}(\text{pk}, M)$. The decryption algorithm PKE.Dec takes as input a private key sk and a ciphertext c and returns a message $M = \text{PKE.Dec}(\text{sk}, c)$ or \perp in the case of failure. A PKE scheme is required to be indistinguishable under chosen plaintext attacks (IND-CPA). Abstractly, private key (or symmetric) encryption schemes can be defined analogously, whereas PKE.KeyGen only generates a single key K which is used as input to the encryption and decryption algorithms. For the security of a private key encryption scheme also IND-CPA security is required. Note that when applying PKE to a larger message M , then it is implicitly meant to be applying *hybrid encryption*, i.e., choosing a random symmetric key K and sending/storing the tuple $(c_1 = \text{PKE.Enc}(K, \text{pk}), c_2 = \text{PKE.Enc}'(M, K))$.

7.3.2.6 Proxy Re-Encryption

Proxy re-encryption is a public key encryption paradigm where a semi-trusted proxy can transform a message encrypted under the key of party A into another ciphertext, containing the initial plaintext, such that another party B can decrypt with its key. Although the proxy can perform this re-encryption operation, it neither gets access to the plaintext nor to the decryption keys. According to the direction of this re-encryption, such schemes can be classified into bidirectional, i.e., the proxy can transform from A to B and vice versa, and unidirectional, i.e., the proxy can convert in one direction only, schemes. Furthermore, one can distinguish between multi-use schemes [Chow et al., 2010], i.e., the ciphertext can be transformed from A to B to C etc., and single-use schemes Green and Ateniese [2007], i.e., the ciphertext can be transformed only once. In the following, proxy re-encryption is described first more general based on the non-identity-based work of Ateniese et al. [2006]; Chow et al. [2010] and afterwards the unidirectional single-use identity-based proxy re-encryption scheme of Green and Ateniese [2007] is explained. Depending on the use case and its requirements in the following sections an appropriate scheme (single use or multi-use, identity-based or non-identity-based, etc.) will be selected. Proxy re-encryption can be described as follows [Zwattendorfer and Slamanig, 2013a; Slamanig et al., 2014]:

RE.Setup: This probabilistic algorithm gets a security parameter and a value `MaxLevel` indicating the maximum number of consecutive re-encryptions permitted by the scheme (in case of single-use `MaxLevel=2` is set). It outputs the master public parameters $params$, which are accessible by any other algorithm.

RE.KeyGen: This probabilistic key generation algorithm gets $params$ and outputs a private and public key pair (sk_A, pk_A) for party A .

RE.Enc: This probabilistic encryption algorithm gets $params$, a private key sk_A , and a plaintext m and outputs $c_A = \text{RE.Enc}(params, sk_A, m)$.

RE.RKGen: This probabilistic re-encryption key generation algorithm gets $params$, a private key sk_A , a different public key pk_B and outputs a re-encryption key $rk_{A \rightarrow B} = \text{RE.RKGen}(params, sk_A, pk_B)$.

RE.ReEnc: This (probabilistic) re-encryption algorithm gets as input a ciphertext c_A encrypted for party A and a re-encryption key $rk_{A \rightarrow B}$ (generated by RE.RKGen) and outputs a re-encrypted ciphertext $c_B = \text{RE.ReEnc}(c_A, rk_{A \rightarrow B})$.

RE.Dec: This decryption algorithm gets $params$, a private key sk_B , and a ciphertext c_B and outputs $m = \text{RE.Dec}(params, sk_B, c_B)$ or an error.

Scheme 7.4: Non-identity-based Proxy Re-encryption

RE.Setup: This probabilistic algorithm gets a security parameter and a value **MaxLevel** indicating the maximum number of consecutive re-encryptions permitted by the scheme (in case of single-use **MaxLevel**=2 is set). It outputs the master public parameters $params$, which are distributed to users, and the master private key msk , which is kept private.

RE.KeyGen: This probabilistic key generation algorithm gets $params$, the master private key msk , and an identity $id \in \{0, 1\}^*$ and outputs a private key sk_{id} corresponding to that identity.

RE.Enc: This probabilistic encryption algorithm gets $params$, an identity $id \in \{0, 1\}^*$, and a plaintext m and outputs $c_{id} = \text{RE.Enc}(params, id, m)$.

RE.RKGen: This probabilistic re-encryption key generation algorithm gets $params$, a private key sk_{id_1} (derived via **RE.KeyGen**), and two identities $(id_1, id_2) \in \{0, 1\}^*$ and outputs a re-encryption key $rk_{id_1 \rightarrow id_2} = \text{RE.RKGen}(params, sk_{id_1}, id_1, id_2)$.

RE.ReEnc: This (probabilistic) re-encryption algorithm gets as input a ciphertext c_{id_1} under identity id_1 and a re-encryption key $rk_{id_1 \rightarrow id_2}$ (generated by **RE.RKGen**) and outputs a re-encrypted ciphertext $c_{id_2} = \text{RE.ReEnc}(c_{id_1}, rk_{id_1 \rightarrow id_2})$.

RE.Dec: This decryption algorithm gets $params$, a private key sk_{id} , and a ciphertext c_{id} and outputs $m = \text{RE.Dec}(params, sk_{id}, c_{id})$ or an error.

Scheme 7.5: Identity-based Proxy Re-encryption [Zwattendorfer and Slamanig, 2013a]

7.3.2.7 Fully Homomorphic Encryption

Fully homomorphic encryption (FHE) schemes are semantically secure (public-key) encryption schemes which allow arbitrary functions to be evaluated on ciphertexts given the (public) key and the ciphertext. Gentry [2009] provided the first construction along with a general blue-print to construct (bootstrap) such schemes from less powerful ones. Since then lots of improvements and alternate approaches have been proposed [Vaikuntanathan, 2011]. However, it seems to require some more years of research to make them practical in general [Gentry et al., 2012]. A fully homomorphic (public-key) encryption scheme is defined by the following efficient algorithms [Zwattendorfer and Slamanig, 2013a]:

FHE.KeyGen: This probabilistic key generation algorithm takes a security parameter and produces and outputs a public-key pk , a public evaluation key evk , and a private key sk .

FHE.Enc: This probabilistic encryption algorithm takes a message $m \in \{0, 1\}^n$ and a public-key pk and outputs a ciphertext $c = \text{FHE.Enc}(m, pk)$.

FHE.Dec: This deterministic algorithm takes a ciphertext c and a private key sk and outputs $m = \text{FHE.Dec}(c, sk)$.

FHE.Eval: This homomorphic evaluation algorithm takes an evaluation key evk , a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ and k ciphertexts and outputs a ciphertext $c_f = \text{FHE.Eval}(f, c_1, \dots, c_k, evk)$.

Scheme 7.6: Fully Homomorphic Encryption [Zwattendorfer and Slamanig, 2013a]

In this definition messages are bits, but this can easily be generalized to larger spaces. Let us consider arbitrary message spaces in the following. For one approach it is assumed that FHE schemes exists which are "key-homomorphic". Loosely speaking, this means that for each pair of public keys pk_1 and pk_2 one can derive $f_{1,2}$ and $evk_{1,2}$ such that

$$m = \text{FHE.Dec}(\text{FHE.Eval}(f_{1,2}, \text{FHE.Enc}(m, pk_1), evk_{1,2}), sk_2).$$

This means that by using $f_{1,2}$ one performs a "re-encryption" of m encrypted under pk_1 to another ciphertext under pk_2 , which can then be decrypted using sk_2 . Such a scheme can trivially be realized

using any FHE scheme by letting $f_{1,2}$ represent the circuit, which firstly decrypts the ciphertext c using sk_1 obtaining m and then encrypts m using pk_2 and $evk_{1,2} = evk_1$. However, since now sk_1 would be explicitly wired in the circuit, this would reveal the secret key which is clearly undesirable. Since Zwattendorfer and Slamanig [2013a] are currently not aware of an FHE construction which supports this (loosely defined) property, it needs to be assumed that such a scheme will be available in the future.

7.3.3 MOA-ID in the Public Cloud

In order to make a migration of the basic Austrian eID system and MOA-ID into the public cloud possible, three approaches to adapt the existing basic Austrian eID system for running it in the public cloud were identified. The adapted basic Austrian eID system of the respective solution will provide all functions of MOA-ID (identification, ssPIN generation, and authentication) as in the current status, but protects citizen's privacy with respect to the cloud provider. For providing compact descriptions, in the following the author denotes the SourcePIN Register Authority by SRA and the Identity Link by $\mathcal{I} = ((A_1, a_1), \dots, (A_k, a_k))$ as a sequence of attribute labels and attribute values. The set of citizens is denoted as $C = \{C_1, \dots, C_n\}$, the set of service providers as $S = \{S_1, \dots, S_\ell\}$, and the citizen's client-side middleware as M . Moreover, it is assumed that citizen C_i wants to authenticate at service provider S_j who requires the set of attributes \mathcal{A}_j from \mathcal{I} and exactly one "pseudonym", i.e., the ssPIN for the sector s the service provider S_j is associated to. Additionally, recall that every citizen C_i has a signing key sk_{C_i} stored on the card and the public key pk_{C_i} is publicly available (cf. Section 3.6.2).

7.3.3.1 Approach 1: Using Proxy Re-Encryption and Redactable Signatures

Here, the Identity Link \mathcal{I} is modified in a way that it does not include the sourcePIN, but additionally all ssPINs according to all possible governmental sectors. In this augmented Identity Link \mathcal{I}' , every attribute a_i is encrypted using an uni-directional single-use proxy re-encryption scheme under a public key (the identity of MOA-ID) such that the corresponding private key is *not* available to MOA-ID and is only known to the SRA. Furthermore, instead of using a conventional digital signature scheme, \mathcal{I}' is signed by the SRA using a redactable signature scheme such that every a_i from \mathcal{I}' can be redacted. The public verification key is available to MOA-ID. Every service provider S_j obtains a key pair for the proxy re-encryption scheme when registering at the SRA. The latter entity produces a re-encryption key, which allows to re-encrypt ciphertexts intended for MOA-ID to S_j , and gives it to MOA-ID. Below the detailed workflow is presented:

Setup: SRA generates $(pk_{SRA}, sk_{SRA}) = \text{RS.KeyGen}(\kappa)$, $(params_{RE}, msk_{RE}) = \text{RE.Setup}(\kappa, 1)$ as well as $sk_{MOA-ID} = \text{RE.KeyGen}(params_{RE}, msk_{RE}, id_{MOA-ID})$. It keeps secret $(sk_{RS}, msk_{RE}, sk_{MOA-ID})$ and publishes $params_{RE}$ as well as pk_{RS} .

Citizen registration: The registration of a citizen C_i at the SRA works as it is done now with the exception that \mathcal{I}' includes additional attributes a_{k+1}, \dots, a_m representing ssPINs for all sectors. Furthermore, for every $(A_i, a_i) \in \mathcal{I}'$ the SRA replaces a_i by $c_{a_i} = \text{RE.Enc}(params_{RE}, a_i, id_{MOA-ID})$ and produces a redactable signature $\sigma_{\mathcal{I}'} = \text{RS.Sign}(sk_{SRA}, \mathcal{I}')$. Then, $(\sigma_{\mathcal{I}'}, \mathcal{I}')$ is stored on C_i 's citizen card.

Service provider registration: The registration for service provider S_j at the SRA works as follows. SRA produces a private key $sk_{S_j} = \text{RE.KeyGen}(params_{RE}, msk_{RE}, id_{S_j})$ for S_j and a re-encryption key $rk_{MOA-ID \rightarrow S_j} = \text{RE.RKGen}(params_{RE}, sk_{MOA-ID}, MOA-ID, S_j)$ and gives sk_{S_j} to S_j and $rk_{MOA-ID \rightarrow S_j}$ to MOA-ID respectively.

Authentication at online services:

1 & 2: After having received an authentication request from S_j , MOA-ID starts the citizen identification process by requesting C_i 's Identity Link \mathcal{I}' through M . Thereby, two possibilities exist:

1. If MOA-ID tells M which attributes \mathcal{A}_j are required by S_j , then M runs $(\hat{\mathcal{I}}', \hat{\sigma}_{\mathcal{I}'}) = \text{RS.Redact}(\mathcal{I}', pk_{RS}, \sigma_{\mathcal{I}'}, \text{MOD})$ where MOD contains all the indices of c_{a_i} from \mathcal{I}' with exception of \mathcal{A}_j (including the ssPIN required by S_j). Then, M sends $(\hat{\mathcal{I}}', \hat{\sigma}_{\mathcal{I}'})$ to MOA-ID which runs $b = \text{RS.Verify}(pk_{RS}, \hat{\mathcal{I}}', \hat{\sigma}_{\mathcal{I}'})$ and proceeds if $b = \text{true}$ and aborts otherwise.
2. M sends $(\mathcal{I}', \sigma_{\mathcal{I}'})$ to MOA-ID which runs $b = \text{RS.Verify}(pk_{RS}, \mathcal{I}', \sigma_{\mathcal{I}'})$ and proceeds if $b = \text{true}$ and aborts otherwise. Then, MOA-ID runs $(\hat{\mathcal{I}}', \hat{\sigma}_{\mathcal{I}'}) = \text{RS.Redact}(\mathcal{I}', pk_{RS}, \sigma_{\mathcal{I}'}, \text{MOD})$, whereas MOD contains the indices of all attributes in \mathcal{I}' with exception of \mathcal{A}_j (including the ssPIN required by S_j).

3: In this step, MOA-ID usually requests the generation of a qualified electronic signature from C_i . Here the following possibilities exist:

1. MOA-ID requests no signature, since \mathcal{I}' is signed and only available to C_i .
2. M produces a standard signature $\sigma = \text{DSS.Sign}(sk_{C_i}, m^*)$ for a special message m^* on behalf of C_i (which, however, allows unique identification of C_i by MOA-ID).
3. M produces a ring signature $\sigma = \text{AS.Sign}(sk_{C_i}, R, m^*)$ for a special message m^* on behalf of ring R including pk_{C_i} .

4: MOA-ID verifies the validity of signature σ either by running $b = \text{DSS.Verify}(pk_{C_i}, m^*, \sigma)$ or $b = \text{AS.Verify}(R, m^*, \sigma)$ (note that due to $\sigma_{\mathcal{I}'}$ and it's potentially redacted version can always be linked together, it is advisable that every citizen C_i uses a fixed ring all the time, i.e., all citizens in R use the same ring, since otherwise, e.g., when they are sampled uniform at random, then intersection attacks on the rings will soon reveal C_i).

5: MOA-ID takes all remaining attributes c_{a_i} from \mathcal{I}' (or $\hat{\mathcal{I}}'$) and computes for every such attribute $c'_{a_i} = \text{RE.ReEnc}(c_{a_i}, rk_{\text{MOA-ID} \rightarrow S_j})$ and assembles all these resulting c'_{a_i} into the SAML structure, which is then communicated to S_j . S_j can then decrypt all the attributes using sk_{S_j} .

Scheme 7.7: Approach 1: Using Proxy Re-Encryption and Redactable Signatures [Zwattendorfer and Slamanig, 2013a]

7.3.3.2 Approach 2: Using Anonymous Credentials

The Identity Link \mathcal{I} is augmented to \mathcal{I}' in a way that it does not include the sourcePIN but additionally all ssPIN's. Now, the SRA issues an anonymous credential Cred to every citizen for attr being all attributes in \mathcal{I}' . Essentially, a citizen then authenticates to a service provider by proving to MOA-ID the possession of a valid credential, i.e., MOA-ID checks whether the credential has been revoked or not. Note that for one show credentials, if the entire credential Cred is shown to MOA-ID, this amounts to a simple lookup in a blacklist. If the credential is not revoked, MOA-ID signs the credential to confirm that it is not revoked and the citizen performs via M a (non-interactive) proof by revealing the necessary attributes \mathcal{A}_j including the required ssPIN to S_j , who can then in turn verify the proof(s) as well as MOA-ID's signature.

Setup: SRA generates $(pk_{\text{SRA}}, sk_{\text{SRA}}) = \text{AC.KeyGen}(\kappa)$ and keeps secret sk_{SRA} and publishes pk_{SRA} . Furthermore, MOA-ID produces a key pair for a digital signature scheme $(pk_{\text{MOA-ID}}, sk_{\text{MOA-ID}}) = \text{DSS.KeyGen}(\kappa)$ and publishes $pk_{\text{MOA-ID}}$.

Citizen registration: At registration of citizen C_i at the SRA a modified Identity Link \mathcal{I}' is generated, which includes additional attributes a_{k+1}, \dots, a_m representing ssPINs for all sectors and other citizen attributes. Then, SRA and C_i run AC.Issue and the resulting credential Cred is stored on C_i 's Citizen Card.

Service provider registration: The registration for service provider S_j works as it is done now.

Authentication at online services:

- 1, 2 & 3:** After having received an authentication request from S_j , MOA-ID starts the citizen identification process by requesting C_i 's credential Cred and checks whether Cred has not been revoked. If Cred has not been revoked MOA-ID produces a signature $\sigma = \text{DSS.Sign}(sk_{\text{MOA-ID}}, \text{Cred}, \sigma)$ and sends σ along with a description of \mathcal{A}_j to M .
- 4:** M runs $b = \text{DSS.Verify}(pk_{\text{MOA-ID}}, \text{Cred}, \sigma)$ and if $b = \text{true}$ produces a non-interactive proof π which opens all attribute values of \mathcal{A}_j including the ssPIN required by S_j and sends $(\text{Cred}, \pi, \sigma)$ to S_j . Otherwise, M aborts.
- 5:** S_j computes $b = \text{DSS.Verify}(pk_{\text{MOA-ID}}, \text{Cred}, \sigma)$ and if $b = \text{true}$ verifies the proof π . If both checks verify, C_i is authenticated, otherwise S_j aborts.

Scheme 7.8: Approach 2: Using Anonymous Credentials [Zwattendorfer and Slamanig, 2013a]

Note that in this approach Cred is shown to MOA-ID, which however does not reveal the attribute values but makes revocation easier, since it only requires blacklist lookups. One could also use multi-show credentials, whereas M would then have to perform a proof with MOA-ID which convinces MOA-ID that the credentials are not revoked [Lapon et al., 2011], which provides stronger privacy guarantees.

A similar approach combining anonymous credentials and eIDs has been presented by Bjones et al. [2014].

7.3.3.3 Approach 3: Using Fully Homomorphic Encryption

This approach is a rather theoretic one and requires an FHE scheme which is also "key-homomorphic" as already discussed before in Section 7.3.2.7. The idea for this approach is the following: The Identity Link \mathcal{I} of a citizen holds the same attributes as now (and in particular the sourcePIN), but every attribute a_i is encrypted using an FHE scheme with the above described property under MOA-ID's public key for which MOA-ID does *not* hold the private key. Furthermore, this resulting \mathcal{I}' is conventionally signed by the SRA. Then, for authentication at S_j , the resulting \mathcal{I}' and the signature σ are sent to MOA-ID who checks the signature and homomorphically computes the respective ssPIN from the encrypted sourcePIN (without learning neither the sourcePIN nor the ssPIN). Then, for all encrypted attributes required by S_j (including the afore computed encrypted ssPIN), MOA-ID performs the "FHE re-encryption" to S_j 's public key. On receiving the respective information from MOA-ID, the service provider can decrypt all attribute values.

Setup: SRA generates $(pk_{\text{MOA-ID}}, evk_{\text{MOA-ID}}, sk_{\text{MOA-ID}}) = \text{FEH.KeyGen}(\kappa)$ and keeps secret $sk_{\text{MOA-ID}}$ and publishes $(pk_{\text{MOA-ID}}, evk_{\text{MOA-ID}})$. Furthermore, SRA produces a key pair for a digital signature scheme $(pk_{\text{SRA}}, sk_{\text{SRA}}) = \text{DSS.KeyGen}(\kappa)$ and publishes pk_{SRA} .

Citizen registration: During registration of citizen C_i at the SRA, for every $(A_i, a_i) \in \mathcal{I}$ SRA replaces a_i by $c_{a_i} = \text{FHE.Enc}(a_i, pk_{\text{MOA-ID}})$ and produces a signature $\sigma_{\mathcal{I}'} = \text{DSS.Sign}(sk_{\text{SRA}}, \mathcal{I}')$. Then, $(\sigma_{\mathcal{I}'}, \mathcal{I}')$ is stored on C_i 's citizen card.

Service provider registration: For the registration of service provider S_j , SRA computes $(pk_{S_j}, evk_{S_j}, sk_{S_j}) = \text{FEH.KeyGen}(\kappa)$ as well as $evk_{\text{MOA-ID}, S_j}$ and $f_{\text{MOA-ID}, S_j}$, and gives sk_{S_j} to S_j as well as $evk_{\text{MOA-ID}, S_j}$ and $f_{\text{MOA-ID}, S_j}$ to MOA-ID.

Authentication at online services:

- 1 & 2:** After having received an authentication request from S_j , MOA-ID starts the citizen identification process by requesting C_i 's Identity Link \mathcal{I}' and its corresponding signature $\sigma_{\mathcal{I}'}$. MOA-ID runs $b = \text{DSS.Verify}(pk_{\text{SRA}}, \mathcal{I}', \sigma_{\mathcal{I}'})$ and proceeds if $b = \text{true}$ and aborts otherwise. Let c_{a_k} be the encrypted sourcePIN, then MOA-ID computes $c'_{a_k} = \text{FHE.Eval}(f_H, c_{a_k} \parallel \text{FHE.Enc}(s_j, pk_{\text{MOA-ID}}), evk_{\text{MOA-ID}})$ where s_j is the sector specific identifier required by S_j and f_H is a circuit representing the evaluation of the SHA-1 hash function, which is used for ssPIN generation.
- 3:** In this step MOA-ID requests the generation of a qualified electronic signature from C_i . Here the following possibilities exist:
1. MOA-ID requests no signature, since \mathcal{I}' is signed and only available to C_i .
 2. M produces a standard signature $\sigma = \text{DSS.Sign}(sk_{C_i}, m^*)$ for a special message m^* on behalf of C_i (which, however, allows unique identification of C_i by MOA-ID).
 3. M produces a ring signature $\sigma = \text{AS.Sign}(sk_{C_i}, R, m^*)$ for a special message m^* on behalf of ring R including pk_{C_i} .
- 4:** MOA-ID verifies the validity of signature σ either by running $b = \text{DSS.Verify}(pk_{C_i}, m^*, \sigma)$ or $b = \text{AS.Verify}(R, m^*, \sigma)$.
- 5:** MOA-ID takes all attributes c_{a_i} in \mathcal{A}_j from \mathcal{I}' including c_{a_k} and computes for every such attribute $\hat{c}_{a_i} = \text{FHE.Eval}(f_{\text{MOA-ID}, S_j}, c_{a_i}, evk_{\text{MOA-ID}, S_j})$, thus performing a re-encryption to pk_{S_j} , and assembles all these resulting \hat{c}_{a_i} into the SAML structure, which is then communicated to S_j . S_j can now decrypt all attributes using sk_{S_j} .

Scheme 7.9: Approach 3: Using Fully Homomorphic Encryption [Zwattendorfer and Slamang, 2013a]

7.3.3.4 Evaluation

In this section the different approaches based on selected criteria targeting several aspects are evaluated e.g., evaluating the overall architecture or aspects regarding the individual entities. The selected criteria for evaluation are briefly described below and Table 7.1 shows a comparison of the three approaches. For the evaluation, the following symbols are used: \checkmark is used to indicate as the criterion being full applicable, \times as not applicable, and \approx as partly applicable. For quantitative criteria L for *low*, M for *medium*, and H for *high* is used.

Re-use of existing infrastructure: How much of the existing infrastructure of the Austrian eID system can be re-used or do a lot of parts need to be exchanged or modified?

Conformance to current workflow: Is the authentication process flow of the approach conform to the existing citizen card authentication process flow?

Scalability: Is the approach applicable in a large scale or not?

Practicability: Can the authentication process be carried out within a reasonable time frame?

Extensibility: Is the applied infrastructure of the approach easily extensible to new requirements, e.g., adding new sectors and thus requiring new ssPINs.

Middleware complexity: Does the approach require high complexity or computational power from the client-side middleware?

Service provider effort: How much effort is required by the service provider adopting a particular approach?

Trust in MOA-ID: Does the approach require MOA-ID being trusted?

Anonymity: Does the approach support citizens to be anonymous with respect to MOA-ID?

Unlinkability: Are users unlinkable to MOA-ID, i.e., can different authentications of one citizen be linked together?

Authentication without prior registration: The current Austrian eID system allows registration-less authentications. Hence, is this feature still possible or not?

Table 7.1: Evaluation of the various approaches [Zwattendorfer and Slamanig, 2013a]

Criterion	Approach 1	Approach 2	Approach 3
<i>Re-use of existing infrastructure</i>	≈	≈	≈
<i>Conformance to current workflow</i>	✓	≈	✓
<i>Scalability</i>	✓	✓, ≈	✓
<i>Practicability</i>	✓	✓, ≈	×
<i>Extensibility</i>	×	≈	✓
<i>Middleware complexity</i>	L	L, H	L
<i>Service provider effort</i>	L	M	H
<i>Trust in MOA-ID</i>	L	L	L
<i>Anonymity</i>	×, ✓	✓	×, ✓
<i>Unlinkability</i>	×	×, ✓	×
<i>Authentication without prior registration</i>	✓	✓	✓

In the following, some explanations are given why specific criteria could be fulfilled, partly fulfilled, or not-fulfilled by the respective approach.

Re-use of existing infrastructure: This criterion can only be partly fulfilled by all approaches since all approaches require some modification of the existing Austrian eID infrastructure. Approach 1 and 3 require some kind of additional governance structure, as proxy re-encryption keys for service providers have to be generated and managed by the SRA. Additionally, the attribute values of the existing Identity Link structure must be exchanged by encrypted values and the Identity Link needs to be augmented. For approach 1, the conventional signature of the Identity Link must also be exchanged by a redactable signature. In contrast to that, Approach 2 using anonymous credentials requires a complete re-structuring of the Identity Link. However, all approaches can still rely on the same basic architectural concept of the Austrian eID infrastructure, using MOA-ID as identity provider.

Conformance to current workflow: Approach 1 and 3 fully comply with the current citizen card authentication process flow, hence they follow the steps identification, ssPIN provision, and authentication. Approach 2 is slightly different as MOA-ID just checks if a provided credential is not revoked. The actual verification of the credential is carried out directly at the service provider.

Scalability: Basically, all approaches can be adopted in a large scale. Approach 1 and 3 are similar to the existing Austrian eID system as only a few attributes need to be exchanged within the Identity Link and the computational requirements for the middleware remain low. For approach 2, it must be distinguished whether one-show or multi-show anonymous credentials will be used. For one-show credentials, revocation checking is a very light-weight process and hence easy adoptable. In contrast to that, revocation for multi-show credentials is much more complex and not easily applicable for a large amount of users such as the Austrian population. Finally, any scalability doubts concerning MOA-ID can be neglected as it is running in a public cloud providing nearly unlimited resources.

Practicability: Approach 1 and 2 seem to be to date the most promising practical approaches. Approach 1 relies only on cryptographic mechanisms, which can already efficiently implemented. For approach 2, again it must be distinguished between one-show and multi-show credentials. For one-show credentials, proof generation requires moderate effort. For multi-show credentials, proof generation for non-revocation proofs is complex and computationally expensive. This gives a lot of load to the client-side middleware, which makes approach 2 using multi-show credentials quite impracticable. For approach 3, the assumptions that were made for FHE still require further research activities and are far away from any implementation. Although it is relied on public clouds, FHE is currently not practicable.

Extensibility: For adding new sectors, approach 1 would require a full exchange of the Identity Link as it must be re-signed when adding a new encrypted ssPIN. The same issue holds for approach 2, since a new credential incorporating the new ssPIN must be stored on the citizen card with exception when using scope-exclusive pseudonyms as proposed in ABC4Trust¹⁶. In approach 3, ssPIN's are computed from the encrypted version of the sourcePIN and no modifications of the Identity Link are required.

Middleware complexity: In approach 1, client-side middleware complexity is low as only redaction of the Identity Link is required. Middleware complexity in approach 2 depends on the type of anonymous credentials used. Proof computation of multi-show credentials is computationally expensive, which would impose a significant computational burden on M [Lapon et al., 2011] when taking into account that the system covers all citizens of Austria. For approach 3, middleware complexity is low again as its functionality is equal to current middleware implementations.

Service provider effort: The effort for service providers adopting approach 1 is low. Service providers just need to verify the data received by MOA-ID and do some decryption operations. For approach 2, the effort is slightly higher because service providers need to set up appropriate verification mechanisms for the claims provided by the user. The effort for service providers in approach 3 is the highest as FHE decryption is currently still computationally expensive.

Trust in MOA-ID: Since no sensitive citizen data such as the sourcePIN or any ssPIN are revealed to MOA-ID, no full trust is required. In approach 1 and 3 MOA-ID only sees encrypted citizen data. In approach 2 MOA-ID does only see the credential but none of its attribute values. However, some trust assumptions are required that MOA-ID works correctly, i.e., assuming that MOA-ID is *honest but curious* [Chen and Sion, 2010].

Anonymity: For approach 2, anonymity is obvious as the whole approach sets up on anonymous credentials. Achieving anonymity in approach 1 and 3 depends on the sub-processes to be chosen for citizen authentication (signature creation). Both approaches 1 and 3 rely on three similar alternative sub-processes. Sub-process 1 does not request a citizen signature and fully relies on the Identity Link's signature for citizen authentication, as the Identity Link is only available to the citizen. In this case, the citizen stays fully anonymous in the face of MOA-ID. In sub-process 2, citizen signature creation is requested by MOA-ID for citizen authentication. In this case, citizens are uniquely identifiable by MOA-ID due to pk_{C_i} . Finally, within sub-process 3 ring signatures are created and enable citizen anonymity with respect to the defined ring.

Unlinkability: For these approaches, it is very hard to achieve unlinkability with respect to MOA-ID. In approach 1 and 3 citizens are linkable because they always present the same Identity Link and corresponding signature. Citizens could only be unlinkable in approach 2, where one-show credentials provide linkability and multi-show credentials provide unlinkability.

¹⁶<https://abc4trust.eu>

Authentication without prior registration: This criterion can still be fulfilled by all of the three approaches.

Based on the results of the evaluation, it can be concluded that all approaches might be feasible but not all of them might be really practical when considering an implementation of a cloud-based approach instead of the current Austrian eID system. Approach 1 might be the best as it could be quickly realized and requires less effort for the client-side middleware and the service provider. However, linkability and higher efforts for extensions are the drawbacks of this approach. Depending on the type of anonymous credential system, approach 2 might also be practicable and possible to implement. Although it provides more complexity and efforts for the client-side middleware, compared to approach 1 it could provide full anonymity and unlinkability. Finally, although approach 3 has its advantages, e.g., in terms of extensibility, and would be promising for the future, it is currently not practicable. Implementations of fully homomorphic encryption schemes are currently still in the early stages which definitely hinder a fast adoption of this approach.

Nevertheless, according to this evaluation approach 1 does best with respect to the defined criteria. To further show the applicability of this approach, the complete Austrian eID system will be migrated into the public cloud using proxy re-encryption and redactable signatures, which is shown in the next section.

7.3.4 The complete Austrian eID Architecture in the Public Cloud

In this section, the author refers back to Section 3.6.3, where the Austrian eID architecture and the individual authentication use cases in Austria (identification and authentication of Austrian citizens, legal persons and electronic mandates, and identification and authentication of foreign citizens) are described. Based on these descriptions, in the following the move of relevant components of the complete Austrian eID architecture into the public cloud as well as the necessary process flow differences in the three individual identification and authentication use cases are described.

Referring back to Figure 3.13, the individual components of the Austrian eID architecture have different deployment approaches. MOA-ID follows a local deployment approach, where each service provider operates one MOA-ID instance in its domain. In comparison to that, the MIS and the SPR-GW are operated centrally in the domain of the *SourcePIN Register Authority*. Additionally, the deployment of the STORK infrastructure follows a central approach, where each member state operates a central gateway (PEPS) providing cross-border eID functionality.

As already discussed in Section 7.3.1, scalability is probably the main issue when considering a central deployment of MOA-ID as all citizen authentication processes will run through this central instance. This can easily lead to load bottlenecks, as theoretically the whole population of Austria could use this service. The same argument holds for the MIS, the SPR-GW, or the PEPS, which are currently all deployed centrally within a trusted environment. While the use of electronic mandates and cross-border authentications are still in its start-up phase, frequent usages are to be expected in the future. The use of electronic mandates in Austria gets increasing popularity. For instance, professional representation or natural-to-legal person representation constitute daily business in legal procedures. Additionally, representation of parents for their children or children for elderly people are frequent use cases especially in health services. Furthermore, cross-border identifications are steadily increasing as STORK is currently heavily pushed by the European Commission and will be the dominant authentication framework across Europe in the future.

Coping with such increased load may not be easy to handle within the current deployment scenarios, where each entity is deployed in a trusted data center. Therefore, the author proposes a move of the individual entities (MOA-ID, MIS, SPR-GW, PEPS) into a public cloud. Deployment in a public cloud could definitely mitigate any scalability issues due to the characteristics provided by a public cloud environment. However, a move of such trusted service into a public cloud brings up new obstacles,

especially with respect to citizen’s privacy. While privacy in the current scenarios is ensured through organizational means, in the following sections the author illustrates how such a move of these trusted services into a public cloud can be successfully realized using cryptographic technologies (by particularly using proxy re-encryption) by still preserving citizens’ privacy.

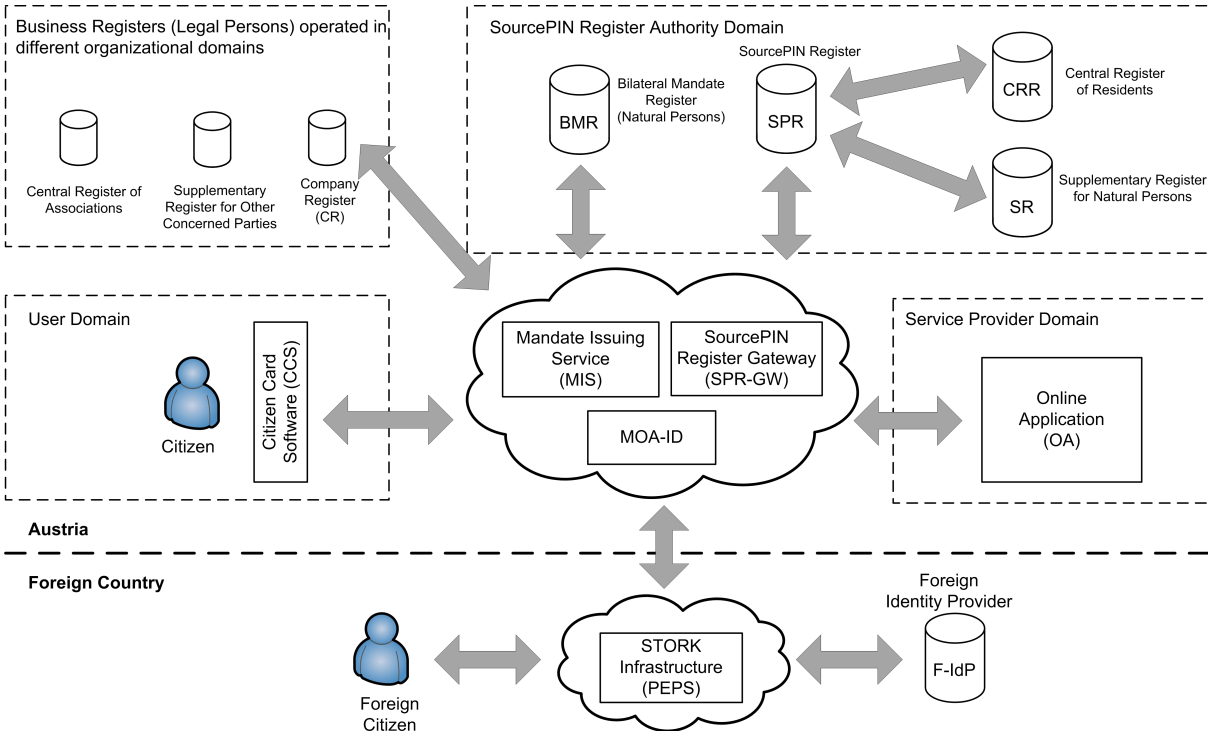


Figure 7.10: The Austrian eID Architecture in the Public Cloud

Figure 7.10 illustrates the new architecture of the Austrian eID system when moving important components into the public cloud. In this figure, for simplicity the components MOA-ID, MIS, and SPR-GW were subsumed to be deployed in one public cloud. However, all three components could be operated by different public cloud providers. The STORK PEPS component is assumed to be operated in a different public cloud, as it will be under responsibility of the foreign country.

For being able to move the Austrian eID infrastructure into a public cloud, a few minor changes in the corresponding infrastructure are necessary. In the next subsections it is explained in detail which changes are required. Furthermore, the adapted process flows of the individual use cases to support an operation of the Austrian eID system in a public cloud are described.

7.3.4.1 Identification and Authentication of Austrian Citizens

Basically, similar to the current situation it is assumed that the *SourcePIN Register Authority* (SRA) is a trusted entity. In this setup scenario, the SRA will be also responsible for the issuance of a slightly modified Identity Link. Additionally, the SRA will manage service provider registration to build appropriate trust relationships between the individual entities.

Setup: In the proposed cloud scenario, it is assumed that the modified Identity Link (denoted by \mathcal{I}') does not contain a sourcePIN but furthermore all ssPINs according to all governmental sectors. Furthermore, all ssPINs are encrypted using a proxy re-encryption scheme, hence every $(A_i, a_i) \in \mathcal{I}'$ is replaced by the SRA by the encrypted attributes $c_{a_i} = \text{RE.Enc}(params, a_i, sk_{SRA})$. The ssPINs and additional citizen attributes (e.g., name, date of birth) are encrypted under the public key of MOA-ID (pk_{MOA-ID}). The key pair $(pk_{MOA-ID}, sk_{MOA-ID})$ is generated by the SRA. However, the SRA as

trusted entity keeps the corresponding private key (sk_{MOA-ID}) and thus MOA-ID will not be able to decrypt the individual attributes. In the current approach, conventional signatures are used to ensure authenticity and integrity of the Identity Link. However, in this cloud-based approach the SRA signs the modified Identity Link using a redactable signature scheme resulting in $\sigma_{\mathcal{I}'} = \text{RS.Sign}(sk_{\text{SRA}}, \mathcal{I}')$. By this, each individual attribute of the modified Identity Link can be redacted. The modified Identity Link \mathcal{I}' is finally stored on the citizen card. In this setup, it is further assumed that the signature creation certificate stored on the citizen card does not contain any citizen identifying information.

In addition, service providers need to register their online applications at the SRA. The set of service providers is denoted as $S = \{S_1, \dots, S_\ell\}$. For service provider registration, the SRA produces a private key $sk_{S_j} = \text{RE.KeyGen}(params)$ for S_j and a re-encryption key $rk_{MOA-ID \rightarrow S_j} = \text{RE.RKGen}(params, sk_{MOA-ID}, MOA-ID, S_j)$. The key sk_{S_j} is issued to S_j and $rk_{MOA-ID \rightarrow S_j}$ to MOA-ID. It is further assumed that an appropriate signing key pair $(pk'_{MOA-ID}, sk'_{MOA-ID})$ for MOA-ID is available.

Process Flow: Figure 7.11 illustrates the process flow using the cloud-based approach. In fact, the process flow is very similar as in the current scenario. However, the differences will be highlighted next.

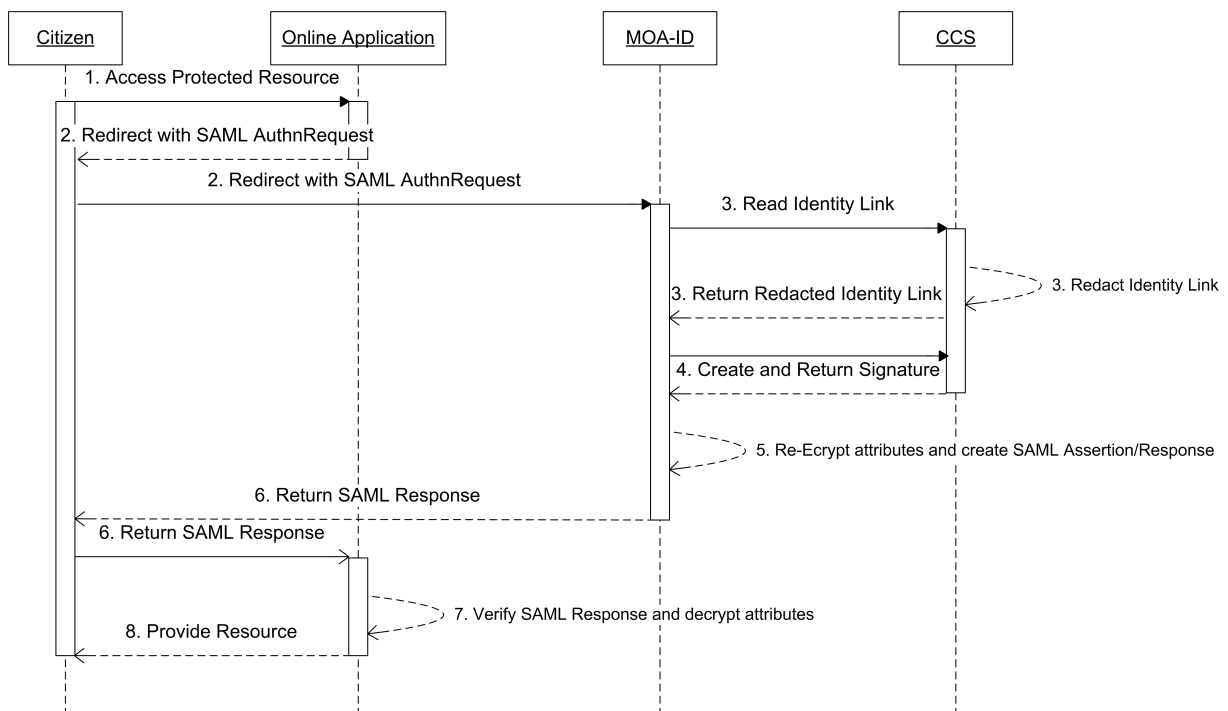


Figure 7.11: Process flow of Austrian citizen identification and authentication in the cloud approach

1. The citizen wants to access a protected resource at the online application, which requires proper authentication (Same as in the current approach – cf. Section 3.6.4).
2. The online application assembles a SAML authentication request, which is transmitted via HTTP-Redirect to MOA-ID (Same as in the current approach – cf. Section 3.6.4).
3. In this step, MOA-ID sends an appropriate XML request to the CCS for retrieving the Identity Link from the citizen card. This request further includes now the governmental sector s . By having s , the CCS can now redact all ssPINs except the ssPIN corresponding to s . The redacted Identity Link \mathcal{I}' is returned to MOA-ID and verified.

4. MOA-ID requests the creation of a qualified electronic signature indicating the willingness of the citizen for online application authentication. The citizen creates a signature, which is sent back to MOA-ID and verified. The citizen authorizes this request appropriately depending on the CCS implementation (Same as in the current approach – cf. Section 3.6.4).
5. Instead of deriving an ssPIN, MOA-ID re-encrypts the attributes c_{a_i} of the redacted Identity Link \mathcal{I}' for the authentication requesting service provider S_j by using the re-encryption key $rk_{MOA-ID \rightarrow S_j}$. This results in $c_{S_j} = \text{RE.ReEnc}(rk_{MOA-ID \rightarrow S_j}, c_{a_i})$. Furthermore, MOA-ID signs the result coming out with $\sigma_{MOA-ID} = \text{DSS.Sign}(sk_{MOA-ID}, c_{S_j})$. More precisely, the complete SAML assertion/response is signed.
6. MOA-ID returns the SAML assertion/response, which includes all re-encrypted attributes, to the online application via HTTP-POST.
7. The online application verifies the SAML response (σ_{MOA-ID}), extracts the encrypted citizen attributes c_{S_j} , and decrypts them using the private key sk_{S_j} .
8. After successful verification, the online application grants access to the resource (Same as in the current approach – cf. Section 3.6.4).

7.3.4.2 Identification and Authentication on behalf

Setup: In this scenario, again it is assumed that the modified Identity Link \mathcal{I}' is used. Furthermore, in this scenario it is additionally relied on the encryption and decryption functionality of the Austrian citizen card. Besides a signature key pair, each Austrian citizen C has an encryption key pair (pk_C, sk_C) stored on her citizen card. This key pair is also generated by the SRA.

In addition to (pk_{S_j}, sk_{S_j}) and $rk_{MOA-ID \rightarrow S_j}$, the SRA has to generate additional encryption and re-encryption keys for the individual entities required for mandate processing. For the MIS and for the CR the keys (pk_{MIS}, sk_{MIS}) and (pk_{CR}, sk_{CR}) are created. Since the MIS will be operated in the cloud, the SRA keeps secret sk_{MIS} and only distributes pk_{MIS} to the MIS. In addition, the following re-encryption keys are generated: $rk_{MOA-ID \rightarrow MIS}$, $rk_{MIS \rightarrow CR}$, and $rk_{MIS \rightarrow MOA-ID}$. It is further assumed that appropriate signing keys are available for the individual entities: $(pk'_{MOA-ID}, sk'_{MOA-ID})$, (pk'_{MIS}, sk'_{MIS}) , and (pk'_{CR}, sk'_{CR}) .

Process Flow: Figure 7.12 illustrates the process flow for representative authentication in the cloud-based approach. In the following, the process flow is described in detail.

1. This process step is equal to normal Austrian citizen authentication. However, the citizen indicates that she wants to authenticate on behalf of somebody (e.g., by activating a checkbox) (Same as in the current approach – cf. Section 3.6.5).
2. The online application assembles a SAML authentication request, which is transmitted via HTTP-Redirect to MOA-ID (Same as in the current approach – cf. Section 3.6.5).
3. MOA-ID sends a request for retrieving the Identity Link to the CCS. The CCS redacts all ssPINs which are not required in this authentication scenario. This includes all ssPINs except the one the service provider belongs to ($ssPIN_{SP}$) and the ssPINs required for querying the individual registers for mandate information ($ssPIN_{CR}$ in this example).
4. MOA-ID requests the creation of a qualified electronic signature indicating the willingness of the citizen for online application authentication. The citizen creates a signature, which is sent back to MOA-ID and verified. The citizen authorizes this request appropriately depending on the CCS implementation (Same as in the current approach – cf. Section 3.6.5).

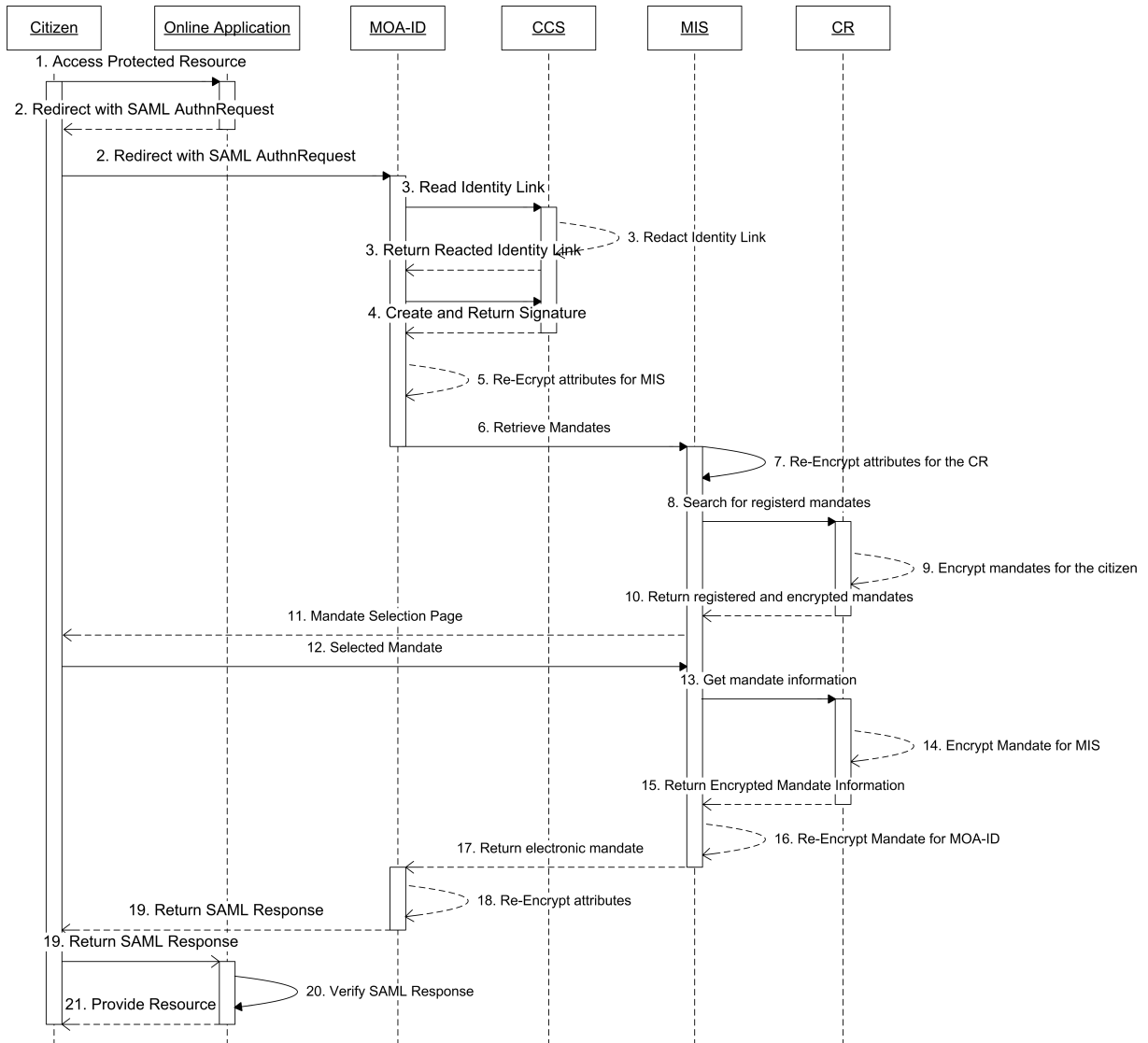


Figure 7.12: Process flow representing a legal person electronically in the cloud approach

5. In this step, MOA-ID re-encrypts the attribute $ssPIN_{CR}$ from \mathcal{I}' for the MIS using $rk_{MOA-ID \rightarrow MIS}$ resulting in $c_{MIS} = RE.ReEnc(rk_{MOA-ID \rightarrow MIS}, ssPIN_{CR})$. This re-encryption result is signed by MOA-ID which outputs $\sigma_{MOA-ID} = DSS.Sign(sk'_{MOA-ID}, c_{MIS})$.
6. MOA-ID sends the tuple $(c_{MIS}, \sigma_{MOA-ID})$ to the MIS for mandate retrieval.
7. The MIS verifies σ_{MOA-ID} and re-encrypts c_{MIS} for the CR using $rk_{MIS \rightarrow CR}$ and signs the result c_{CR} . The resulting signature is denoted as $\sigma_{MIS} = DSS.Sign(sk'_{MIS}, c_{CR})$.
8. The MIS sends (c_{CR}, σ_{MIS}) to the CR. The CR verifies σ_{MIS} , decrypts c_{CR} , and searches its register for mandates using the plain $ssPIN_{CR}$. In this example, it is assumed that the mandate information $mand$ and the corresponding mandate ID $mandID$ has been found. The CR signs the mandate and the signature $\sigma_{CR} = DSS.Sign(sk_{CR}, mand, mandID)$ is calculated.
9. Since the citizen is known to the CR (the mandate contains further information of the citizen), it can encrypt the mandate for the citizen using pk_C resulting in $c_C = PKE.Enc(pk_C, mand, mandID, \sigma_{CR})$. The CR again signs the encryption result for ensuring integrity and authenticity calculating $\sigma'_{CR} = DSS.Sign(sk_{CR}, c_C)$.

10. The data (c_C, σ'_{CR}) are returned to the MIS, which verifies the signature¹⁷.
11. The MIS presents the citizen a selection page of all available mandates for her. In this example, c_C is sent to the citizen.
12. The citizen decrypts c_C and verifies σ_{CR} . The citizen selects the mandate she wants to use for authentication. In this scenario it is assumed that she wants to act on behalf of a company and thus selects $mandID$. The citizen signs $mandID$ resulting in $\sigma_C = \text{DSS.Sign}(sk_C, mandID)$. $(mandID, \sigma_C)$ are returned to the MIS.
13. The MIS queries again the CR for retrieving all necessary information for the selected mandate by using $(mandID, \sigma_C)$.
14. The CR calculates $c_{MIS} = \text{RE.Enc}(pk_{MIS}, mand, mandID)$ and signs it resulting in $\sigma''_{CR} = \text{DSS.Sign}(sk_{CR}, c_{MIS})$.
15. The CR transmits (c_{MIS}, σ''_{CR}) to the MIS.
16. The MIS verifies σ''_{CR} and re-encrypts c_{MIS} for MOA-ID using $rk_{MIS \rightarrow MOA-ID}$. The MIS signs this re-encryption result c_{MOA-ID} by calculating the signature $\sigma'_{MIS} = \text{DSS.Sign}(pk'_{MIS}, c_{MOA-ID})$.
17. The MIS returns $(c_{MOA-ID}, \sigma'_{MIS})$ to MOA-ID.
18. MOA-ID verifies σ'_{MIS} and re-encrypts the data c_{MOA-ID} , $ssPIN_{SP}$, and c_{a_i} for S_j using the key $rk_{MOA-ID \rightarrow S_j}$. The result c_{S_j} is additionally signed using sk'_{MOA-ID} resulting in σ'_{MOA-ID} .
19. MOA-ID assembles $(c_{S_j}, \sigma'_{MOA-ID})$ in the SAML response and transmits it to the online application.
20. The online application verifies the signature σ'_{MOA-ID} and decrypts the mandate and citizen information c_{S_j} by using the key sk_{S_j} .
21. If verification is successful the online application grants access. The citizen is now able to do online procedures on behalf of the selected company (Same as in the current approach – cf. Section 3.6.5).

A more detailed discussion on this approach can be found in Zwattendorfer and Slamanig [2013c].

7.3.4.3 Identification and Authentication of Foreign Citizens

Setup: In the previous scenarios it was assumed that the SRA is a trusted entity that issues appropriate key material to the involved entities in the Austrian eID system. In this scenario it must be dealt with a cross-border scenario, hence a trusted entity being able to serve entities across borders is needed. In the current STORK concept, the European Commission (EC) will play a central role managing trust across the involved STORK entities. Therefore, also for this scenario the EC is assumed being the entity that issues secure key material to the individual STORK entities and thus a detailed description on that is skipped. In this scenario, the EC generates (pk_{PEPS}, sk_{PEPS}) and issues pk_{PEPS} to the PEPS only. It keeps secret sk_{PEPS} . Furthermore, the SRA issues $(pk_{MOA-ID}, sk_{MOA-ID})$, $(pk_{SPR-GW}, sk_{SPR-GW})$, (pk_{SP}, sk_{SP}) , and (pk_{SR}, sk_{SR}) . It keeps secret sk_{MOA-ID} and sk_{SPR-GW} . The other keys are distributed to the respective entities. In addition, the EC generates a re-encryption key

¹⁷In this scenario, for simplicity the CR has been queried for mandate information only. However, the MIS actually queries all registers that have mandate information available.

$r_{pk_{PEPS} \rightarrow MOA-ID}$ and the SRA the re-encryption keys $r_{pk_{MOA-ID} \rightarrow SPR-GW}$, $r_{pk_{SPR-GW} \rightarrow SR}$, and $r_{pk_{MOA-ID} \rightarrow SP}$. For further explanations, the identity data of the foreign citizen is denoted as f^c_{data} .

It is further assumed that appropriate signing keys are available for the individual entities:

$(pk'_{MOA-ID}, sk'_{MOA-ID})$, (pk'_{PEPS}, sk'_{PEPS}) , $(pk'_{F-IdP}, sk'_{F-IdP})$, $(pk'_{SPR-GW}, sk'_{SPR-GW})$, and (pk'_{SR}, sk'_{SR}) .

Process Flow: Figure 7.13 illustrates the process flow identifying and authenticating a foreign citizen in the cloud-based approach. In the following, the process flow is described in detail.

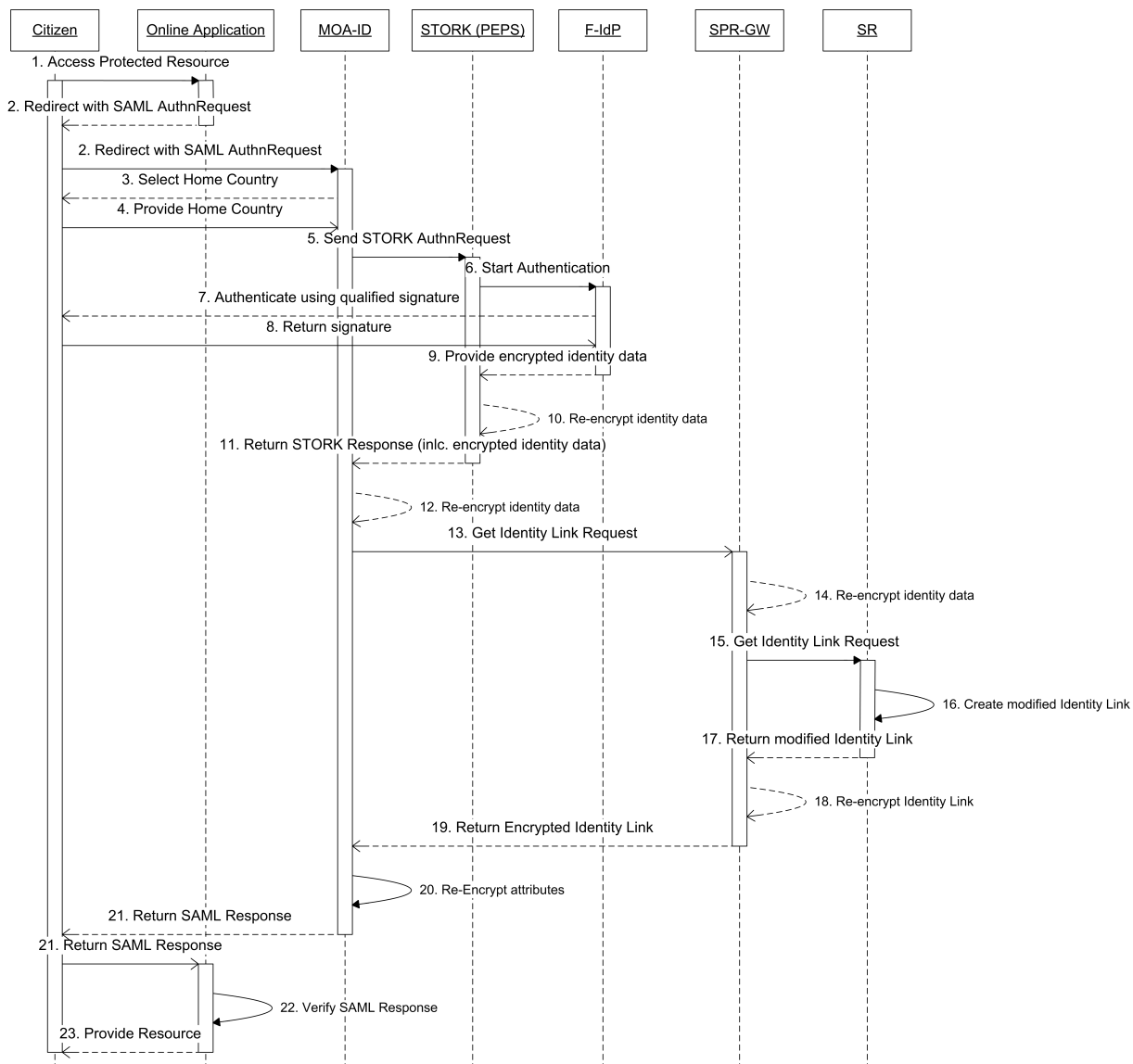


Figure 7.13: Process flow representing identifying and authenticating a foreign citizen in the cloud approach

1. A foreign EU citizen wants to access a service of an Austrian online application (Same as in the current approach – cf. Section 3.6.6).
2. The online application assembles an appropriate SAML authentication request and sends it to MOA-ID (Same as in the current approach – cf. Section 3.6.6).

3. MOA-ID presents the foreign citizen a page where the citizen can select her country of origin (Same as in the current approach – cf. Section 3.6.6).
4. The citizen provides her home country she originates from (Same as in the current approach – cf. Section 3.6.6).
5. According to the STORK idea, the foreign citizen will be authenticated in her home country. Therefore, the citizen is redirected to a single gateway (PEPS) in the foreign country, being part of the STORK infrastructure. For starting this authentication process, MOA-ID transmits a STORK authentication request to the foreign PEPS. The PEPS selects an appropriate foreign IdP (F-IdP), where the citizen actually authenticates (Same as in the current approach – cf. Section 3.6.6).
6. The PEPS forwards the authentication request to the F-IdP (Same as in the current approach – cf. Section 3.6.6).
7. The F-IdP requests the citizen to authenticate using a qualified signature (Same as in the current approach – cf. Section 3.6.6).
8. The qualified signature is returned to the F-IdP (Same as in the current approach – cf. Section 3.6.6).
9. The Foreign IdP is assumed to be a trusted entity and that it encrypts the foreign citizen's identification data for the PEPS using pk_{PEPS} resulting in $c_{PEPS} = \text{RE.Enc}(pk_{PEPS}, f_{c_{data}})$. Furthermore, c_{PEPS} is signed using sk'_{F-IdP} resulting in σ_{F-IdP} . Both results $(c_{PEPS}, \sigma_{F-IdP})$ are sent to the PEPS.
10. The PEPS verifies σ_{F-IdP} and re-encrypts c_{PEPS} for MOA-ID using $c_{MOA-ID} = \text{RE.ReEnc}(rk_{PEPS \rightarrow MOA-ID}, c_{PEPS})$. In addition, c_{MOA-ID} is signed using sk'_{PEPS} resulting in σ_{PEPS} .
11. The tuple $(c_{MOA-ID}, \sigma_{PEPS})$ is sent to MOA-ID.
12. MOA-ID verifies σ_{PEPS} and again re-encrypts the foreign citizen data for the SPR-GW: $c_{SPR-GW} = \text{RE.ReEnc}(rk_{MOA-ID \rightarrow SPR-GW}, c_{MOA-ID})$. c_{SPR-GW} and the governmental sector s of the SP is signed resulting in $\sigma_{MOA-ID} = \text{DSS.Sign}(sk_{MOA-ID}, c_{SPR-GW}, s)$.
13. The tuple $(c_{SPR-GW}, s, \sigma_{MOA-ID})$ is sent to the SPR-GW.
14. The SPR-GW verifies σ_{MOA-ID} and does the re-encryption for the SR: $c_{SR} = \text{RE.ReEnc}(rk_{SPR-GW \rightarrow SR}, c_{SPR-GW})$. Again, the values c_{SR} and s are signed resulting in σ_{SPR-GW} .
15. The tuple $(c_{SR}, s, \sigma_{SPR-GW})$ is sent to the SPR-GW.
16. The SR verifies σ_{SPR-GW} , decrypts c_{SR} using sk_{SR} , and registers the foreign citizen. During registration, a new modified Identity Link \mathcal{I}' is created for the foreign citizen. Since the modified Identity Link is created on the fly, it just contains the encrypted $ssPIN$ for the sector s and all other $ssPINs$ are redacted.
17. This new Identity Link \mathcal{I}' is encrypted for the SPR-GW using pk_{SPR-GW} resulting in c'_{SPR-GW} . The result c'_{SPR-GW} is signed by applying $\sigma_{SR} = \text{DSS.Sign}(sk_{SR}, c'_{SPR-GW})$. Both results $(c'_{SPR-GW}, \sigma_{SR})$ are transferred to the SPR-GW.
18. The SPR-GW again verifies σ_{SR} , re-encrypts c'_{SPR-GW} applying $c'_{MOA-ID} = \text{RE.ReEnc}(rk_{SPR-GW \rightarrow MOA-ID}, c'_{SPR-GW})$, and signs the result c'_{MOA-ID} applying $\sigma'_{SPR-GW} = \text{DSS.Sign}(sk_{SPR-GW}, c'_{MOA-ID})$.

19. The re-encrypted Identity Link c'_{MOA-ID} and σ'_{SPR-GW} are transmitted to MOA-ID.
20. MOA-ID verifies σ_{SPR-GW} , re-encrypts $c_{SP} = \text{RE.ReEnc}(rk_{MOA-ID \rightarrow SP}, c'_{MOA-ID})$, and signs c_{SP} applying $\sigma'_{MOA-ID} = \text{DSS.Sign}(sk_{MOA-ID}, c_{SP})$. MOA-ID also assembles a SAML response including c_{SP} and σ'_{MOA-ID} to be transferred to the SP.
21. MOA-ID returns the SAML response to the online application via HTTP-POST (Same as in the current approach – cf. Section 3.6.6).
22. The SP verifies σ'_{MOA-ID} and decrypts c_{SP} using sk_{SP} . Based on the included attributes, the SP can either grant or deny access.
23. After successful verification, the online application grants access to the resource (Same as in the current approach – cf. Section 3.6.6).

7.3.5 Identity as a Service-Model for Electronic Identities

In this section a new user-centric identification and authentication model is proposed, which is particularly applicable for semi-trusted environments (in terms of data protection and privacy) such as the public cloud. The model allows the usage of both server-side and client-side approaches for user data storage, while still putting users under full control of their data, i.e., providing selective disclosure in both approaches.

The previous sections explained how the Austrian eID architecture could be migrated into semi-trusted environments such as the public cloud using appropriate cryptographic technologies. Referring to Zwattendorfer and Slamanig [2013a], they concluded that the approach by using proxy re-encryption and redactable signatures is the most practicable one.

However, a main drawback of the approach proposed in Section 7.3.3.1 and Section 7.3.4 is that the approach is strongly tailored to the Austrian eID system, which does not allow for general applicability. Furthermore, it requires quite cumbersome registration processes of identity providers and service providers at a trusted authority. In addition, the approach is not fully user-centric as the user data are encrypted for a trusted third party and not the user herself.

Since proxy re-encryption seems to be a promising approach for modeling eID systems also in semi-trusted environments such as the public cloud, based on the previous work described in Section 7.3.3 a more generic identification and authentication model for semi-trusted environments has been developed. This model enhances the model proposed in Section 7.3.3.1 in terms of privacy as the user is put into full control of her identity data.

Figure 7.14 illustrates the new identification and authentication model for eIDs, which is applicable as an *Identity as a Service-Model* in semi-trusted environments. The following entities are involved in this model:

Registration authority: The registration authority (RA) is a trusted entity which issues qualified and authentic identity data to the user. The identity data can be either stored on client-side, e.g., a secure token, or on server-side at a trusted identity and/or attribute provider.

User: The user wants to access protected resources of a service provider. For gaining access, the user can reveal selected identity data issued from the registration authority.

Service provider: The service provider (SP) offers different resources or services which require qualified identification and authentication using eIDs.

Identity provider: The identity provider (IdP) is deployed in the cloud, meaning in a semi-trusted environment. The identity provider manages the identification and authentication process for the

service provider and provides the service provider with asserted data via well-known protocols such as SAML or OpenID.

Identity and/or attribute provider: This entity holds qualified and authentic identity data of the user on server-side.

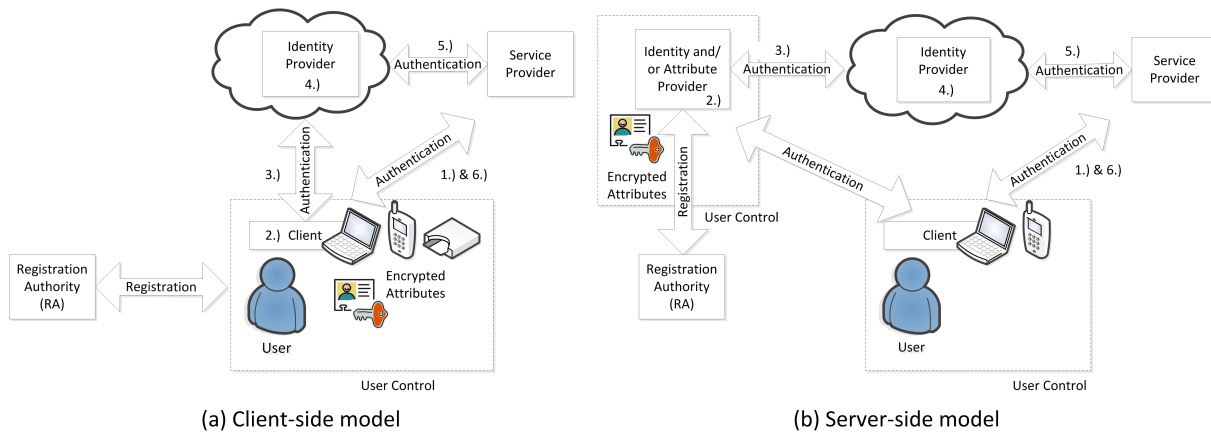


Figure 7.14: A user-centric and privacy-preserving Identity as a Service-Model for eIDs. [Sla-manig et al., 2014]

In this proposed model for eIDs, identity data will be encrypted (using a proxy re-encryption scheme) by the registration authority for the user in such a way that only the user is able to decrypt the data. Encrypting attributes only for the user gives the user sole control to her data. This form of encryption and selective disclosure enables user-centricity on the one side, and the support of semi-trusted identity providers on the other side, as only encrypted data are provided to the identity provider. The user can give a subset of re-encrypted attributes to a service provider such that it can only be decrypted by this service provider (selective disclosure). Furthermore, the encrypted identity data are digitally signed by the trusted registration authority using a malleable signature scheme (redactable signatures). Signing the data has basically two functions. First, the data are authentic and integrity can be assured as the data are signed by the trusted registration authority. Second, by using a malleable signature scheme, it can be guaranteed that only required (encrypted) attributes can be disclosed to the service provider without invalidating the signature of the trusted registration authority. Finally, the model can be easily integrated into existing infrastructures as existing identity protocols already support the transfer of encrypted data and digital signatures out-of-the-box.

In the following, details on the registration process and the identification and authentication process when applying this model are given. The registration process has to be conducted only once, whereas the latter must be performed for each access to a protected resource.

Registration Process: Qualified and authentic identity data issuance is carried out by a trusted third party, the registration authority. Data provisioning is done during an appropriate registration process between the user and the registration authority. Details of the registration process are out of scope of this model and are dependent on the respective eID approach. Nevertheless, registered identity data are encrypted for the user using a proxy re-encryption scheme and signed by the registration authority using a redactable signature scheme. The encrypted and signed data can be either stored on a secure token featuring a client-side approach or on a remote server modeling a server-side approach. However, irrespective of the underlying approach, identity data are always provided by a trusted authority in an authentic and qualified manner. This allows the approach to be used for national eID solutions.

Identification and Authentication Process: Figure 7.14 also illustrates the identification and authentication process when applying this model. For better illustration, it is assumed that the identity provider is running in a public cloud to fully feature the Identity as a Service paradigm. Basically, the identity provider in the public cloud has three main responsibilities: 1.) user authentication and verification of authenticity of encrypted identity data, 2.) re-encrypting the identity data for the service provider, and 3.) structuring and transferring identity data to the service provider. To illustrate the individual responsibilities, an authentication process using this model is briefly described.

1. The user wants to access a protected resource at the service provider that requires authentication. Authentication is carried out by the identity provider. Hence, the user is forwarded there.
2. The user redacts all encrypted attributes which she does not want to disclose to the service provider. Depending on the underlying approach, this can be done on client-side or server-side. However, in both cases the user remains under sole control of her data. At the same time, the user also generates a re-encryption key based on a public key of the service provider and the user's private key.
3. The redacted identity data and the re-encryption key are sent to the identity provider in the cloud.
4. The identity provider verifies the authenticity and integrity of the identity data, i.e., the signature, and re-encrypts it for the service provider. Additionally, the identity data are structured accordingly for being transferred to the service provider.
5. The identity provider transfers the data to the service provider using appropriate existing identity protocols such as SAML or OpenID. To ensure authenticity and integrity, the identity provider signs the transferred data.
6. The service provider verifies the received data and decrypts the provided and asserted attributes. Based on the attribute values, the service provider either grants or denies access.

To securely and reliably support these functionality, some assumptions are made:

Assumptions: It is assumed that whenever public parameters or public keys are used that they are available in an authentic fashion, e.g., via a PKI. Furthermore, the channels between all parties provide confidentiality as well as authenticity, e.g., via the use of TLS.

The applicability of this generic *Identity as a Service-Model for eIDs* has been demonstrated by Slamanig et al. [2014] by applying it to the Austrian eID concept.

7.4 Chapter Conclusions

Secure and reliable identity management plays a vital role in several security-sensitive areas of applications e.g., in e-Government, e-Business, or e-Health. Due to the increasing number of cloud computing adoption and the deployment of security-sensitive cloud applications, secure identity management becomes also more and more important in the cloud domain. Most cloud computing service providers secure their offered cloud services by username/password schemes, which have been proven to be weak. While such schemes may be sufficient for simple personalized services, e-Government or e-Health applications in the cloud require more reliable and stronger mechanisms. To bypass this issue, the author presented how various national eIDs can be used for secure cloud authentication. To achieve this, the STORK eID interoperability framework, which will be the relevant identification and authentication framework across Europe in future, was properly extended. Furthermore, usability was increased by additionally enabling single sign-on (SSO). By this, the author has shown how secure and qualified identification and authentication mechanisms such as eIDs could be used for securing SaaS applications.

In addition, the author has also shown how existing identity management systems for eIDs could be successfully migrated into the public cloud without losing any privacy for citizens.

Outsourcing identity management systems to the cloud can bring up several benefits such as higher scalability or cost savings, since no in-house infrastructure needs to be hosted and maintained. However, the move of an identity management system into the public cloud brings up new obstacles since the cloud cannot be considered trustworthy. The author encountered these obstacles by introducing and evaluating three distinct approaches relying on different cryptographic technologies (proxy re-encryption and redactable signatures, anonymous credentials, and fully homomorphic encryption). Based on the evaluation, the approach using proxy re-encryption and redactable signatures turned out to do best as it could be quickly realized and requires less effort for changing existing infrastructure. The applicability of this approach has been further demonstrated by applying it to the Austrian eID system. Finally, this approach builds the basis for the next chapter where a new cloud identity model is proposed, which enables a federated cloud identity architecture by still preserving users' privacy.

Chapter 8

Federated Identity as a Service

The previous chapter basically elaborated on deploying one identity provider or identity broker centrally in a public cloud. However, this model reaches its limits as both service provider and user need to rely on the same identity provider or identity broker for authentication. This limits flexibility for users to select their own preferred and trusted identity provider or broker. To bypass this issue, the author proposes a new cloud identity model where identity brokers in the cloud are federated. The federation allows both users and service providers greater flexibility in choosing their desired identity provider/identity broker. As those entities are deployed and operated in the public cloud, emphasis will be put on privacy-preservation to avoid undesired inspection of personal data by the cloud provider.

The chapter is structured as follows. The motivation for this new model and the problem statement is elaborated in more detail in Section 8.1. The new *Federated Identity as a Service-Model* is described in Section 8.2, whereas the enhanced version preserving users' privacy by using proxy re-encryption is explained in Section 8.3. A proof of concept implementation of this *Privacy-Preserving Federated Identity as a Service-Model* is described in Section 8.4. Afterwards, in Section 8.5 the concept of the *Privacy-Preserving Federated Identity as a Service-Model* is applied to an existing use case, namely to the STORK PEPS approach (cf. Section 5.5.4.1). Finally, all cloud identity models described in Chapter 7 and in this chapter will be discussed and evaluated based on selected criteria.

8.1 Motivation and Problem Statement

The single *Cloud Identity Broker-Model* (cf. Section 7.1.3.1) does best compared to all other cloud identity-management models of Section 7.1 in terms of flexibility. Besides the benefits the cloud delivers off the shelf, further advantages of *Cloud Identity Broker-Model* are the support of multiple identity providers by hiding their complexity from service providers at the same time. Nevertheless, still a couple of drawbacks can be found when applying this model.

One major drawback of this model is that both the user and the service provider must rely on the same central entity, namely the cloud identity broker. Hence, both are more or less dependent on the functionality the cloud identity broker supports. Authentication using the cloud identity broker is only possible if the cloud identity broker supports one identity provider the user is registered with. If this is not the case, users are actually cut off service provisioning by the service provider as no successful authentication process through the cloud identity broker is possible. In addition, service providers are limited to the functionality and features offered by the cloud identity broker. If the cloud identity broker has, for instance, no contract with a specific identity provider the service provider actually requires (e.g., an identity provider that supports national eID solutions for qualified and unique identification and authentication), the service provider still needs to implement the communication with such identity providers on their own. Furthermore, if the communication interface used between the service provider

and the cloud identity broker is suddenly quit, the service provider is cut off service provisioning. The implementation of a new interface provided by the cloud identity broker would cost a lot of money and efforts. Summing up, in the simple *Cloud Identity Broker-Model* both the user and the service provider have no real free choice on the cloud identity broker they want to communicate with. Both need to rely on and trust the same cloud identity broker irrespective if it fully satisfies their demands and requirements or not.

A second major drawback relating to the *Cloud Identity Broker-Model* – but actually applicable to all cloud identity-management models when deployed in a public cloud – is privacy. Privacy is one of the main issues with respect to cloud computing [Pearson and Benameur, 2010; Zissis and Lekkas, 2012]. In this particular case, cloud providers might be interested or curious in inspecting identity data processed or stored by the identity broker in the cloud. Moreover, such sensitive data may be leaked if the identity broker gets compromised.

To overcome these issues, a new model architecture for identity management in the cloud is proposed. In particular, this new cloud identity management-Model allows the free selection of the desired cloud identity broker for both, the service provider and the user. The requirement for relying on the same cloud identity broker is not needed anymore, which enables greater flexibility. In addition, appropriate cryptographic mechanisms (digital signatures and proxy re-encryption – cf. Section 7.3.2.1 and 7.3.2.6) are used to enhance users' privacy.

8.2 Federated Identity as a Service-Model

The proposed new cloud identity management model relies on a federated approach. The so-called *Federated Identity as a Service-Model* (*Federated Cloud Identity Broker-Model*) [Zwattendorfer et al., 2013a] solves the issue on being dependent on just one and the same identity broker for both, the service provider and the user. The dependency on one single cloud identity broker is removed by using multiple cloud identity brokers that are able to communicate with each other. In this federated model, users and service providers do not need to rely on the same identity broker as authenticating authority. Both can actually contract their individual identity broker of choice, which offers greater flexibility. In addition, the individual identity broker can easier respond on individual requirements, either from the user or the service provider. Such requirements might be some local or domestic regulations specific to a country. This means for example, a user can rely on her desired identity broker, which acts compliant to such local or national regulations. Although there is no direct trust relationship between the user and the affiliated identity broker of the service provider, due to identity broker federation the user is still able to authenticate at the service provider. Summing up, users and service providers can select their preferred cloud identity broker for authentication, thus both identity brokers can actually provide and support different functionality. The only prerequisite is that identity data transfer is possible between the individual cloud identity brokers. Figure 8.1 illustrates this *Federated Cloud Identity Broker-Model*.

In the following, the components that are involved in this model are briefly described.

User: A user (U) wants to access protected resources from a service provider. For identification and authentication, the user relies on her favorite cloud identity broker (user's home broker), which manages different identity providers and attribute providers the user is registered with.

Service Provider: A service provider (cloud-based or a traditional web application) offers various services to users and requires proper identification and authentication.

Identity Provider: The identity provider stores user's identity data. Furthermore, the identity provider is responsible for user identification and authentication.

Attribute Provider: The attribute provider stores additional attributes of a user's identity. These additional attributes can be retrieved from the attribute provider during an authentication process.

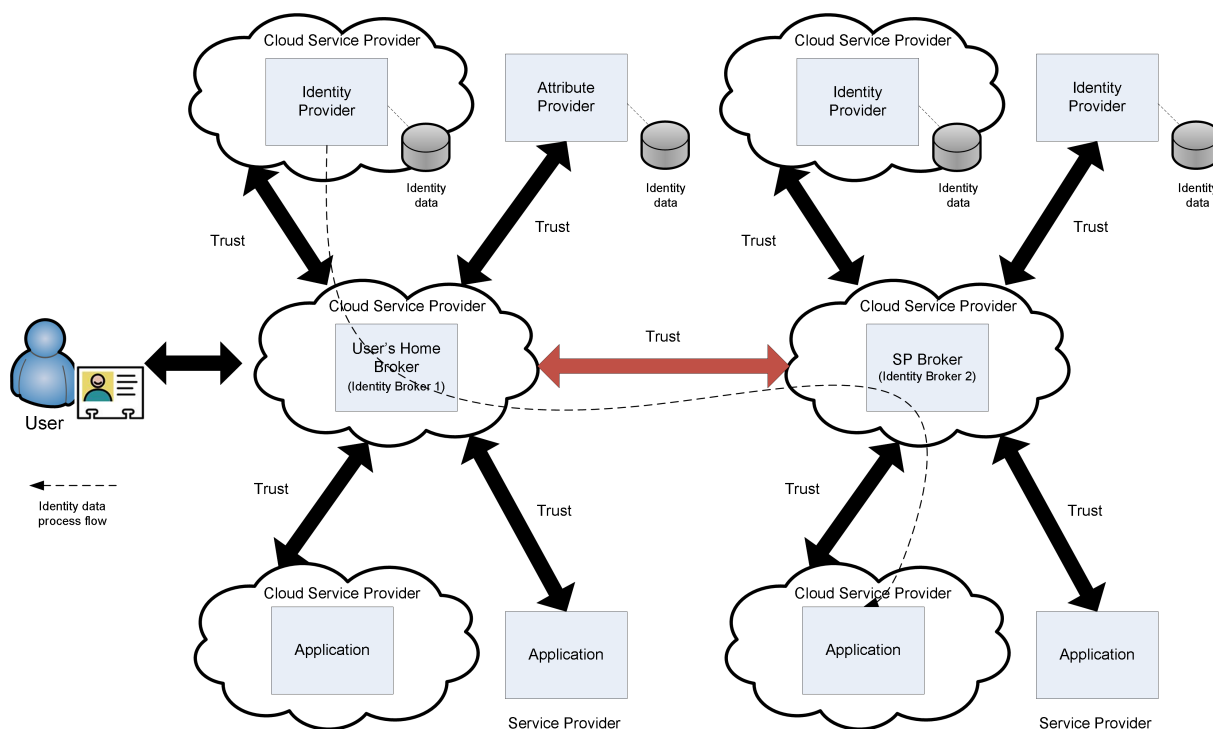


Figure 8.1: Federated Identity as a Service-Model [Zwattendorfer et al., 2013a]

Home Broker: The user's home broker constitutes the cloud identity broker the user is affiliated with. The user trusts this broker and has a contractual relationship with it. The home broker manages all identity providers and attribute providers, where the user is registered with.

Service Provider Broker: The service provider broker (SP broker) has an affiliation with the service provider the user wants to authenticate. The SP broker manages the communication with the user's home broker for the service provider.

In this federated model it is possible that the service provider has a contractual relationship with identity broker 2 (SP broker), whereas the user has a contractual relationship with identity broker 1 (home broker). In addition, both cloud identity brokers have some kind of trust and contractual relationship amongst each other. This model fully features the brokered trust model across multiple identity brokers as discussed in Section 3.1.6.

Having a closer look at the information and process flow, in a first step the user contacts a service provider by stating that she wants to consume a protected resource. For accessing this protected resource, proper identification and authentication is required. The service provider has a contractual and trust relationship with identity broker 2. However, the user only has a contractual and trust relationship with identity broker 1, which supports – in contrast to identity broker 2 – the identity provider the user actually wants to use for authentication. To use this intended identity provider, in a next step the user is forwarded to her affiliated identity broker 1. After that, the user's home broker (identity broker 1) initiates the identification and authentication process with the desired identity provider. The user provides appropriate credentials for successful authentication at the desired identity provider. If authentication was successful, identification and authentication data will be transmitted to the user's home broker (identity broker 1). Subsequently, identity broker 1 forwards the user's identity and authentication data to identity broker 2 (SP broker), which in turn transmits these data to the service provider. Based on the received data, the service provider either grants or denies access to the protected resource.

In this model, there are three communication channels (cf. Figure 8.1) where identity data are transferred, namely between

1. identity provider and user's home broker (identity broker 1)
2. user's home broker (identity broker 1) and SP broker (identity broker 2)
3. SP broker (identity broker 2) and service provider.

All communication channels can be covered by existing identity protocols such as SAML, OAuth, etc. (cf. Section 3.5).

8.3 Privacy-Preserving Federated Identity as a Service-Model

This model constitutes a slight extension to the *Federated Identity as a Service-Model*. The main aim of this model is – similar to the *BlindIdM-Model* (cf. Section 7.1.3.2) and the *Identity as a Service-Model for Electronic Identities* (cf. Section 7.3.5) – an improved privacy-preservation for the user. Thereby, the same concept of "blinding" identity data is applied to the basic *Federated Identity as a Service-Model*. Hence, this model combines the advantages of the *Federated Identity as a Service-Model* with the advantages of the *BlindIdM-Model* and the *Identity as a Service-Model for Electronic Identities*. A big advantage of this model is that it can be applied when being deployed in semi-trusted environments and thus semi-trusted cloud identity brokers in terms of privacy and data protection can be supported.

The general concept of this model is similar to the *BlindIdM-Model* and the *Identity as a Service-Model for Electronic Identities* because also proxy re-encryption (cf. Section 7.3.2.6) is used for protecting identity data from the cloud service providers. However, the main differences to the *BlindIdM-Model* are that the data can also be stored encrypted at non-cloud identity providers and that the data can also be encrypted by the user and not only by an organization. This concept – storing identity data encrypted for the user – is also applied in the *Identity as a Service-Model for Electronic Identities* (cf. 7.3.5). In other words, this *Privacy-Preserving Federated Identity as a Service-Model* supports both encryption concepts of the *BlindIdM-Model* and the *Identity as a Service-Model for Electronic Identities*. More precisely, the *Privacy-Preserving Federated Identity as a Service-Model* supports identity data stored at identity providers

1. encrypted for the user
2. encrypted for the home organization¹

The *Privacy-Preserving Federated Identity as a Service-Model* supporting the processing of encrypted identity data, either encrypted for the user or a home organization, is illustrated in Figure 8.2.

Depending on the implementation concept of this model, either one or two re-encryption steps can be necessary. In the first case, encrypted identity data, which has been provided from the identity provider to the user's home broker, is directly re-encrypted by the home broker for the service provider. Hence, only one re-encryption step is required since the re-encrypted identity data are just tunneled through the SP broker to the service provider. The re-encryption key to be provided to the home broker must be generated supporting the directions *user* → *service provider*, if the identity data was encrypted for the user, or *home organization* → *service provider*, if the identity data was encrypted for the home organization. In the second case, encrypted identity data can be first re-encrypted by the user's home broker for the SP broker and then – in a subsequent step – be re-encrypted by the SP broker for the service provider. Hence, in this case two re-encryption steps are required.

If one or two re-encryption steps are required mainly depends on the key management and key distribution approach. If the public encryption key of the service provider can be transferred by the

¹According to Nuñez and Agudo [2014], a home organization is responsible and in control of the organization's identity management. This includes identity data storage, authentication, etc.

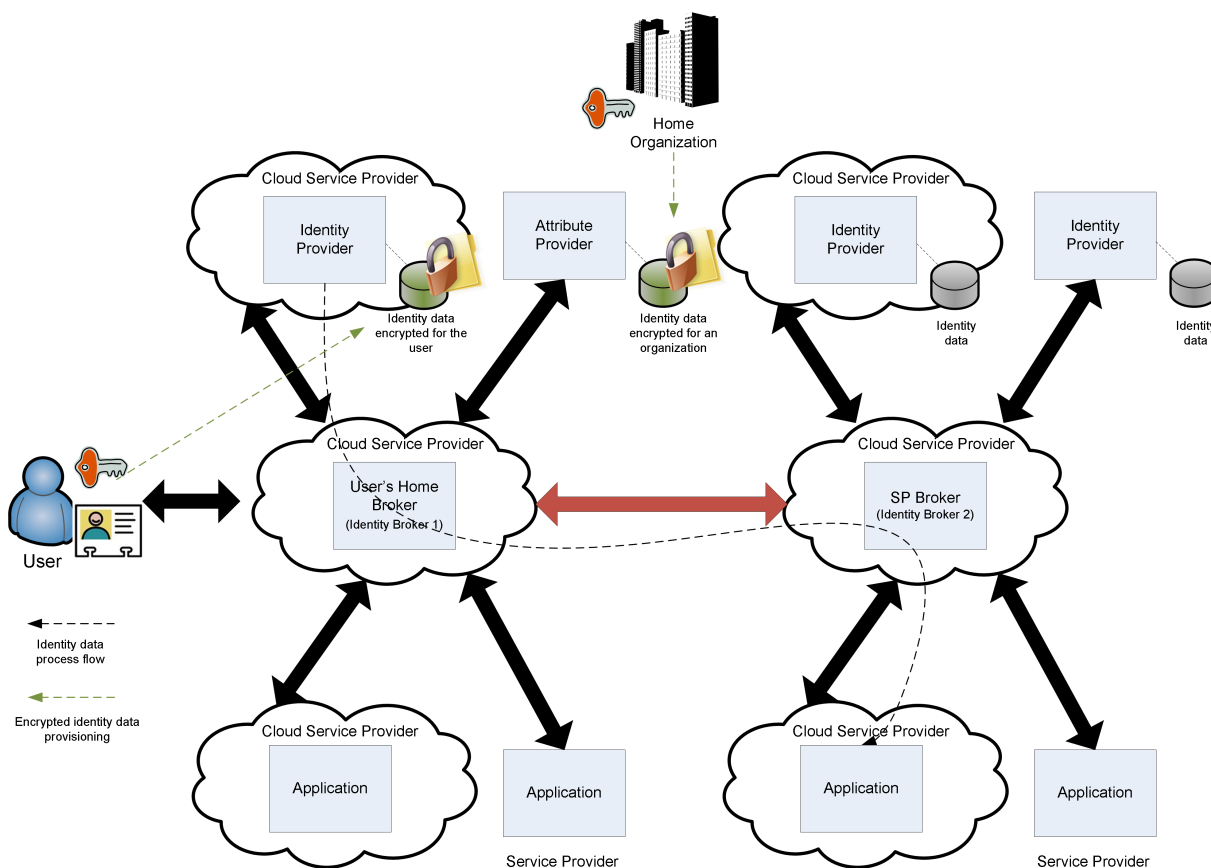


Figure 8.2: Privacy-Preserving Federated Identity as a Service-Model

communication protocol to the user's home broker or is available by other means, then just one re-encryption step at the home broker is necessary. In contrast to that, if the public encryption key of the service provider is only available at the SP broker, then two re-encryption steps from the home broker over the SP broker to the service provider need to be carried out.

To ensure the applicability of this model and to illustrate the two different process flow possibilities, the author proposes in the next section a prototypical implementation which uses just one re-encryption step. In the subsequent section, the author shows a concept for an application of this model, which requires two re-encryption steps. In more detail, the author applies the *Privacy-Preserving Federated Identity as a Service-Model* to the STORK cross-border PEPS approach (cf. Section 5.5.4.1).

8.4 Proof of Concept Implementation

Subsequently, details of the *Privacy-Preserving Federated Identity as a Service-Model* by means of a proof of concept implementation are provided. To implement the model, one demo service provider, two cloud identity brokers (the user's home broker and the SP broker), and one attribute provider were designed and developed. Additionally, two existing identity providers i.e., Twitter² and one self-hosted OpenID provider, were integrated. Figure 8.3 illustrates the implemented architecture.

²<http://www.twitter.com>

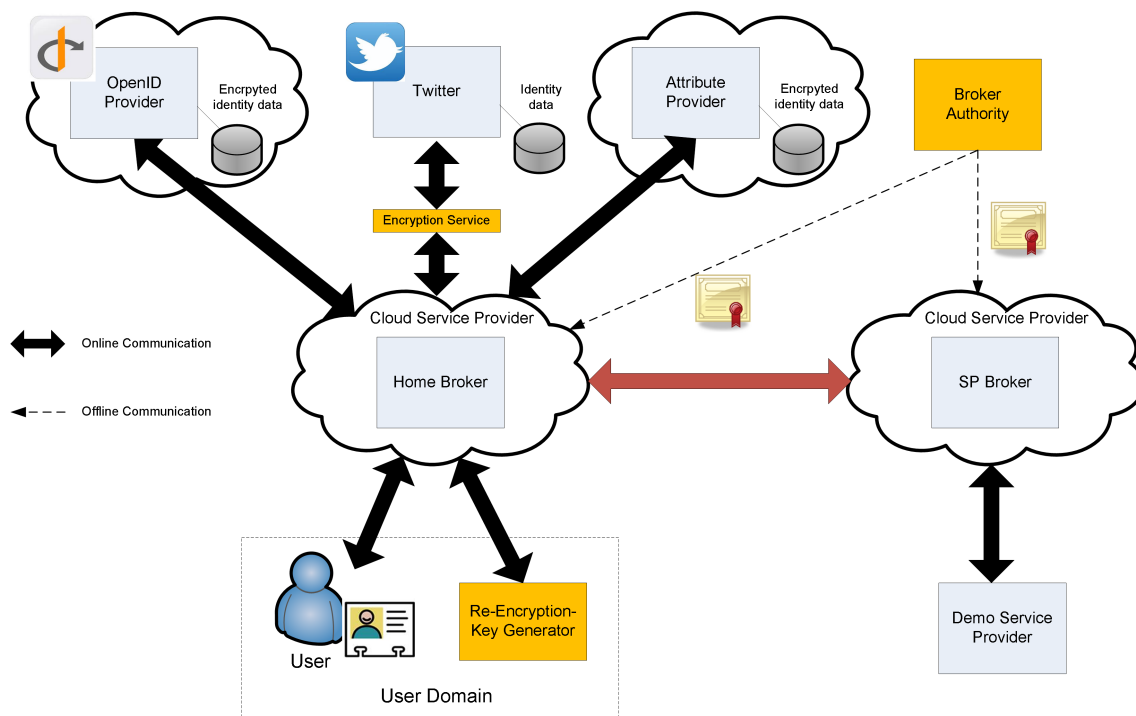


Figure 8.3: Implementation Architecture of the Federated Cloud Identity Broker-Model

8.4.1 Requirements

When designing this new *Privacy-Preserving Federated Cloud Identity Broker-Model*, the following requirements were kept in mind, which need to be fulfilled by the implementation:

Individual selection of the cloud identity broker: Both users and service providers are able to individually select the cloud identity broker of their choice.

Trust: The service provider and identity provider are trusted, whereas the cloud provider which hosts and operates the identity broker, is assumed to be semi-trusted (*honest but curious*). This means, the identity broker works correctly, but might be interested in inspecting users' identity data. With this model the identity providers can also be assumed to be semi-trusted.

Privacy: Since the identity brokers are operated in the cloud, privacy is an important issue. For this model the support of the privacy characteristics *user-centricity* (the user always stays under full control on which data are disclosed to the service provider and cloud identity broker) and *selective disclosure* (the user is able to select the amount of data to disclose to the service provider and cloud identity broker) are demanded. Furthermore, users' identity data should be treated confidential and users' privacy must be preserved with respect to all entities in the cloud.

Usability: Implementations of the model should be comfortable to use, thus no burdensome user interactions should be required.

Easy integration into existing infrastructures: The new model should be easily integrable into existing infrastructures, meaning that service providers and identity providers can easily connect to the cloud identity broker through standardized and already existing interfaces.

8.4.2 Components

In order to meet the previously defined requirements, three additional components need to be introduced. First, a so-called *broker authority* is introduced, which is mainly responsible for managing the trust relationships between individual cloud identity brokers. Second, a *re-encryption key generator* is introduced, which is capable of generating encryption keys. Third, an *encryption service* is required, which is capable of encrypting arbitrary data. All new components are trusted entities. These new as well as the other components are described in detail in the next paragraphs.

Demo Service Provider: The demo service provider has actually no particular functionality, it just requires proper user identification and authentication. However, identification and authentication is delegated to the SP broker to minimize efforts. If a user wants to authenticate, the user is forwarded to the SP broker to request authentication. To minimize the amount of data transferred and to respect user's privacy, the service provider is able to request only specific attributes from the user for service provisioning. In addition, the service provider can request a certain level of quality for the identity and the authentication process. This form of quality assurance is modeled as authentication levels, similar to the ones proposed by the NIST [Burr et al., 2013], STORK [Hulsebosch et al., 2009] (cf. also Section 5.5.2), or ISO/IEC [ISO/IEC JTC 1, 2012].

SP Broker: The SP broker has been selected by the service provider and thus they share a contractual relationship. The SP broker communicates with the user's home broker and forwards the authentication request to it. Additionally, the SP broker offers a user interface where the user can provide location information of her home broker.

Home Broker: The location of the user's home broker is identified via a user-specific URL, which points to this broker. The URL format is similar to the one used by the OpenID protocol. The user-customized URL is not persistent and can be changed by the user anytime. Before being able to use the functionality of the home broker, the user has to register with it. The home broker holds metadata for the user which include the identity providers the user is able to use and is registered with, and which attribute providers can be connected. The home broker communicates with the identity providers for user identification and authentication and with the attribute providers for attribute transfer. During the authentication process, the home broker presents the user an identity provider selection page and the requested attributes from the service provider. Thereby, the user can select the identity source the requested attributes should be retrieved from. If data are retrieved from different identity data sources (e.g., from an identity provider and an attribute provider), the home broker does a mapping to a common (semantic) format.

Broker Authority: The broker authority is responsible for managing the trust relationships between cloud identity brokers. For that, it issues certificates for signature public keys of the individual brokers. The respective signing keys are used to sign messages exchanged between brokers, ensure an authentic communication channel, and thus verify the trust relationships. Note that this is merely a virtual entity and any (set of) mutually trusted certification authorities will be sufficient in practice.

Twitter: In the prototypical scenario, Twitter is used as an identity provider. When registering, Twitter stores a couple of user attributes such as the user's full name or language. Those attributes can be used for identification and authentication at the service provider.

OpenID Provider: In this implementation an own OpenID provider was set up. The reason is that confidentiality of user's attributes with respect to the identity provider and the two brokers needs to be ensured. To achieve this, the user encrypts her attributes under the user's public key of a proxy re-encryption scheme before storing them at the OpenID provider. At this stage, only the

user is able to decrypt the attributes again. The sole attribute, which is visible in plaintext to the OpenID provider, is the user's OpenID identifier.

Attribute Provider: For the attribute provider the same approach as for the OpenID provider is used. Hence, the user stores her identity data at the attribute provider in encrypted format only. The only attribute the attribute provider is able to inspect in plaintext is an identifier to link the encrypted attributes to a specific user. At the attribute provider, no explicit user authentication is required.

Re-Encryption-Key Generator: The re-encryption-key generator is an entity that runs directly in the user's domain to avoid any private key transfer to another party. In the implementation, the user allows her identity data, which are encrypted for her and stored at the identity/attribute provider, to be re-encrypted by the home broker for a service provider. This way, the identity data remains always confidential even if routed through the identity brokers residing in the cloud. The functionality of the re-encryption-key generator is computing the re-encryption $rk_{U \rightarrow SP}$ by taking the private key of the user sk_U and the public key of the service provider pk_{SP} .

Encryption Service: The encryption service enables the encryption of data coming from an identity provider such as Twitter, which does not support storage of encrypted attributes, by the user. Hence, identity data stays always confidential before transmission to the cloud identity brokers.

8.4.3 Communication Interfaces

Since data are transferred between the individual components, the author now briefly describes the used communication protocols and how they were implemented. Thereby, the interfaces and protocols, respectively, between two entities at a time are described. All communication interfaces are secured using SSL/TLS for transport security, hence this fact will not be mentioned again explicitly in the individual descriptions.

Service Provider ↔ SP Broker: Actually, arbitrary identity and authentication protocols can be used for this communication channel. Which protocol should be used depends on the support of the SP broker and the protocol preferred by the service provider. Nevertheless, in the prototypical implementation an amended version of the SAML AuthnRequest/Response Protocol [Cantor et al., 2009b] using the SAML HTTP-POST Binding [Cantor et al., 2009a] was relied on. In particular, amendments are the inclusion of requested attributes as well as the requested authentication level in the SAML authentication request. In fact, the amended protocol is similar to the STORK protocol [Alcalde-Moraño et al., 2011], which will play an important role in identification and authentication processes across Europe in the near future³. Trust is established by means of signature certificates. However, there is no explicit trust framework required, trust can be negotiated bilaterally.

SP Broker ↔ Home Broker: Again, for this communication path the amended SAML protocol is relied on. Exchanged messages are also digitally signed (certificates are signed by the trusted broker authority). This ensures that only by the authority authorized brokers are able to trust and communicate with each other. Referring to Hühnlein et al. [2013], SAML is the best choice for integrating digital identities because SAML is a broad adopted standard.

Home Broker ↔ Twitter: For retrieving identity data from Twitter the OAuth 1.0 protocol is used. However, the communication path is intercepted by the trusted encryption service that allows users to encrypt their identity data before presenting it to the home broker.

³There are only minor differences between the used amended SAML protocol and the STORK protocol. Differences mainly target the format and semantic of transferred attributes as e.g., single encrypted attributes are not supported within STORK.

Home Broker ↔ OpenID Provider: For this communication channel the OpenID 2.0 interface was implemented. This is somewhat related to the work in Nunez et al. [2012].

Home Broker ↔ Attribute Provider: For simplicity, in the proof of concept implementation a customized web service interface was used. The request message includes requested attributes and an identifier of the user, the response then simply returns the corresponding encrypted attributes.

Home Broker ↔ Re-Encryption-Key Generator: Communication is based on the SAML Attribute-Query/Response Protocol [Cantor et al., 2009b]. The attribute query thereby includes the public key of the service provider pk_{SP} . By calling the local re-encryption-key generator, combining the public key of the service provider pk_{SP} with the users private key sk_U the user obtains the re-encryption key $rk_{U \rightarrow SP}$, which is wrapped in the response. In the implementation a non-interactive, unidirectional, and single-use proxy re-encryption scheme of Ateniese et al. [2006] was used (cf. Section 7.3.2.6).

Broker Authority ↔ SP Broker/Home Broker: The exchange of certificates between the broker authority and the brokers is actually an offline process. Exchange is carried out using appropriate organizational mechanisms.

8.4.4 Process Flows

Subsequently, the secure identification and authentication process using the implementation of the proposed *Federated Cloud Identity Broker-Model* is presented. Identification and authentication is explained by contacting the OpenID and the attribute provider.

8.4.4.1 Setup

The following setup is required before running an authentication process:

- It is assumed that the user trusts the service provider, Twitter, the encryption service, and the re-encryption-key generator (latter runs in the user's domain). In contrast to that, it is assumed that the cloud identity brokers (SP broker and home broker), the OpenID provider, and the attribute provider are semi-trusted (*honest but curious*), meaning that they work correctly but might be interested in inspecting user's data.
- The broker authority has certified the trustworthiness of the two brokers by certifying the signature public keys and thus verifying the trust relationship between the brokers. The respective signature key pairs are denoted as $(sk'_{SP-Broker}, pk'_{SP-Broker})$ and $(sk'_{Home-Broker}, pk'_{Home-Broker})$. These keys are used for signing the SAML messages exchanged between the two brokers.
- A bilateral trust relationship has been negotiated between the service provider and the SP broker. To enforce this trust relationship on technical level, certified signature public keys have been exchanged. These signing key pairs of the SP are denoted as (sk'_{SP}, pk'_{SP}) and it is assumed that the SP broker uses $(sk'_{SP-Broker}, pk'_{SP-Broker})$. These keys are used for signing the exchanged SAML messages between SP and SP Broker. In addition, the service provider holds a proxy re-encryption key pair (sk_{SP}, pk_{SP}) .
- A bilateral trust relationship exists between the user's home broker and the individual identity providers. The establishment of this trust relationship is protocol dependent, however, both channels (between home broker and Twitter and between home broker and the OpenID provider) are authentic.

- The user possesses a proxy re-encryption key pair (sk_U, pk_U) and has already stored personal attributes in encrypted format at the OpenID provider and the attribute provider. A set of user encrypted attributes are denoted as $c_{U_i} = (c_{U_1}, \dots, c_{U_m})$ and the corresponding plaintext attributes are denoted as $a_i = (a_1, \dots, a_m)$.
- The user has a contractual relationship with the home broker, has registered in her profile the identity/attribute providers she wants to use, and has stored appropriate authentication credentials for the attribute provider. Additionally, the user holds a unique personal identifier (uniqueID) to be identifiable at the home broker.

8.4.4.2 Authentication Process

The sequence diagram in Figure 8.4 illustrates the authentication process flow. In the following details to the individual steps are given.

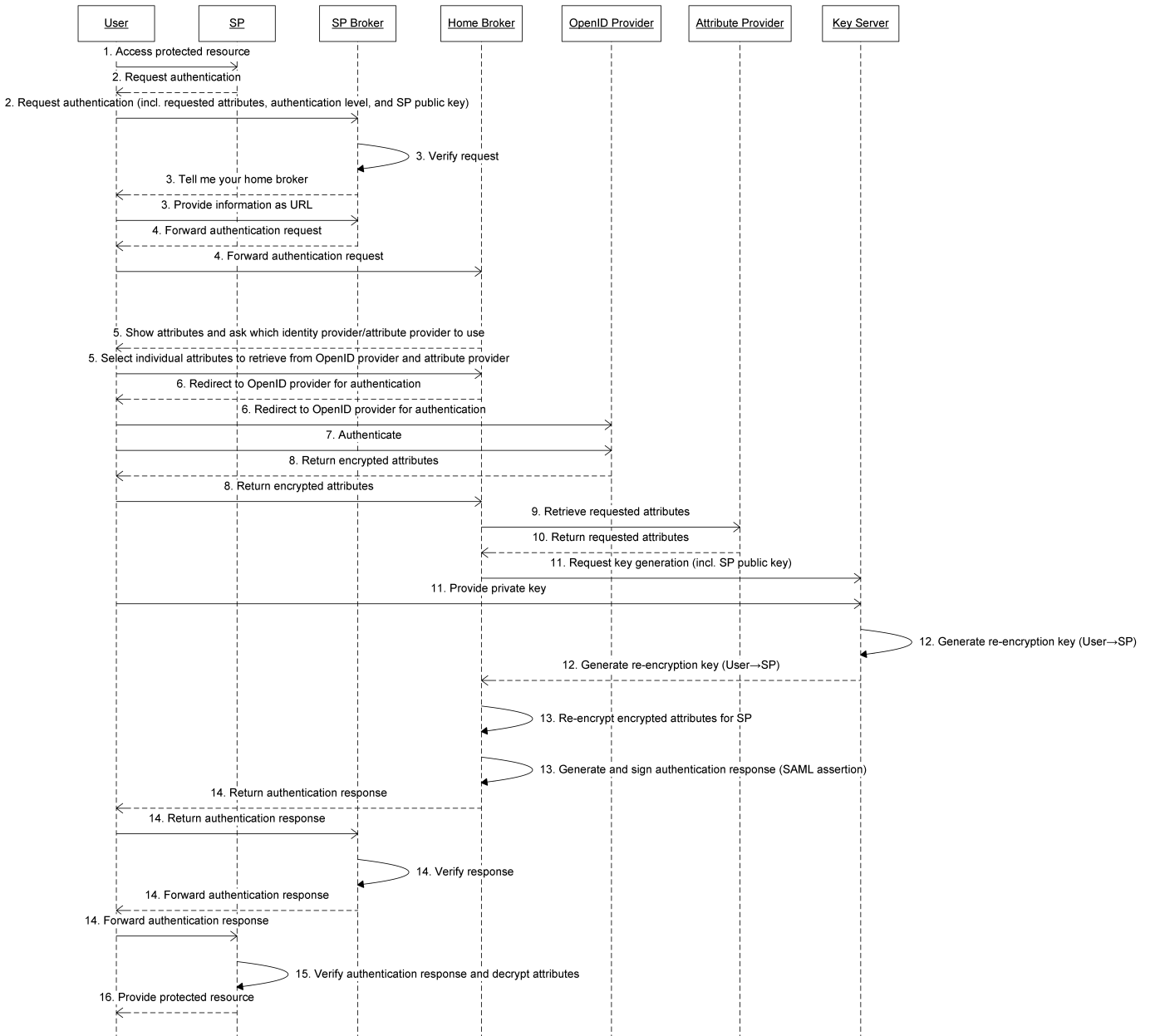


Figure 8.4: Authentication process flow

1. A user wants to access a protected resource from the service provider.
2. Since the service provider requires authentication, it forwards the user to its affiliated SP broker. This SAML authentication request includes the set of attributes (req_attr), which should be provided during the authentication process, the requested authentication level (req_auth_level), and the public encryption key pk_{SP} of the service provider. The request is signed by the service provider resulting in the signature $\sigma_{SP} = DSS.Sign(sk'_{SP}, req_attr || req_auth_level || pk_{SP})$.
3. First, the broker verifies σ_{SP} . Furthermore, the SP broker asks the user to provide location information of her home broker. The user enters a URL, which is a composition of a uniqueID of the user at the home broker and the home broker's domain (e.g., `https://user.home-broker.com`).
4. The SP broker creates a signature $\sigma_{SP-Broker} = DSS.Sign(sk'_{SP-Broker}, req_attr || req_auth_level || pk_{SP} || uniqueID)$ and forwards the authentication request of the SP to the user's home broker (using the SAML protocol).
5. The home broker verifies $\sigma_{SP-Broker}$. Based on the uniqueID, the user is identified at the home broker. The home broker presents the user a web page, which shows the requested attributes req_attr of the service provider. Additionally, the user can select at which identity provider she wants to authenticate (only those identity providers are shown, which were registered by the user and which support the requested authentication level req_auth_level). Furthermore, the user can select for every individual attribute if it should be retrieved from the identity provider – if providable – or from an affiliated attribute provider. In this example it is assumed that the user selects the OpenID provider as an identity provider and that additional attributes should be retrieved from the attribute provider.
6. Based on the user's OpenID identifier the user is redirected to the OpenID provider.
7. The user authenticates at the OpenID provider using appropriate credentials.
8. The attributes, which have been selected for retrieval from the OpenID provider, are returned to the home broker in encrypted fashion. The user encrypted attributes $(c_{U_1}, \dots, c_{U_j})$ are assumed to be returned.
9. Since in this scenario only a subset of the requested attributes can be retrieved from the OpenID provider, additional attributes are fetched from the attribute provider. Communication and retrieval is based on a pre-negotiated access token as used in OAuth, which is shared between the home broker and the attribute provider, to identify the user at the attribute provider and allow the broker access to the user's data.
10. The remaining attributes $(c_{U_k}, \dots, c_{U_m})$ are returned to the home broker in encrypted format.
11. Now all requested attributes $(c_{U_1}, \dots, c_{U_m})$ are located at the home broker, but they are still encrypted for the user. To make these attributes readable for the service provider, re-encryption needs to be applied. A re-encryption key generation request is sent from the home broker to the local re-encryption key generator, which includes the public key of the service provider pk_{SP} . The user additionally has to provide the key generator access to her private key sk_U .
12. The re-encryption key generator computes the re-encryption key out of the service provider's public and the user's private key and returns the re-encryption key $rk_{U \rightarrow SP} = RE.RKGen(sk_U, pk_{SP})$ to the home broker.
13. The home broker re-encrypts all collected attributes for the service provider resulting in $(c_{SP_1}, \dots, c_{SP_m})$ by running $c_{SP_i} = RE.ReEnc(rk_{U \rightarrow SP}, c_{U_i})$ for all $1 \leq i \leq m$. Additionally, it wraps the

re-encrypted attributes and the actual authentication level `auth_level` into a SAML assertion and computes a signature $\sigma_{Home-Broker} = \text{DSS.SignKey}_{Home-Broker}, c_{SP_1} \parallel \dots \parallel c_{SP_m} \parallel \text{auth_level}$.

14. The SAML assertion is returned within the authentication response to the SP broker. The SP broker verifies $\sigma_{Home-Broker}$, computes a signature $\sigma_{SP-Broker} = \text{DSS.SignKey}'_{SP-Broker}, c_{SP_1} \parallel \dots \parallel c_{SP_m} \parallel \text{auth_level}$, and forwards the authentication response to the service provider.
15. The service provider verifies the received response by verifying $\sigma_{SP-Broker}$ and obtains the decrypted attributes $(a_1 \dots, a_m)$ by running $a_i = \text{RE.Dec}(sk_{SP}, c_{SP_i})$ for all $1 \leq i \leq m$.
16. Based on the decrypted identity and attribute data $(a_1 \dots, a_m)$ and the `auth_level` the service provider is able to provide the desired protected resources to the user.

In contrast to the above description, Twitter does not allow to store encrypted data. In the proposed solution, it is still possible to achieve privacy when using Twitter as identity provider. In this case, identity data needs to be encrypted by the user before being transferred from Twitter to the home broker.

Recurring Authentications: Most of the time, running through the complete authentication process described before might be cumbersome for the user. Therefore, the implementation is able to remember some selections the user did in her first authentication process, if the user wants so. For instance, in a recurring authentication process the steps 3 and 4 (indicating the home broker) can be omitted, because the SP broker is able to remember user's choice during her first authentication. In addition, step 9 (providing authentication credentials to the identity provider) can be skipped if single sign-on (SSO) (cf. Section 3.4.1) is supported by the selected identity provider. Also the key generation steps 13-15 are not necessary as the re-encryption key for a particular service provider can be stored for re-use in the user's profile at the home broker. Avoiding as many user interactions as possible definitely increases usability of the proposed solution.

8.4.5 Screenshots

In this section, details of the implemented prototype are given by presenting appropriate screenshots. The individual screenshots will be discussed according to the process steps described in the previous section.

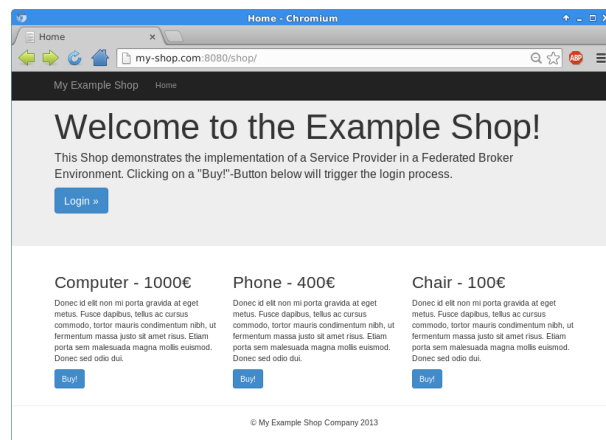


Figure 8.5: Step 1: Access protected resource

Figure 8.5 illustrates the welcome screen of the demo service provider. The demo service provider represents a sample web shop which requires proper identification and authentication. For starting the

identification and authentication process, the user just needs to press the login button. This corresponds to *Step 1* of the authentication process flow.

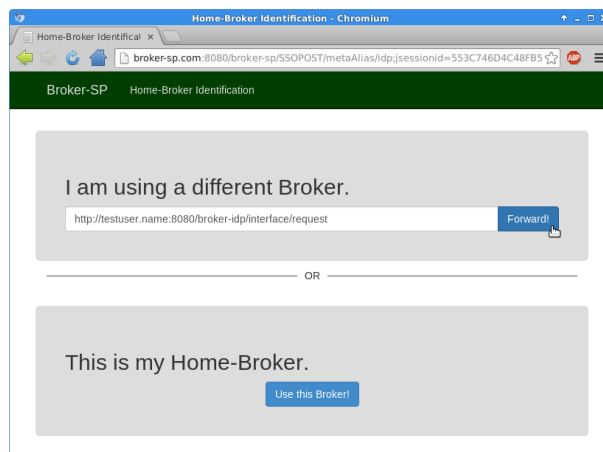


Figure 8.6: Step 3: Tell me your home broker

After pressing the login button, a SAML authentication request is sent via the user to the affiliated SP broker. After verifying the request, the SP broker asks the user to tell her home broker. According to Figure 8.6, the user enters a URL, which is a composition of a uniqueID of the user at the home broker and the home broker's domain. Corresponding to Figure 8.6, this URL is `http://testuser.name:8080/broker-idp/interface/request`. Alternatively, the SP broker could be already the user's home broker. Hence, no URL input would be required and just a simple button can be clicked. According to the process flow, this screenshot corresponds to *Step 3*.

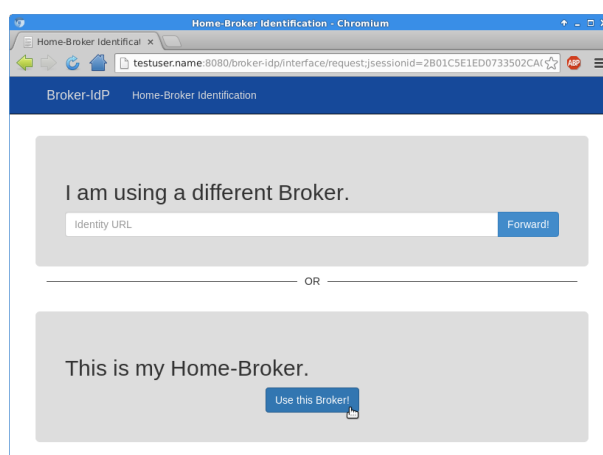


Figure 8.7: Step 4: Forward authentication request

A similar screen is actually presented to the user in *Step 4*, as illustrated in Figure 8.7. Since the user is now at her home broker, the user just needs to consent that this is her home broker.

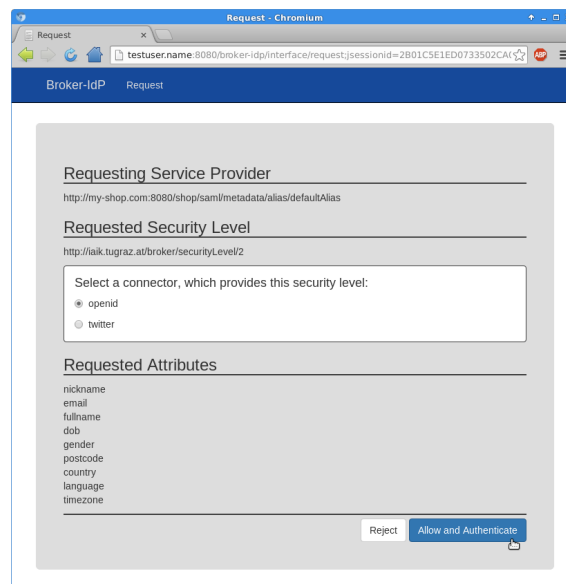


Figure 8.8: Step 5.1: Show attributes and ask which identity provider or attribute provider to use

In the next *Step 5* the user is shown a page which illustrates the requesting service provider, the requested attributes (*req_attr*), and the required authentication level (*req_auth_level*) for satisfying the authentication process. Furthermore, the user is provided a list of identity providers, which the user is registered with and which are able to satisfy the requested authentication level. All this information is shown in Figure 8.8. According to this screenshot, the requesting service provider is `http://my-shop:8080/shop/saml/metadata/alias/defaultAlias`, the requested authentication level is `http://iaik.tugraz.at/broker/securityLevel/2`. This authentication level is supported by Twitter and OpenID. The requested attributes are *nickname*, *email*, *fullname*, etc. Finally, the user selects OpenID as desired identity provider and continues the authentication process.

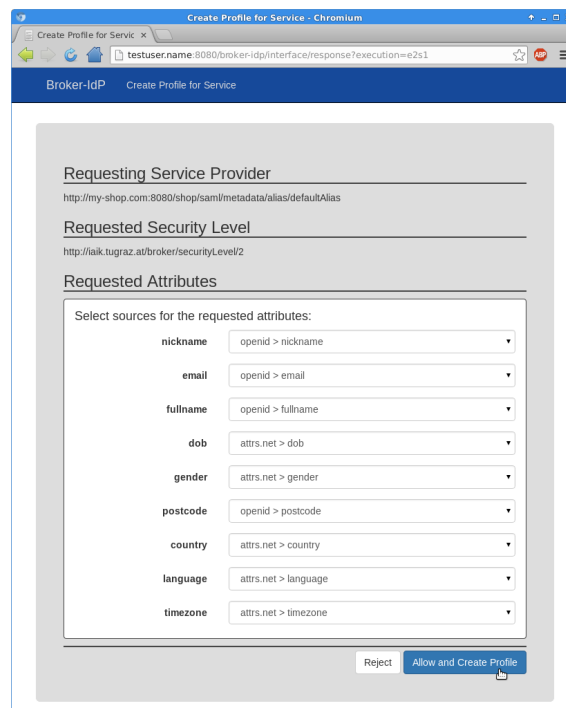


Figure 8.9: Step 5.2: Select individual attributes to retrieve from OpenID provider and attribute provider

Figure 8.9 illustrates the screen presented to the user for retrieving requested attributes. According to this screenshot, the user can select whether attributes should be retrieved from the OpenID provider or from the separate attribute provider. This screen still corresponds to *Step 5* of the described process flow.

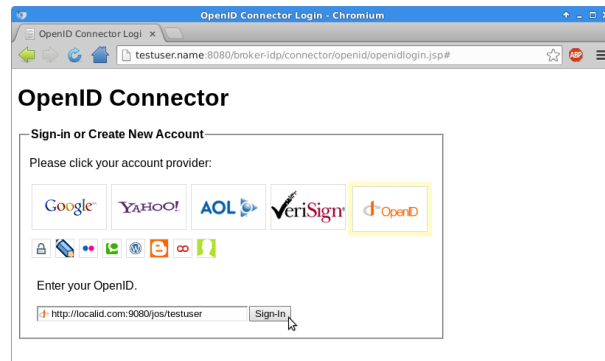


Figure 8.10: Step 6: Redirect to OpenID provider for authentication

Since the user selected the OpenID provider for authentication, the user needs to provide her OpenID identifier to the home broker. This *Step 6* of the OpenID authentication process is illustrated in Figure 8.10. According to this screenshot, the OpenID identifier the user enters is `http://localid.com:9080/jos/testuser`. Based on that identifier, the user is redirected to the OpenID provider.

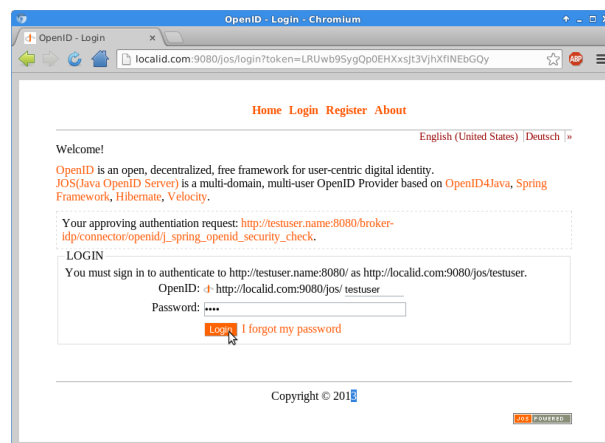


Figure 8.11: Step 7: Authenticate

The user now authenticates at the OpenID provider (*Step 7*) by providing her secret password. This authentication process is illustrated in Figure 8.11.

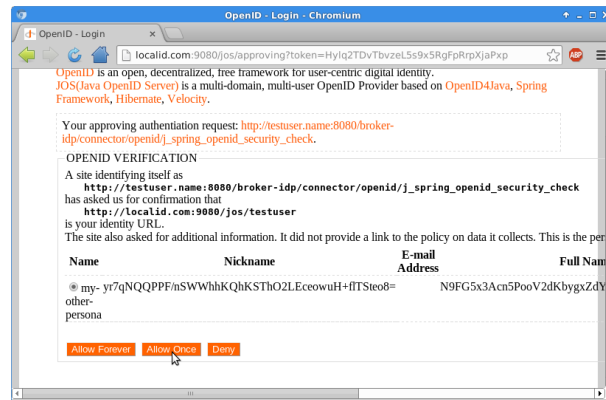


Figure 8.12: Step 8: Return encrypted attributes

Figure 8.12 illustrates the attributes that can be provided by the OpenID provider. As can be seen from this screenshot, all attributes are stored at the OpenID provider in encrypted format. These encrypted attributes are then returned from the OpenID provider to the home broker.

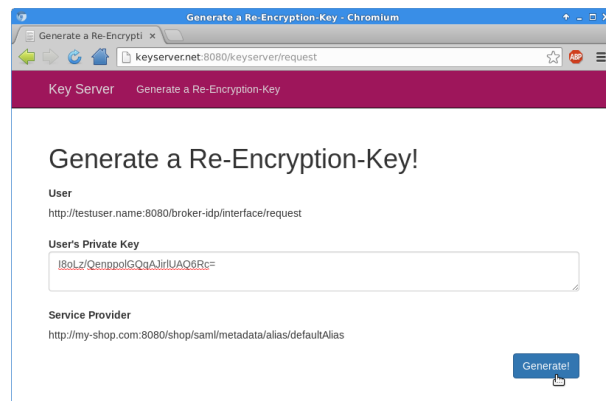


Figure 8.13: Step 12: Generate re-encryption key (*User*→*SP*)

Figure 8.13 illustrates the re-encryption key generation process of *Step 12*. Thereby, the user needs to provide her private key sk_U to the local re-encryption key generator.

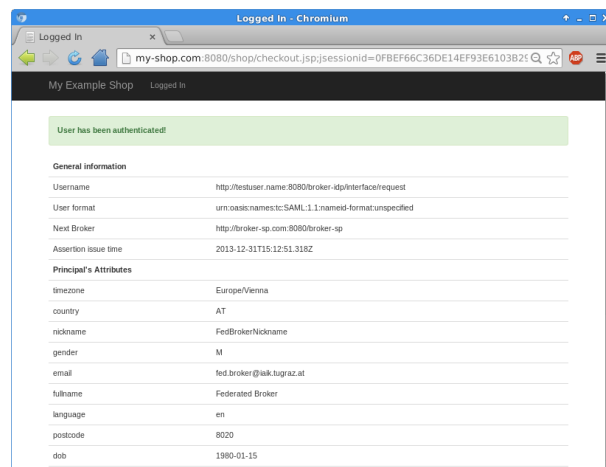


Figure 8.14: Step 16: Successful authentication and illustration of transferred identity data and attributes

Figure 8.14 already illustrates the final page of a successful authentication process. At the demo service provider, the attribute values of the requested attributes are shown.

8.4.6 Discussion

In this section the new model and implemented solution is discussed with respect to the requirements specified in Section 8.4.1.

Individual selection of the cloud identity broker: In the implemented solution, both the user and the service provider are able to select the cloud identity broker of their choice. The service provider just needs to establish a trust relationship with the broker and implement the communication interface it offers. In addition, the user can contract another broker and registers her desired identity and attribute providers. The user is identified by the broker by a uniqueID.

Trust: The individual cloud identity brokers are able to communicate with each other because trust is grounded through the broker authority. The pairwise trust relationships between service provider and SP broker, and between home broker and identity provider depend on bilateral agreements. There is no direct trust relationship between service provider and identity provider because the brokers act as intermediary. Hence, trust is brokered between service provider and identity provider.

Privacy: The requirement of user-centricity is achieved because individual attributes can be stored encrypted for the user only at an identity provider or attribute provider. If this is not possible (e.g., with Twitter), a trusted encryption service can be used as intermediary to encrypt identity data before transmitting it to the cloud identity broker. Only the user is in control to decrypt the data or to generate re-encryption keys. The requirement of selective disclosure is achieved because the user is able to select the attributes she wants to transfer at the home broker (i.e., the service provider only gets the attributes which it has requested and the user gave consent for). In addition, confidentiality of user attributes with respect to the cloud identity broker is achieved through proxy re-encryption. To illustrate user's privacy and the amount of data which is disclosed to the individual entities, a comparison was made in Table 8.1.

Table 8.1: Data visible to the individual entities

Entity	Service Provider	SP Broker	Home Broker	Identity Provider (OpenID Provider)
<i>Personal data</i>	<ul style="list-style-type: none"> • User attributes requested (if the user gave consent) • Authentication level 	<ul style="list-style-type: none"> • uniqueID and domain of home broker • SP the user wants to authenticate 	<ul style="list-style-type: none"> • uniqueID of the user at the home broker • Identity providers and attribute providers the user is registered with • Local re-encryption key generator of the user • Credentials for accessing attribute providers • Re-encryption keys for recurrent authentications 	<ul style="list-style-type: none"> • OpenID identifier • Credentials for authentication

More precisely, the service provider only gets the attributes which it has requested and the authentication level. The SP broker just knows the service provider the user wants to authenticate and the

uniqueID and domain of the home broker. The home broker is the entity which gets to know most information because it has a user profile. The profile includes the identity/attribute providers the user is registered with, credentials for accessing the attribute provider, and the re-encryption keys for recurrent authentications. This profile is accessible by the uniqueID of the user at the home broker. Finally, also the OpenID provider does not know any user attributes except the OpenID identifier and the corresponding credentials for verifying an authentication process.

Usability: Usability is given because the user is able to select her preferred cloud identity broker. Additionally, the user can register her desired identity and attribute providers at her home broker and can select the desired providers during authentication. Furthermore, the user is able to select the identity attributes which should be disclosed to the service provider. Finally, recurrent user authentications are more comfortable for the user as some user interactions can be skipped.

Easy integration into existing infrastructures: The complete model can be easily adopted by service providers. Service providers just need to establish a contractual and trust relationship with their desired SP broker. Furthermore, they just need to implement one specific interface to the SP broker and not many interfaces to different identity providers as required in traditional settings. Implementation efforts can be reduced by providing appropriate software libraries.

Additional identity providers or attribute providers can be easily integrated by home brokers. The brokers just need to implement the communication protocol provided and offered by the identity providers or attribute providers.

8.5 Applying the Federated IdMaaS-Model to the PEPS Approach

The current PEPS Model (cf. Section 5.5.4.1) relies on a central PEPS instance, which is operated for every single country in a trusted conventional data center. Since STORK (cf. Section 5.5) will be the dominant authentication framework across Europe in the future, quite a large number of authentications running through the PEPS are to be expected. This, however, can lead to scalability issues at the data center, especially when imaging that the population of an entire country is able to use this PEPS. Consequently, a move of the trusted PEPS service into the public cloud considerably improves scalability. Nevertheless, a move of a trusted service into the public cloud clearly brings up new obstacles, especially with respect to citizens' privacy. Even when assuming that the PEPS in the public cloud works correctly, it still has to be assured that the cloud provider does neither learn nor leak any sensitive information.

In the following, a solution is proposed how the PEPS model can be securely realized in the public cloud by still preserving citizens' privacy. To achieve this, the *Privacy-Preserving Federated Identity as a Service-Model* is applied in such a way that the S-PEPS and the C-PEPS represent the two cloud identity brokers. Thus, both the S-PEPS and the C-PEPS can be moved into the public cloud. In the following, details on the required setup and the modified process flow are given [Zwattendorfer and Slamanig, 2013b].

8.5.1 Setup

For the setup of this cloud-based PEPS-PEPS scenario, similar to the current situation, the author considers a trusted European Commission body to be responsible for managing and maintaining the PEPS metadata. In particular, the following metadata for accomplishing this cloud approach are required.

The European Commission body denoted as EC generates a unidirectional and multi-use PRE and DSS key pair (cf. Section 7.3.2) for every countries' S-PEPS and C-PEPS, resulting in $(rsk_{S-PEPS_i}, rpks_{S-PEPS_i})$ and $(sk'_{S-PEPS_i}, pk'_{S-PEPS_i})$, and $(rsk_{C-PEPS_i}, rpks_{C-PEPS_i})$ and $(sk'_{C-PEPS_i}, pk'_{C-PEPS_i})$ respectively. The EC, however, must ensure that the secret keys rsk_{S-PEPS_i} and rsk_{C-PEPS_i} are kept secret by the EC and cannot be accessed by $S - PEPS_i$ or $C - PEPS_i$. Additionally, it provides every SP_j and IdP_k

taking part in this cloud-based STORK architecture with appropriate unidirectional and multi-use PRE keys: (rsk_{SP_j}, rpk_{SP_j}) and $(rsk_{IdP_k}, rpk_{IdP_k})$. Also the following re-encryption keys $r_{k_{S-PEPS_i \rightarrow C-PEPS_i}}$, $r_{k_{C-PEPS_i \rightarrow IdP_k}}$, $r_{k_{C-PEPS_i \rightarrow S-PEPS_i}}$, $r_{k_{S-PEPS_i \rightarrow SP_j}}$ are generated. The DSS key pairs ensuring integrity and authenticity of outgoing messages from either SP_j or IdP_k are created by the individual entities themselves, resulting in the key pairs (sk'_{SP_j}, pk'_{SP_j}) and $(sk'_{IdP_k}, pk'_{IdP_k})$, where the corresponding certificates must be publicly available.

To support the same logging and audit capability as in the current approach, the EC additionally generates re-encryption keys for itself $r_{k_{S-PEPS_i \rightarrow EC}}$ and $r_{k_{C-PEPS_i \rightarrow EC}}$. During the authentication process, the individual $S-PEPS_i$ and $C-PEPS_i$ log the same data as in the current approach but in encrypted form using either key $r_{k_{S-PEPS_i \rightarrow EC}}$ or $r_{k_{C-PEPS_i \rightarrow EC}}$. This allows the EC to inspect or audit transaction data if required.

8.5.2 Process Flow

In the following the detailed process flow when moving the individual PEPS instances into the public cloud is discussed. A simplified notation for the individual entities (SP instead of SP_j , etc.) is used to describe the process flow of one particular authentication. The individual process steps are basically conform to the current PEPS-PEPS process flow (cf. Section 5.5.4.4).

Figure 8.15 illustrates the process flow, which is as follows:

1. *Access protected resource:* A citizen (user) originating from country B wants to access a protected (e-Government) service in the foreign country A .
2. *SP Authentication Request:* This step is similar to the current situation. However, instead of including the data `reqAttr`, `reqQAA`, and `sp_name` in plain in the SP authentication request, the SP computes $c_{S-PEPS} = RE.Enc(rpk_{S-PEPS}, reqAttr || reqQAA || sp_name)$ and signs this ciphertext resulting in $\sigma_{SP} = DSS.Sign(sk'_{SP}, c_{S-PEPS})$. Both the signature σ_{SP} and the ciphertext c_{S-PEPS} are transmitted to the S-PEPS.
3. *Select home country:* The S-PEPS verifies σ_{SP} and if valid, the S-PEPS provides the citizen a country selection page.
4. *Provide home country information:* The citizen selects her country of origin and submits the information `country` (B) back to the S-PEPS.
5. *S-PEPS Authentication Request:* The S-PEPS takes the ciphertext c_{S-PEPS} received from the SP, re-encrypts it for the C-PEPS using key $r_{k_{S-PEPS \rightarrow C-PEPS}}$ resulting in c_{C-PEPS} , and finally signs it using its private key sk'_{S-PEPS} resulting in $\sigma_{S-PEPS} = DSS.Sign(sk'_{S-PEPS}, c_{C-PEPS})$. Depending on `country`, the S-PEPS forwards its authentication request including the data $(\sigma_{S-PEPS}, c_{C-PEPS})$ to the C-PEPS, which is responsible for authentications of `country`.
6. *Connect to appropriate IdP:* The C-PEPS verifies σ_{S-PEPS} . Additionally, the C-PEPS re-encrypts c_{C-PEPS} for the IdP using $r_{k_{C-PEPS \rightarrow IdP}}$ and signs the resulting ciphertext c_{IdP} using key sk'_{C-PEPS} . Both results $(c_{IdP}, \sigma_{C-PEPS})$ are transmitted to the IdP.
7. *Show requested attributes:* The IdP verifies σ_{C-PEPS} , decrypts c_{IdP} , and presents the citizen `reqAttr` and `sp_name`.
8. *Confirm/deselect requested attributes:* According to STORK, citizens must confirm the reception of `reqAttr` from the IdP. Thereby, citizens can deselect attributes for denying further transmission of those attributes to the SP, whereas only attributes which have been requested as being optional by the SP can be deselected. This step is only similar to the current situation. Instead of the C-PEPS in the current situation, the IdP carries out this process step in this scenario.

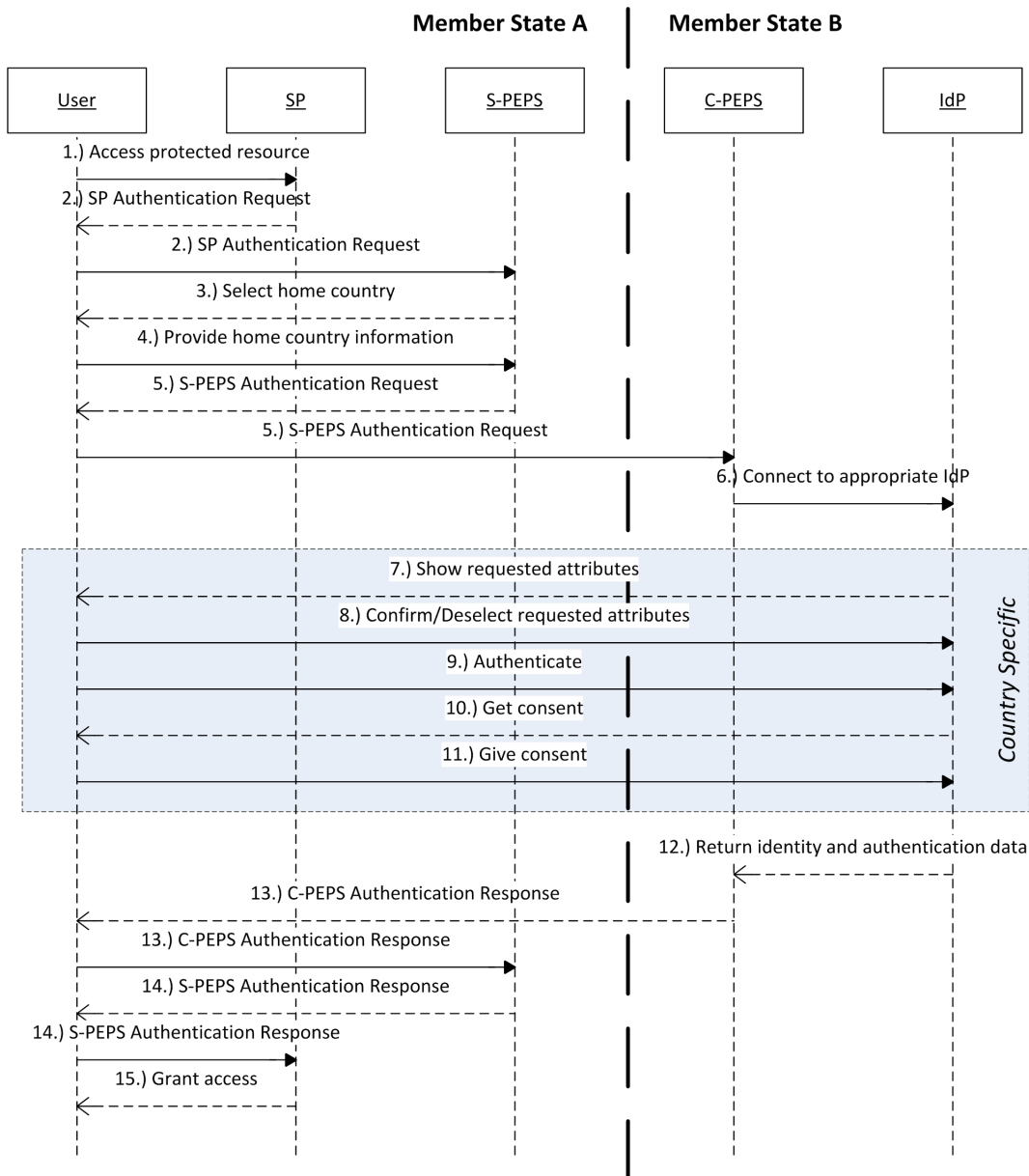


Figure 8.15: PEPS-PEPS process flow applying the *Privacy-Preserving Federated Identity as a Service-Model* [Zwattendorfer and Slamánig, 2013b]

9. *Authenticate*: Depending on the IdP, the citizen authenticates using the respective authentication method. For the highest authentication level reqQAA, the citizen must authenticate using her official national eID.
10. *Get consent*: Instead of the C-PEPS in the current situation, in this scenario the IdP sends `attr` to the citizen to get consent for further transmission to the C-PEPS and SP subsequently.
11. *Give consent*: The citizen may give or deny consent for `attr` transmission. Additionally, the IdP encrypts `attr` and QAA for the C-PEPS resulting in $c'_{C-PEPS} = \text{RE.Enc}(\text{rp}k_{C-PEPS}, \text{attr}||\text{QAA})$.
12. *Return identity and authentication data*: Subsequently, the IdP generates the signature $\sigma_{IdP} = \text{DSS.Sign}(\text{sk}'_{IdP}, c'_{C-PEPS})$ and transfers $(\sigma_{IdP}, c'_{C-PEPS})$ to the C-PEPS.
13. *C-PEPS Authentication Response*: This step is similar to the current situation. However, in this

cloud-based approach, the C-PEPS verifies σ_{IdP} , re-encrypts c'_{C-PEPS} for the S-PEPS resulting in $c'_{S-PEPS} = \text{RE.ReEnc}(\text{rk}_{C-PEPS \rightarrow S-PEPS}, c'_{C-PEPS})$, and signs c'_{S-PEPS} using key sk'_{C-PEPS} . The signature denoted as σ'_{C-PEPS} and the ciphertext c'_{S-PEPS} are transmitted to the S-PEPS.

14. *S-PEPS authentication response*: The S-PEPS verifies σ'_{C-PEPS} and re-encrypts c'_{S-PEPS} for the SP using key $\text{rk}_{S-PEPS \rightarrow SP}$. Finally, the S-PEPS signs the resulting ciphertext c_{SP} using key sk'_{S-PEPS} . $(\sigma'_{S-PEPS}, c_{SP})$ are transmitted to the SP.
15. *Grant access*: The SP verifies σ'_{S-PEPS} and decrypts c_{SP} to extract `attr` and QAA. The SP checks the QAA the citizen has been authenticated with and based on the attributes `attr` received, the SP either grants or denies access to the requested service to the citizen.

8.5.3 Discussion

In this section the proposed cloud-based PEPS-PEPS approach is discussed firstly with respect to privacy and security aspects, and, secondly, with respect to operational and practicability issues.

8.5.4 Security and Privacy Discussion

As already noted, it is assumed that the cloud providers are acting *honest but curious*. In this section it is investigated which personal and thus sensitive information are disclosed to an S-PEPS or C-PEPS operated in the public cloud. Table 8.2 compares the information seen by the individual entities (SP, S-PEPS, C-PEPS, IdP) in the current PEPS-PEPS scenario with the cloud-based scenario.

Table 8.2: Comparison of personal data disclosure between the current and the cloud-based PEPS-PEPS approach [Zwattendorfer and Slamanig, 2013b]

Approach / Entity	SP	S-PEPS	C-PEPS	IdP
Current	reqAttr, reqQAA, sp_name, attr, QAA	reqAttr, reqQAA, sp_name, attr, QAA, country	reqAttr, reqQAA, sp_name, attr, QAA	reqAttr, reqQAA, sp_name, attr, QAA
Cloud	reqAttr, reqQAA, sp_name, attr, QAA	country	×	reqAttr, reqQAA, sp_name, attr, QAA

Note that the SP, in both approaches, clearly obtains all citizen information, since they are required for successfully providing its services.

The S-PEPS, acting as first gateway, also sees all citizen information in the current approach. Additionally, it gains knowledge on the country the citizen originates from. In contrast, the originating country remains the only information visible to the S-PEPS in the cloud-based approach. All other information is only available in encrypted form. With just the information of the country of origin, the S-PEPS is not able to determine the identity of any authenticating citizen.

For the current approach, also the C-PEPS sees all citizen information. Adopting the cloud-based approach, the C-PEPS is able to inspect processed data in encrypted form only, which does not allow for any personal data disclosure.

Finally, the IdP is considered to be trusted in the current and the cloud-based approach. The IdP gets knowledge on `reqAttr`, `reqQAA`, `sp_name`, `attr`, and `QAA`. Compared to the current approach, in the cloud-based approach the IdP gets to know which particular SP the information is provided to.

8.5.5 Practicability Discussion

In this section the proposed cloud approach based on selected criteria relating to practicability are discussed.

Re-Use of Existing Infrastructure: One criterion when designing the cloud approach was to keep as much as of the existing infrastructure unaltered or unchanged. In general, main parts of the existing infrastructure can be kept untouched. This is particular important for the individual countries' eID infrastructures, as no new eID solution needs to be rolled out, which follows the general objective of STORK. The remaining entities (SP, S-PEPS, C-PEPS, IdP) need to be adapted to support unidirectional multi-use PRE. The STORK protocol may need minor extensions only as SAML already supports the transfer of encrypted attributes and messages out of the box.

Conformance to Current Process Flow: When designing the cloud-based approach, care was taken on staying conform with the current process flow. Basically, for supporting the cloud approach no severe changes in the communication and authentication process flow are necessary. However, Steps 7 and 8 (*Show requested attributes* and *Confirm/Deselect requested attributes*) and Steps 10 and 11 (*Get consent* and *Give consent*) must be carried out at the IdP when operating the C-PEPS in a public cloud. The reason is that otherwise the C-PEPS could present the citizen a list of different attributes than actually requested from the IdP. In this case, the C-PEPS could provide the SP with more citizen information than actually required.

Scalability: The main objective of this work was to design a scalable PEPS-PEPS scenario as increased and high usage of STORK can be expected in the future. This objective is mainly realized by moving important components, where high load can be expected, such as the S-PEPS and the C-PEPS, into the public cloud. Load bottlenecks at the SP or IdP are rather unlikely, because not all citizens are going to use the same SP or IdP at the same time.

Governance Structure: The governance structure of the STORK framework is currently in its detailed setup process. Thereby, a European Commission body will manage and maintain the individual PEPS metadata. This metadata includes the URLs and the individual signature certificates of the countries' PEPS. For supporting the cloud-based approach, this governance structure needs to be extended. In particular, the European Commission body additionally will be responsible for managing and issuing appropriate encryption keys based on a public key infrastructure (PKI) to the individual PEPS. However, the effort for these tasks can be kept within reasonable limits as it can be considered to have one single S-PEPS and C-PEPS per country only.

8.6 Evaluation of Cloud Identity Models

In this section the various cloud identity management-models are evaluated, discussed, and compared based on different criteria [Zwattendorfer et al., 2014]. Comparison criteria are defined in the following Subsection 8.6.1 whereas the comparison itself is elaborated in Subsection 8.6.2.

8.6.1 Evaluation Criteria

The following criteria act as a basis for comparing the various cloud identity management-models. Some of the comparison criteria were selected or derived from Cao and Yang [2010], Nuñez et al. [2013], and Birrell and Schneider [2013]. The selected criteria target aspects of different areas (e.g., general architecture, trust, privacy, etc.). The diversity of the criteria was deliberately considered to give a comprehensive overview on the different cloud identity management-models.

Number of SPs supported: Is the model limited to one SP or can multiple SPs be supported?

Number of IdPs supported: Is the model limited to one IdP or can multiple IdPs be supported?

Trust domains: Is authentication supported only within a single trust domain or also across different trust domains?

Trust model: Is a direct trust model or a brokered trust model applied?

Trust in the cloud IdP/identity broker: Must the cloud identity provider/identity broker be trusted or can they be semi-trusted?

Single sign-on (SSO): Can the model support single sign-on (SSO)?

Storage location of identity data: Where are users' identity data stored?

Scalability: Is the model applicable in a large scale?

Extensibility: Is the model easily extensible e.g., by adding new service providers?

Governance framework: Is a governance framework involving several entities required?

Cost effectiveness: Is the model cost effective?

Confidentiality: Does the identity data stay confidential at the identity provider/identity broker?

Minimal/Selective disclosure: Can the user select the amount of identity data to be disclosed to the identity provider/service provider?

User control: Does the user have full control over her identity data?

Unlinkability: Is the user unlinkable to the identity provider/identity broker? In other words, are different authentication processes of the same user linkable?

Anonymity: Can the user stay anonymous with respect to the identity provider/identity broker?

8.6.2 Evaluation

In this section the individual cloud identity management-models are compared and evaluated with respect to the prior defined criteria. Table 8.3 shows and summarizes this comparison. For some comparisons qualitative arguments are used, for others quantitative arguments (low, medium, high), and for the rest simply boolean (e.g., yes/no for being applicable or not) arguments. The options marked in bold indicate the respective best option (only applicable for quantitative and boolean values). The underlying principle for all comparisons (in particular for those that are related to privacy such as confidentiality, minimal/selective disclosure, etc.) is assuming that an identity provider or an identity broker deployed in the cloud is acting *honest but curious* (thus being semi-trusted). In contrast to that, applications in the cloud and their hosting service providers are assumed as being trusted, as they anyhow require users' identity data for service provisioning.

In the following the various models are discussed based on the individual criteria.

Number of SPs supported: Since in the *Identity in the Cloud-Model* the service provider and the identity provider are the same entity, the identity provider can only serve one service provider. All other models have no such restriction and thus can provide multiple service providers with identity data.

Table 8.3: Comparison of the individual cloud identity management-Models based on selected criteria [Zwattendorfer et al., 2014]

Criterion vs. Model	Identity in the Cloud-Model	Identity to the Cloud-Model	Identity from the Cloud-Model	Cloud Identity Broker-Model	BlindIdM Model	Identity as a Service-Model for Electronic Identities	Federated Cloud Identity Broker-Model	Privacy-Preserving Federated Cloud Identity Broker-Model
<i>Number of SPs supported</i>	One	Multiple	Multiple	Multiple	Multiple	Multiple	Multiple	Multiple
<i>Number of IdPs supported</i>	One	One	One	Multiple	One	One	Multiple	Multiple
<i>Trust domains</i>	One	One	One	Multiple	One	One	Multiple	Multiple
<i>Trust model</i>	Direct	Direct	Direct	Brokered	Direct	Direct	Brokered	Brokered
<i>Trust in the cloud IdP/identity broker</i>	Trusted	Trusted	Trusted	Trusted	Semi-Trusted	Semi-Trusted	Trusted	Semi-Trusted
<i>Single sign-on (SSO)</i>	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<i>Storage location of identity data</i>	Cloud identity provider	External identity provider	Cloud identity provider	Cloud identity provider and external identity provider	Cloud identity provider	eID of the user	Cloud identity provider and external identity provider	Cloud identity provider and external identity provider
<i>Scalability</i>	Medium	Low	Medium	High	Medium	Medium	High	High
<i>Extensibility</i>	Low	Medium	Medium	High	Medium	Medium	High	High
<i>Governance framework</i>	No	No	No	Yes	Yes	Yes	Yes	Yes
<i>Cost effectiveness</i>	Medium	Medium	Medium	High	Medium	Medium	High	High
<i>Confidentiality</i>	No	No	No	No	Yes	Yes	No	Yes
<i>Minimum/Selective disclosure</i>	No	Yes	No	Yes	No	Yes	Yes	Yes
<i>User Control</i>	No	Yes	No	Yes	No	Yes	Yes	Yes
<i>Unlinkability</i>	No	No	No	No	No	No	No	Yes
<i>Anonymity</i>	No	No	No	No	Yes	Yes	No	Yes

Number of IdPs supported: Only those models that rely on a broker-based approach are able to deal with multiple connected identity providers. All others just include one identity provider. Dealing with multiple identity providers has the advantage that a user can simply select her preferred identity provider for an authentication process. Different identity providers can have different identity data stored or support different qualities in the authentication mechanisms. This allows users to select the identity provider satisfying best the needs for authentication at a service provider. The

Identity as a Service-Model for Electronic Identities also supports multiple identity providers if the support of different eIDs is treated as the support of different identity providers.

Trust domains: The broker-based models support authentication across multiple trust domains, as multiple entities are involved during an authentication process. All others support authentication in single domains only. Single trust domains are usually easier to manage than multiple trust domains.

Trust model: Again, all models which rely on an identity broker also feature a brokered trust model, hence the trust relationships are segmented. All other models rely on a direct or pairwise trust model, as only the service provider and the identity provider communicate with each other during an authentication process. A clear statement which model has more advantages cannot be made. Both have their benefits and drawbacks, however, direct trust relationships are probably easier to manage. Details on the individual trust models can be found in Section 3.1.6 and in Linn et al. [2004].

Trust in the cloud IdP/identity broker: For the three models (*BlindIdM-Model*, *Identity as a Service-Model for Electronic Identities*, and *Privacy-Preserving Federated Cloud Identity Broker-Model*), which rely on proxy re-encryption for securing the data during cloud transmission, it is sufficient when the identity provider/identity broker is considered semi-trusted. In all other cloud identity models the identity provider/identity broker must be trusted.

Single sign-on (SSO): In fact, all models that can handle multiple service providers are principally applicable to support single sign-on. This means, that only the *Identity in the Cloud-Model* cannot support a simplified log-in process.

Storage location of identity data: In the *Identity to the Cloud-Model* identity data are stored on a single external identity provider, which is capable of providing identity data to the cloud application through a well-defined interface. In the broker-based models, identity data can be stored distributed across multiple different identity providers, being either deployed in the cloud or in a conventional data center. However, the different identity providers could also have identity data stored redundantly, i.e., the same attribute name/value-pair is stored at different providers. No identity data are actually stored at the identity broker. Also in the *Identity as a Service-Model for Electronic Identities* no identity data is stored at the identity provider and hence in the cloud. In this model, all identity data are stored user-centric on the users eID. In the remaining cloud identity models identity data are stored directly at the cloud identity provider.

Scalability: The *Identity to the Cloud-Model* has the lowest scalability, as an external identity provider is usually not designed for dealing with high load activities. In addition, an external identity provider has not that flexibility or elasticity that an identity provider deployed in a cloud has. Hence, cloud identity providers (*Identity in the Cloud-Model*, *Identity from the Cloud-Model*, *BlindIdM-Model*, and *Identity as a Service-Model for Electronic Identities*) have higher scalability features. Although in these three models the identity provider/identity broker is deployed in the cloud, the models were rated just with medium level scalability. The reason is that with the broker-based models load can additionally be distributed to other identity providers and thus is not bundled at one single provider. Hence, the broker-based models achieve the highest scalability.

Extensibility: The *Identity in the Cloud-Model* cannot be extended because service provider and identity provider are one and the same entity. The *Identity to the Cloud-Model*, the *Identity from the Cloud-Model*, the *BlindIdM-Model*, and the *Identity as a Service-Model for Electronic Identities* can be extended to integrate additional service providers. Nevertheless, the broker-based models have the best extensibility as from their nature the general aim is to support multiple service providers and identity providers.

Governance framework: The non-broker-based cloud identity models do not require an extensive governance framework as only a simple pairwise (direct) trust model applies. In the broker-based concepts a thorough governance framework is required as multiple providers have to interact. For the privacy-preserving models (*BlindIdM-Model*, *Identity as a Service-Model for Electronic Identities*, and *Privacy-Preserving Federated Cloud Identity Broker-Model*) the governance framework gets even more complex, as encryption keys have to be managed for the individual entities.

Cost effectiveness: The broker-based models have the highest cost effectiveness, since the identity brokers are deployed in the cloud and additionally multiple identity providers can be connected and re-used. Due to the re-use of existing external identity providers, costs can be saved. The same arguments also hold for the *Identity to the Cloud-Model*, where an existing identity management-system through an external interface is re-used for identity data provisioning. However, this model cannot benefit from the advantages of an identity provider in the cloud deployment, which leads to medium cost effectiveness only. All other models also have medium cost effectiveness, as the identity provider is deployed in the cloud but no existing identity providers can be re-used.

Confidentiality: Only the *BlindIdM-Model*, the *Identity as a Service-Model for Electronic Identities*, and the *Privacy-Preserving Federated Cloud Identity Broker-Model* support confidentiality with respect to the cloud service provider because the identity data transferred through the cloud service provider are encrypted. In comparison, in all other cloud identity models identity data are routed in plain through the cloud service provider that hosts the cloud identity provider/identity broker.

Minimum/Selective disclosure: For evaluating this criterion it was assumed that minimum/selective disclosure is in any case possible at trusted identity providers. Hence, this feature is naturally supported where external (and trusted) identity providers are part of the model. These are the broker-based models as well as the *Identity to the Cloud-Model*. Furthermore, selective disclosure is possible in the *Identity as a Service-Model for Electronic Identities*, which was explicitly designed to support this feature. All other models rely on cloud identity providers only.

User control: Again, for evaluating this criterion it was assumed that full user-control is supported best with trusted identity providers. In addition, the *Identity as a Service-Model for Electronic Identities* puts the user under full control of her identity data. Therefore, the same results as for the comparison with respect to minimum/selective disclosure apply.

Unlinkability: The user – in fact – is only unlinkable with respect to the identity broker in the *Privacy-Preserving Federated Cloud Identity Broker-Model*. The reasons are that, on the one hand, the identity broker just sees encrypted data and, on the other hand, that the encrypted data can be randomized if certain proxy re-encryption schemes such as from Ateniese et al. [2006] are used. The randomization feature allows to provide the identity broker with different ciphertexts during different authentication processes although the containing plaintext data remains the same. Hence, this avoids user linkage during different authentication processes of the same user. Although the *BlindIdM-Model* supports proxy re-encryption too, the randomization feature has no effect in this case because the encrypted data are directly stored at the cloud identity provider. If the user wants to update her encrypted identity data at the cloud identity provider, she must somehow be linkable. The same argument also holds for the *Identity as a Service-Model for Electronic Identities*, because randomization techniques are not applicable in this model since the encrypted data are signed by a trusted authority and permanently stored on the user's eID. All other models also do not support unlinkability because identity data flows through the identity provider/identity broker in plaintext.

Anonymity: The only three models that support anonymity with respect to the identity broker are the *BlindIdM-Model*, the *Identity as a Service-Model for Electronic Identities*, and the *Privacy-Preserving Federated Cloud Identity Broker-Model*. In these three models the identity data are

fully hidden from the identity broker due to encryption. Even if the user is linkable, the broker cannot reveal the user's identity. In all other models anonymity with respect to the identity provider/identity broker is not possible because identity data are processed in plaintext.

8.7 Chapter Conclusions

Reliable and secure user identification and authentication are key enablers for regulating access to protected online services. Identification and authentication in and across clouds play an increasing role in this domain too. Several new cloud identity management models such as the *Cloud Identity Broker-Model* have emerged. In this model, an identity broker in the cloud acts as intermediary and as some kind of hub between various service and identity providers. While the *Cloud Identity Broker-Model* seems to be a promising approach for adopting identity management in cloud computing, still some problems with this model can be identified. A notable issue is the dependency of users and service providers on the same central cloud identity broker for identification and authentication processes. Additionally, letting an identity broker to store or process sensitive data such as identity information in the cloud brings up new issues, in particular with respect to user's privacy. To overcome these problems, new cloud identity management models based on the federation between different cloud identity brokers were proposed. Thereby, users and service providers can select their favorite cloud identity broker of choice without being dependent on one and the same broker. Moreover, the *Privacy-Preserving Federated Identity as a Service-Model* enhances user's privacy by the use of proxy re-encryption.

In the proof of concept implementation it was shown that federating identity brokers enables users greater flexibility in identity/attribute provider selection. However, there is a brokered trust relationship between an identity provider and a service provider and no direct one. This might bring up liability discussions, in particular, if identity providers are grounded by national law.

To further demonstrate the applicability of this *Federated Identity as Service-Model*, a solution was presented by moving centralized country PEPS of the STORK framework into a public cloud, which considerably improves scalability. It can be concluded that in terms of privacy, no identifying citizen information will be disclosed to a PEPS in the public cloud when applying the proposed approach. Additionally, existing national eID infrastructures can be kept untouched and no major changes to the current authentication process flow are required. Furthermore, the proposed solution perfectly fits into the STORK governance structure, which is currently being established.

Finally, based on the comparison and discussion of the different cloud identity management-models it can be concluded that the *Privacy-Preserving Federated Cloud Identity Broker-Model* does best with respect to the selected criteria. It supports the main basic functions like all other cloud identity models but additionally tremendously increases users' privacy.

Chapter 9

Summary and Conclusions

Electronic Government (e-Government) facilitates governmental and public administrative procedures by the help of information and communication technologies. Thereby, the efficiency and productivity of governmental procedures can be increased as they can be processed electronically and thus automatically. In addition, also citizens and businesses can benefit from e-Government. For instance, in many situations physical presence during public authorities' office hours is not required anymore because many governmental services are offered and provided online 24/7.

Austria is one of the leading countries in Europe supporting and promoting the use of e-Government. A thorough organizational, legal, and technical framework has been developed over the past years. Based on these frameworks, many e-Government services on different levels (informational, transactional, or integrated services) are already offered online by Austrian public authorities. One main pillar of the Austrian e-Government strategy is a sophisticated identification and authentication system based on electronic identities (eIDs). Thereby, the Austrian citizen card, the official eID in Austria, plays a major role.

Besides Austria, also many other European countries put efforts to foster e-Government. These efforts were mainly tailored to support domestic requirements only. However, for being able to strengthen the EU internal market, data and services also need to be exchanged electronically and accepted across borders. Cross-border services definitely can strengthen the European economy and help in becoming a more dynamic and knowledge-based society. In order to achieve this, cross-border interoperability of the heterogeneous landscape of existing systems, solutions, and infrastructures in the individual member states has been identified by the EU as one of the biggest challenges. To tackle the challenge of cross-border interoperability in public sector areas, the European Commission made a lot of strategic commitments and installed appropriate initiatives and technical programmes.

One of these challenges was also to tackle the challenge of eID interoperability, since the eID landscape across Europe is very heterogeneous. The cross-border acceptance of eIDs is crucial for the support of pan-European e-Government services. To achieve interoperability, the European Commission put a lot of effort in corresponding initiatives and projects. On technical level, the European Commission launched the LSP projects STORK and STORK 2.0 to deal with technical issues on eID acceptance for natural and legal persons. STORK was deeply discussed in this thesis. In particular, the author explained the different interoperability models, their architecture and implementations, and finally the integration of the STORK framework into the Austrian eID concept and infrastructure.

STORK was a success, as cross-border acceptance of national eIDs could be successfully demonstrated in real applications and environments. However, while STORK showed that cross-border eID interoperability is technically feasible, some hindering issues still remain open for future investigations. Issues on organizational level are for example the mapping of personal identifiers from national registers between countries. Another issue is the harmonization of legislation as e.g., eID registration procedures vary between countries. However, this issue will be mainly tackled by the upcoming eIDAS regulation and their implementing acts. Furthermore, in terms of acceptance of individual credentials for authen-

tication still some work needs to be done. For instance, to qualitatively ensure the authentication levels proposed by STORK some independent auditing and validation procedures would be required. Finally, a thorough governance framework needs to be set up to securely manage the trust relationships between the various involved entities.

Cloud computing and its flexible business model of consuming IT resources such as computing power or data storage just on demand promises a lot of benefits and advantages. These advantages also the public sector and governments can benefit from. Many countries have already recognized the benefits of cloud computing for governmental applications and thus have already installed their own cloud systems or have transferred applications into the cloud. Hence, the move of existing services into the cloud could be another piece of the puzzle to strengthen the European digital internal market. Within the public sector the private cloud model or community cloud model currently constitute the dominant deployed approaches. Although this model offers high control it does not take full advantage of the economic benefits of cloud computing. Therefore, in this thesis it was shown that public clouds have the highest economic benefits and thus should be also considered for e-Government. Nevertheless, the move of e-Government services – if sensitive data need to be stored or processed – into the cloud is not trivial, in particular when aiming on migrating or developing applications for the public cloud.

Cloud computing and its benefits can also impact identity management and eID systems. Since cloud computing gains more and more importance, identification and authentication in and across clouds play an increasing role in this domain too. Username/password schemes are still the dominant authentication approach used for protecting SaaS applications. While username/password schemes may be sufficient for simple personalized services, they reach their limits in data sensitive areas such as e-Government. E-Government services require higher security requirements as usually sensitive data are processed. One possibility to meet those requirements is the use of stronger authentication mechanisms for protecting SaaS applications e.g., by the use of eIDs. In this thesis the author demonstrated the use of various national eID solutions for secure cloud authentication. The author therefore relied on the STORK eID interoperability framework, which will be the dominant identification and authentication framework across Europe in future. The author demonstrated the applicability of this approach by securely authenticating at two different public cloud service providers (Google and Salesforce.com) using various national eIDs. The support of high assurance credentials offers cloud service providers the possibility to penetrate new market areas for business generation. While it was illustrated that the use of eIDs for cloud authentication is technically feasible, still cloud providers need to hop on the bandwagon to support high secure authentication mechanisms.

While identity management does not define a new topic, identity management in the cloud brings up new challenges. Traditional identity models have already been transferred to the cloud, hence different cloud identity models have emerged. Depending on the cloud identity model, identity data are either provided in the cloud, to the cloud, or from the cloud. Outsourcing identity management systems to the cloud can bring up several benefits such as higher scalability or cost savings, since no in-house infrastructure needs to be hosted and maintained. However, when porting an identity management system into the public cloud several privacy issues may occur as the cloud service provider operating the identity provider might be able to inspect stored or processed identity data. The author encountered these privacy issues by introducing and evaluating three distinct approaches relying on different cryptographic technologies (proxy re-encryption and redecryptable signatures, anonymous credentials, and fully homomorphic encryption). As a result from an evaluation, the approach using proxy re-encryption and redecryptable signatures turned out to do best as it could be quickly realized and requires less effort for changing existing infrastructure. The applicability of this approach has been further demonstrated by applying it to the Austrian eID system.

Besides these cloud identity models, where an identity provider is operated in the cloud, several new cloud identity management models such as the *Cloud Identity Broker-Model* have emerged. In this model, an identity broker in the cloud acts as intermediary and as some kind of hub between various service and identity providers. While the *Cloud Identity Broker-Model* seems to be a promising approach for

adopting identity management in cloud computing, a notable issue is the dependency of users and service providers on the same central cloud identity broker for identification and authentication processes. To bypass this issue, the author proposed a new cloud identity management model based on the federation between different cloud identity brokers (*Federated Identity as a Service-Model*). Thereby, users and service providers can select their favorite cloud identity broker of choice without being dependent on one and the same broker. Moreover, the author proposed an advanced model (*Privacy-Preserving Federated Identity as a Service-Model*), which enhances user's privacy by the use of proxy re-encryption. The applicability of this *Privacy-Preserving Federated Identity as a Service-Model* was demonstrated by a proof of concept implementation and by applying it to the STORK PEPS-PEPS approach.

Based on a comparison and discussion of the different cloud identity management-models it can be concluded that the *Privacy-Preserving Federated Cloud Identity Broker-Model* does best with respect to the selected criteria of the evaluation. It supports the main basic functions like all other cloud identity models but additionally tremendously increases users' privacy. However, application of this model is also more complex than of the others. Reasons are the support of authentication across several domains of multiple identity providers and service providers and the incorporation of privacy features due to the use of proxy re-encryption. Furthermore, the use of proxy re-encryption requires a thorough key management, which implies the necessity of an appropriate governance framework. In addition, the brokered trust model might be a blocking issue for further adoption of this model as liability is shifted to the intermediary components (identity brokers). However, in general the broker-based cloud identity management-models have more advantages than the simple cloud identity management-models. Nevertheless, the use of any cloud identity management-model is advantageous compared to traditional identity management-models as they provide higher scalability and better cost effectiveness due to the cloud computing features.

Appendix A

List of Acronyms

3DES	Triple DES
A-SIT	Secure Information Technology Center - Austria
ABAC	Attribute Based Access Control
ABC4Trust	Attribute-based Credentials for Trust
AC	Anonymous Credential
API	Application Programming Interface
AS	Anonymous Signature
BELPIC	Belgian Personal Identity Card
BMR	Bilateral Mandate Register
BMWi	Federal Ministry of Economics and Technology
C-PEPS	Citizen PEPS
C2B	Citizen-to-Businesses
CA	Certificate Authority
CA	Competent Authority
CAS	Central Authentication Service
CCE	Citizen Card Encrypted
CCS	Citizen Card Software
CEN	Comité Européen de Normalisation
CERT	Computer Emergency Response Team
CIE	Carta d'Identita Elettronica
CIP	Competitiveness and Innovation Framework Programme
CMS	Cryptographic Message Syntax

CNS	Carta Nazionale dei Servizi
CP	Control Party
CR	Company Register
CRM	Customer Relationship Management
CRR	Central Register of Residence
CSA	Cloud Security Alliance
CTO	Chief Technology Officer
DDS	Document Delivery System
DES	Data Encryption Standard
DILA	Directorate of Legal and Administrative Information
DNS	Domain Name System
DOS	Denial of Service
DSS	Digital Signature Scheme
e-Accessibility	Electronic Accessibility
e-Attestation	Electronic Attestation
e-Banking	Electronic Banking
e-Business	Electronic Business
e-Catalogue	Electronic Catalogue
e-CODEX	E-Justice Communication via Online Data Exchange
e-Delivery	Electronic Delivery
e-Democracy	Electronic Democracy
e-Documents	Electronic Documents
e-Government	Electronic Government
e-Health	Electronic Health
e-Inclusion	Electronic Inclusion
e-Invoicing	Electronic Invoicing
e-Justice	Electronic Justice
e-Learning	Electronic Learning
e-Mail	Electronic Mail
e-Ordering	Electronic Ordering
e-Participation	Electronic Participation

e-Payment	Electronic Payment
e-Prescription	Electronic Prescription
e-Procurement	Electronic Procurement
e-Purchasing	Electronic Purchasing
e-SENS	Electronic Simple European Networked Services
e-Services	Electronic Services
e-Signature	Electronic Signature
e-Tendering	Electronic Tendering
e-Voting	Electronic Voting
ECAS	European Commission Authentication Service
ECC	European Citizen Card
eD	eDispensation
eID	Electronic Identity
EIF	European Interoperability Framework
EIS	European Interoperability Strategy
EJB	Enterprise Java Beans
ENISA	European Network and Information Security Agency
eP	ePrescription
EPAL	Enterprise Privacy Authorization Language
eps	e-Payment standard
epSOS	Smart Open Services for European Patients
EU	European Union
F-IdP	Foreign IdP
FHE	Fully Homomorphic Encryption
FIDIS	Future of Identity in the Information Society
FP	Framework Programme
G-Cloud	Governmental Cloud
G2B	Government-to-Businesses
G2C	Government-to-Citizens
G2E	Government-to-Employee
G2G	Government-to-Government

G2N	Government-to-Nonprofit
G2SC	Government-to-Civil Society Organizations
GDP	Gross Domestic Product
GITS	Government Information Technology Service
GSA	General Service Administration
GW	Gateway
HCP	Health Care Professional
HSM	Hardware Security Module
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
I-S-A	Identification – Signature – Authentication
i-Voting	Internet Voting
laaS	Infrastructure as a Service
ICT	Information an Communication Technology
IDA	Interchange of Date between Administrations
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens
Idemix	Identity Mixer
IdM	Identity Management
IdMaaS	Identity Management as a Service
IdP	Identity Provider
IEC	International Electrotechnical Commission
IND-CPA	Indistinguishability Under Chosen Plaintext Attacks
IP	Internet protocol suite
ISA	Interoperable Solutions for European Public Administrations
ISO	International Organization for Standardization
ISSS	Information Society Standardisation System
IT	Information Technology
J2EE	Java Enterprise Edition
Jasig	Java Architectures Special Interest Group
JSON	JavaScript Object Notation

JTC	Joint Technical Committee
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
LoA	Level of Assurance
LSP	Large Scale Pilot
MARS	Modular Authentication Relay Service
MIS	Mandate Issuing Service
MOA-ID	Module für Online Applikationen – Identifikation
MOA-SP	Module für Online Applikationen – Signaturprüfung
MOA-SS	Module für Online Applikationen – Serversignatur
MOA-ZS	Module für Online Applikationen – Zustellung
MOCCA	Modular Open Citizen Card Architecture
MW	Middleware
N2G	Nonprofit-to-Government
NCP	National Contact Point
NIST	National Institute of Standards and Technology
nPA	neuer Personalausweis
NSTC	National Science and Technology Council
OA	Online Application
OASIS	Organization for the Advancement of Structured Information Standards
OCD	Omnifarious Container for e-Documents
OCSP	Online Certificate Status Protocol
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PC	Personal Computer
PC/SC	Personal Computer/Smart Card
PDF	Portable Document Format
PDF-AS	PDF Amtssignatur
PEPPOL	Pan-European Public Procurement Online
PEPS	Pan-European Proxy Service
PIC	Personal Identification Code

PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PRIME	Privacy and Identity Management for Europe
PS	Patient Summary
PSC	Point of Single Contact
PSP	Policy Support Programme
QAA	Quality Authentication Assurance
R&D	Research and Development
RA	Registration Authority
RBAC	Role Based Access Control
RE	Re-Encryption
REST	Representational State Transfer
RFC	Request for Comments
ROI	Return on Investment
RS	Redactable Signature
RSa	Rückscheinbrief blau
RSb	Rückscheinbrief weiß
S/MIME	Secure/Multipurpose Internet Mail Extensions
S-PEPS	Service Provider PEPS
SaaS	Software as a Service
S2ML	Security Services Markup Language
SAML	Security Assertion Markup Language
SC	Smart Card
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SEPA	Single Euro Payment Area
SHA	Secure Hash Algorithm
SLO	Single Logout
SOA	Service Oriented Architecture

SOAP	SOAP
SP	Service Provider
SPOCS	Simple Procedures Online for Cross-border Services
SPR	SourcePIN Register
SPR-GW	SourcePIN Register – Gateway
SR	Supplementary Register for Natural Persons
SRA	SourcePIN Register Authority
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
SSO	Single Sign-On
ssPIN	Sector-Specific Personal Identification Number
ssPINenc	Encrypted ssPIN
STORK	Secure Identity Across Borders Linked
STS	Security Token Service
SWOT	Strengths-Weaknesses-Opportunities-Threats
TC	Technical Committee
TCP	Transmission Control Protocol
TESTA	Trans-European Services for Telematics between Administrations
TLS	Transport Layer Security
TOC	Total Cost of Ownership
TPM	Trusted Platform Module
TS	Technical Specification
TS	Timestamp
TSL	Trust-Service Status List
UAE	United Arab Emirates
UF-CMA	Unforgeability Under Chosen Message Attack
UK	United Kingdom
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
US	United States
USA	United States of America

USB	Universal Serial Bus
VCD	Virtual Company Dossier
VIDP	Virtual Identity Provider
WAI	Web Accessibility Initiative
WG	Working Group
WS	Web Service
WS-Federation	Web Service – Federation
WS-Policy	Web Service – Policy
WS-Security	Web Service – Security
WS-Trust	Web Service – Trust
XaaS	Everything as a Service
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language
XMLDSig	XML Digital Signature
XRI	Extensible Resource Identifier

Appendix B

List of Publications

The following list contains publications which were published prior or during the course of this thesis and are related to this work. The publications and their relevance are grouped by chapter, if possible. However, a few publications may occur more than once since they could not be clearly categorized into one chapter.

Chapter 2 – E-Government

- Posch, Reinhard, Clemens Orthacker, Klaus Stranacher, Arne Tauber, Thomas Zefferer, and Bernd Zwattendorfer [2010]. *Open Source Bausteine als Kooperationsgrundlage*. In Eixelsberger/Stember, *E-Government - Zwischen Partizipation und Kooperation*, pages 185–210. Springer Wien-New York.
- Posch, Karl-Christian, Reinhard Posch, Arne Tauber, Thomas Zefferer, and Bernd Zwattendorfer [2011]. In *Secure and Privacy-Preserving eGovernment - Best Practice Austria*. *Rainbow of Computer Science*, pages 259–269. Springer Berlin Heidelberg.
- Stranacher, Klaus, Arne Tauber, Thomas Zefferer, and Bernd Zwattendorfer[2013c]. *The Austrian Identity Ecosystem: An E-Government Experience*. In Martínez, Antonio Ruiz, Rafael Marin-Lopez, and Fernando Pereniguez-Garcia, *Architectures and Protocols for Secure Information Technology Infrastructures*, pages 288–309. IGI Global.
- Lenz, Thomas, Bernd Zwattendorfer, Klaus Stranacher, and Arne Tauber [2014]. *Identitätsmanagement in Österreich mit MOA-ID 2.0*. *eGovernment Review*, 13, pages 20–21.

Chapter 3 – Electronic Identity

- Zwattendorfer, Bernd, Arne Tauber, and Thomas Zefferer [2011a]. *A privacy-preserving eID based Single Sign-On solution*. In *5th International Conference on Network and System Security*, pages 295–299. IEEE.
- Zwattendorfer, Bernd, Thomas Zefferer, and Arne Tauber [2012d]. *The prevalence of SAML within the European Union*. In *8th International Conference on Web Information Systems and Technologies (WEBIST)*, pages 571–576.
- Tauber, Arne, Bernd Zwattendorfer, and Klaus Stranacher [2013]. *Elektronische Identität und Stellvertretung in Österreich*. In *D-A-CH Security 2013*, pages 1–9.

- Stranacher, Klaus, Arne Tauber, Thomas Zefferer, and Bernd Zwattendorfer [2013c]. *The Austrian Identity Ecosystem: An E-Government Experience*. In Martínez, Antonio Ruiz, Rafael Marin-Lopez, and Fernando Pereniguez-Garcia, *Architectures and Protocols for Secure Information Technology Infrastructures*, pages 288–309. IGI Global.

Chapter 4 – Cross-Border E-Government

- Zwattendorfer, Bernd, Thomas Zefferer, and Arne Tauber [2011b]. *E-ID Meets E-Health on a Pan-European Level*. In *Proceedings of the IADIS International Conference e-Health*, pages 97–104.
- Stranacher, Klaus, Arne Tauber, Thomas Zefferer, and Bernd Zwattendorfer [2011]. *Grenzüberschreitendes E-Government in Europa*. *eGovernment Review*, 8, pages 8–9.

Chapter 5 – Cross-Border Electronic Identity

- Tauber, Arne, Bernd Zwattendorfer, Thomas Zefferer, Yasmin Mazhari, and Eleftherios Chamakiotis [2010]. *Towards interoperability: an architecture for pan-European eID-based authentication services*. In *Proceedings of the International Conference on Electronic Government and the Information Systems Perspective (EGOVIS)*, pages 120–133.
- Zwattendorfer, Bernd and Ivo Sumelong [2011]. *Interoperable Middleware-Architektur für sichere, länderübergreifende Identifizierung und Authentifizierung*. In *Tagungsband zum 12. Deutschen IT-Sicherheitskongress*, pages 175–189. SecuMedia.
- Leitold, Herbert and Bernd Zwattendorfer [2011]. *STORK: Architecture, Implementation and Pilots*. In *ISSE 2010 Securing Electronic Business Processes*, pages 1–11.
- Knall, Thomas, Arne Tauber, and Thomas Zefferer [2011]. *Secure and Privacy-Preserving Cross-Border Authentication: The STORK Pilot 'SaferChat'*. In *Proceedings of the Conference on Electronic Government and the Information Systems Perspective (EGOVIS 2011)*, pages 94–106.
- Tauber, Arne, Bernd Zwattendorfer, and Thomas Zefferer [2011d]. *STORK: Pilot 4 Towards Cross-border Electronic Delivery*. In *Electronic Government and Electronic Participation - Joint Proceedings of Ongoing Research and Projects of IFIP EGOV and ePart 2011*, pages 295–301.
- Tauber, Arne, Thomas Zefferer, and Bernd Zwattendorfer [2012]. *Approaching the Challenge of eID Interoperability: An Austrian Perspective*. *European Journal of ePractice*, 14, pages 22–39.
- Zwattendorfer, Bernd, Ivo Sumelong, and Herbert Leitold [2012b]. *Middleware Architecture for Cross-Border eID*. In *Eighth International Conference on Information Assurance and Security (IAS)*, pages 303–308. IEEE.
- Zwattendorfer, Bernd, Arne Tauber, Klaus Stranacher, and Peter Reichstädter [2012c]. *Cross-Border Legal Identity Management*. In *Electronic Government 11th IFIP WG 8.5 International Conference, EGOV 2012*, pages 149–161.
- Zwattendorfer, Bernd, Ivo Sumelong, and Herbert Leitold [2013c]. *Middleware Architecture for Cross-Border Identification and Authentication*. *Journal of information assurance and security (JIAS)*, 8, pages 107–118.

Chapter 6 – Cloud Computing

- Zwattendorfer, Bernd and Arne Tauber [2012c]. *The Public Cloud for e-Government*. In *Technology-Enabled Innovation for Democracy, Government and Governance*, pages 129–136.
- Zwattendorfer, Bernd and Arne Tauber [2013]. *The Public Cloud for e-Government*. *International Journal of Distributed Systems and Technologies*, 4(4), pages 1–14.
- Zwattendorfer, Bernd, Klaus Stranacher, Arne Tauber, and Peter Reichstädter [2013b]. *Cloud Computing in E-Government across Europe*. In *Technology-Enabled Innovation for Democracy, Government and Governance*, pages 181–195.
- Zwattendorfer, Bernd, Bojan Suzic, Peter Teufl, and Andreas Derler [2013d]. *Secure Hardware-Based Public Cloud Storage*. In *Open Identity Summit 2013*, pages 43–54.
- Zwattendorfer, Bernd, Bojan Suzic, Peter Teufl, and Andreas Derler [2013e]. *Sicheres Speichern in der Public Cloud mittels Smart Cards*. In Schartner, Peter and Peter Trommler, *D-A-CH Security 2013*, pages 120–132.

Chapter 7 – Electronic Identity and Cloud Computing

- Zwattendorfer, Bernd, Klaus Stranacher, and Arne Tauber [2012a]. *Bürgerkarten-Authentifizierung zur Public Cloud*. In *D-A-CH Security 2012*, pages 136–147.
- Zwattendorfer, Bernd and Arne Tauber [2012a]. *Secure cloud authentication using eIDs*. In *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, pages 397–401. IEEE. Best Paper Award.
- Zwattendorfer, Bernd and Arne Tauber [2012b]. *Secure cross-cloud single sign-on (SSO) using eIDs*. In *Internet Technology And Secured Transactions (ICITST)*, pages 150–155.
- Zwattendorfer, Bernd and Daniel Slamanig [2013a]. *On Privacy-Preserving Ways to Porting the Austrian eID System to the Public Cloud*. In *28th IFIP TC-11 International Information Security and Privacy Conference (SEC 2013)*, pages 300–314.
- Zwattendorfer, Bernd and Daniel Slamanig [2013c]. *Scalable and Privacy-Preserving Variants of the Austrian Electronic Mandate System in the Public Cloud*. In *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEETrustCom-13)*, pages 24–33.
- Zwattendorfer, Bernd, Thomas Zefferer, and Klaus Stranacher [2014]. *An Overview of Cloud Identity Management-Models*. In *10th International Conference on Web Information Systems and Technologies (WEBIST)*, pages 82–92. SCITEPRESS Digital Library.
- Slamanig, Daniel, Klaus Stranacher, and Bernd Zwattendorfer [2014]. *User-Centric Identity as a Service-Architecture for eIDs with Selective Attribute Disclosure*. In *ACM Symposium on Access Control Models and Technologies (SACMAT)*. in press.

Chapter 8 – Federated Identity as a Service

- Zwattendorfer, Bernd, Klaus Stranacher, and Arne Tauber [2013a]. *Towards a Federated Identity as a Service Model*. In *Technology-Enabled Innovation for Democracy, Government and Governance*, pages 43–57.

- Zwattendorfer, Bernd and Daniel Slamanig [2013b]. *Privacy-Preserving Realization of the STORK Framework in the Public Cloud*. In *10th International Conference on Security and Cryptography (SECRYPT 2013)*, pages 419–426. SCITEPRESS Digital Library.
- Zwattendorfer, Bernd, Thomas Zefferer, and Klaus Stranacher [2014]. *An Overview of Cloud Identity Management-Models*. In *10th International Conference on Web Information Systems and Technologies (WEBIST)*, pages 82–92. SCITEPRESS Digital Library.
- Zwattendorfer, Bernd, Klaus Stranacher and Felix Hörandner [2014]. *Föderiertes Identitätsmanagement in der Cloud*. In *D-A-CH Security 2014*, in press.
- Zwattendorfer, Bernd, Daniel Slamanig, Klaus Stranacher and Felix Hörandner [2014]. *A Federated Cloud Identity Broker-Model for Enhanced Privacy via Proxy Re-Encryption*. Under review.

A complete list containing the whole set of publications of the author can be found on https://online.tugraz.at/tug_online/voe_main.persVoes?pPersonNr=60830.

Bibliography

- Abelson, Hal and Lawrence Lessig [1998]. *Digital Identity in Cyberspace*. <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall98-papers/identity/white-paper.html>.
- Alamäki, Tero, Margareta Björkstén, Péter Dornbach, Casper Gripenberg, Norbert Györbíró, Gábor Márton, Zoltán Németh, Timo Skyttä, and Mikko Tarkiainen [2003]. *Privacy enhancing service architectures*. In Dingledine, Roger and Paul Syverson (Editors), *Privacy Enhancing Technologies*, pages 99–109. Springer.
- Albertazzie, Sally [2012]. *E-Commerce Law Week, Issue 719*. *E-Commerce Law Week*, 8(719).
- Alcalde-Moraño, Joaquín, Jorge López Hernández-Ardieta, Adrian Johnston, Daniel Martinez, Bernd Zwattendorfer, Marc Stern, and John Hepe [2011]. *D5.8.3b Interface Specification*. Technical Report, STORK Consortium.
- Alford, Ted [2009]. *The Economics of cloud computing*. Booz Allen Hamilton. <http://www.boozallen.com/media/file/Economics-of-Cloud-Computing.pdf>.
- Alpár, Gergely, Jaap-Henk Hoepman, and Johanneke Siljee [2011]. *The Identity Crisis. Security, Privacy and Usability Issues in Identity Management*. *arXiv:1101.0427*, pages 1–15.
- Alshehri, Mohammed and Steve Drew [2010]. *E-GOVERNMENT FUNDAMENTALS*. In *Proceedings of the IADIS International Conference on ICT, Society and Human Beings*, pages 35–42. 2001.
- Alshehri, Mohammed and Steve J. Drew [2011]. *E-government principles: implementation, advantages and challenges*. *International Journal of Electronic Business*, 9(3), page 255.
- Anchan, Divyangi and Mahmoud Pegah [2003]. *Regaining Single Sign-On Taming the Beast*. In *Proceedings of the 31st annual ACM SIGUCCS conference on User services - SIGUCCS '03*, pages 166–171. ACM Press, New York, New York, USA.
- Andersson, Thomas, Sören Bittins, Jörg Caumanns, Glenn Gran, Seda Guerses, Iannis Krontiris, Herbert Leitold, Lefteris Leontaridis, Pasi Lindholm, Kai Rannenberg, Arne Tauber, Sami Tikkala, Brendan Van Alsenoy, Christian Weber, Bernd Zwattendorfer, and Digital Identity [2011]. *The Individualised Digital Identity Model*. Technical Report, GLOBAL IDENTITY NETWORKING OF INDIVIDUALS (GINI-SA).
- Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia [2009]. *Above the Clouds: A Berkeley View of Cloud Computing*. Technical Report, UC Berkeley Reliable Adaptive Distributed Systems Laboratory (RAD Lab).
- Arora, Siddhartha [2008a]. *National e-ID card schemes: A European overview*. *Information Security Technical Report*, 13(2), pages 46–53.

- Arora, Siddhartha [2008b]. *Review and Analysis of Current and Future European e-ID Card Schemes*. Technical Report, Royal Holloway, University of London.
- AS Sertifitseerimiskeskus [2003]. *The Estonian ID Card and Digital Signature Concept*. http://www.epractice.eu/files/media/media_603.pdf.
- Ateniese, Giuseppe, Jan Camenisch, Marc Joye, and Gene Tsudik [2000]. *A Practical and Provably Secure Coalition-Resistant Group Signature Scheme*. In *Advances in Cryptology - CRYPTO 2000*, pages 255–270.
- Ateniese, Giuseppe, Daniel H Chou, Breno de Medeiros, and Gene Tsudik [2005]. *Sanitizable Signatures*. In *ESORICS 2005*, pages 159–177.
- Ateniese, Giuseppe, Kevin Fu, Matthew Green, and Susan Hohenberger [2006]. *Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage*. *ACM Transactions on Information and System Security*, 9(1), pages 1–30.
- Auffray, Par Christophe [2012]. *Cloud Andromède : Orange et Thales se félicitent et se disent prêts à démarrer*. <http://www.zdnet.fr/actualites/cloud-andromede-orange-et-thales-se-felicitent-et-se-disent-prets-a-demarrer-39770969.htm>.
- Australian Government [2011]. *CLOUD COMPUTING STRATEGIC DIRECTION PAPER*. http://www.finance.gov.au/e-government/strategy-and-governance/docs/final_cloud_computing_strategy_version_1.pdf.
- Austrian Ministry of Finance [2012]. *Verwaltungskosten senken für Bürger/innen und Unternehmen*. https://service.bmf.gv.at/BUDGET/budgets/2013/beilagen/Verwaltungskosten_senken_Beschluss_2013.pdf.
- Backhouse, James [2005]. *D4.1: Structured account of approaches interoperability*. Technical Report, FIDIS.
- Barker, William C. and Elaine Barker [2012]. *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*. Technical Report, NIST.
- Bartel, Mark, John Boyer, Barb Fox, Brian LaMacchia, and Ed Simon [2008]. *XML Signature Syntax and Processing (Second Edition)*. Technical Report, W3C. <http://www.w3.org/TR/xmlsig-core/>.
- Bauer, Matthias, Martin Meints, and Marit Hansen [2005]. *D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems*. Technical Report, FIDIS.
- Baun, C., M. Kunze, J. Nimis, and S. Tai [2011]. *Cloud Computing: Web-basierte dynamische IT-Services*. 2nd Edition. Springer, 1–177 pages.
- Berbecaru, Diana, Joaquín Alcalde-Moraño, Jorge López Hernández-Ardieta, Renato Portela, and Ricardo Ferreira [2011a]. *D5.8.3c Software Design for PEPS architecture*. Technical Report, STORK Consortium.
- Berbecaru, Diana, Eva Jorquera, Joaquin Alcalde Moraño, Renato Portela, Wolfgang Bauer, Bernd Zwatendorfer, Jan Eichholz, and Tim Schneider [2011b]. *D5.8.3a Software Architecture Design*. Technical Report, STORK Consortium.
- Berbecaru, Diana, Antonio Lioy, Marco Mezzalama, Giorgio Santiano, Enrico Venuto, and Marco Oreglia [2011c]. *Federating e-identities across Europe, or how to build cross-border e-services*. In *AICA 2011: Smart Tech and Smart Innovation conference*, pages 1–10.

- Berjon, Robin, Steve Faulkner, Travis Leithead, Erika Doyle Navara, Edward O'Connor, Silvia Pfeiffer, and Ian Hickson [2014]. *HTML5*. Technical Report, W3C. <http://www.w3.org/TR/html5/>.
- Bertino, Elisa and Kenji Takahashi [2011]. *Identity Management: Concepts, Technologies, and Systems*. Artech House, 1–198 pages.
- Bhisikar, Arvind [2011]. *G-Cloud: New Paradigm Shift for Online Public Services*. *International Journal of Computer Applications*, 22(8), pages 24–29.
- Birrell, Eleanor and Fred B. Schneider [2013]. *Federated Identity Management Systems: A Privacy-based Characterization*. *IEEE Security and Privacy*, 11(5), pages 36–48.
- Bjones, Ronny, Ioannis Krontiris, Pascal Paillier, and Kai Rannenberg [2014]. *Integrating Anonymous Credentials with eIDs for Privacy-respecting Online Authentication*. In *Privacy Technologies and Policy*, pages 111–124.
- Blum, Dan and Ramon Krikken [2010]. *Using Encryption to Protect Sensitive Data in Cloud Computing Environments*. Technical Report, burtonGROUP.
- Bohm, Nicholas and Stephen Mason [2010]. *Identity and its verification*. *Computer Law & Security Review*, 26(1), pages 43–51.
- Borcea-Pfitzmann, Katrin, Marit Hansen, Katja Liesebach, Andreas Pfitzmann, and Sandra Steinbrecher [2006]. *What user-controlled identity management should learn from communities*. *Information Security Technical Report*, 11(3), pages 119–128.
- Brands, Stefan A. [2000]. *Rethinking Public Key Infrastructures and Digital Certificates - Building in Privacy*. PhD Thesis, MIT.
- Brücher, Heide and Michael Gisler [2002]. *E-Government - von den Grundlagen zur Anwendung*. *HMD - Praxis der Wirtschaftsinformatik*, 39(226), pages 5–19.
- Bruegger, Bud P and Moritz-Christian Müller [2013]. *The eID-Terminology Work of FutureID*. In Hühnlein, Detlef and Heiko Roß nagel (Editors), *Open Identity Summit 2013*, pages 156–162. Gesellschaft für Informatik e.V. (GI).
- Bundesamt für Sicherheit in der Informationstechnik [2011]. *Sicherheitsempfehlungen für Cloud Computing Anbieter*. Technical Report, Bundesamt für Sicherheit in der Informationstechnik.
- Burr, William E., Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, and Emad A. Nabbus [2013]. *Electronic Authentication Guideline - NIST Special Publication 800-63-2*. Technical Report, National Institute of Standards and Technology (NIST).
- Buyya, Rajkumar, Rajiv Ranjan, and Rodrigo N Calheiros [2010]. *InterCloud : Utility-Oriented Federation of Cloud Computing Environments for Scaling of*. In *Algorithms and Architectures for Parallel Processing (10th International Conference, ICA3PP 20)*, pages 13–31. Springer.
- Camenisch, Jan and Anna Lysyanskaya [2001]. *An efficient system for non-transferable anonymous credentials with optional anonymity revocation*. In Pfitzmann, Birgit (Editor), *Advances in Cryptology - EUROCRYPT 2001*, pages 93–118. Springer Berlin Heidelberg.
- Camenisch, Jan and Anna Lysyanskaya [2003]. *A signature scheme with efficient protocols*. In *Security in communication networks*, pages 268–289.
- Cameron, K [2005a]. *The Laws of Identity*. Technical Report, Microsoft. <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>.

- Cameron, Kim [2005b]. *IdentityBlog - What is a digital identity?* <http://www.identityblog.com/?p=213>.
- Camp, L. Jean [2004]. *Digital identity*. *IEEE Technology and Society Magazine*, 23(3), pages 34–41.
- Campari, Fabio, Herbert Leitold, Manfred Pregartbauer, Thomas Rössler, Roberto Zuffada, and Bernd Zwattendorfer [2010]. *Report on Common Specifications for eHealth LSP*. Technical Report, STORK Consortium.
- Cantor, Scott, Frederick Hirsch, John Kemp, Rob Philpott, and Eve Maler [2009a]. *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0 - Errata Composite*. Technical Report, OASIS.
- Cantor, Scott, John Kemp, Rob Philpott, and Eve Maler [2009b]. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 - Errata Composite*. Technical Report, OASIS.
- Cao, Yuan and Lin Yang [2010]. *A survey of Identity Management technology*. In *2010 IEEE International Conference on Information Theory and Information Security*, pages 287–293. IEEE.
- Carter, Lemuria and France Bélanger [2005]. *The utilization of e-government services: citizen trust, innovation and acceptance factors*. *Information Systems Journal*, 15(1), pages 5–25.
- Catteddu, Daniele [2011]. *Security & Resilience in Governmental Clouds*. Technical Report, ENISA.
- Catteddu, Daniele and Giles Hogben [2009]. *Cloud Computing - Benefits, risks and recommendations for information security*. Technical Report, ENISA.
- CEN/ISSS Workshop on eAuthentication [2004]. *Towards an electronic ID for the European Citizen, a strategic vision*. <http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Documents/WI4vision1.doc>.
- CEN/TC 224 WG15 [2010]. *CEN/TS 15480 - Identification Card Systems - European Citizen Card - Part 3: European Citizen Card Interoperability using an application interface*. Technical Report, CEN.
- CEN/TC 224 WG15 [2012a]. *CEN/TS 15480 - Identification Card Systems - European Citizen Card - Part 1: Physical, electrical and transport protocol characteristics*. Technical Report, CEN.
- CEN/TC 224 WG15 [2012b]. *CEN/TS 15480 - Identification Card Systems - European Citizen Card - Part 2: Logical data structures and card services*. Technical Report, CEN.
- CEN/TC 224 WG15 [2012c]. *CEN/TS 15480 - Identification Card Systems - European Citizen Card - Part 4: Recommendations for European Citizen Card issuance, operation and use*. Technical Report, CEN.
- CEN/TC 224 WG15 [2013]. *CEN/TS 15480 - Identification Card Systems - European Citizen Card - Part 5: General Introduction*. Technical Report, CEN.
- Centner, Martin, Clemens Orthacker, and Wolfgang Bauer [2010]. *Minimal-footprint Middleware for the Creation of Qualified Signatures*. In *WEBIST 2010*, pages 64–69. INSTICC Press.
- Chadwick, David W. [2009]. *Federated Identity Management*. In Aldini, Alessandro, Gilles Barthe, and Roberto Gorrieri (Editors), *Foundations of Security Analysis and Design V*, pages 96–120. Springer Berlin Heidelberg.
- Chandrasekaran, Arun and Mayank Kapoor [2011]. *State of Cloud Computing in the Public Sector - A Strategic analysis of the business case and overview of initiatives across Asia Pacific*. Technical Report, Frost & Sullivan.

- Chen, Yao and Radu Sion [2010]. *On Securing Untrusted Clouds with Cryptography*. In *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, pages 109–114.
- Chow, Sherman S.M., Jian Weng, Yanjiang Yang, and Robert H. Deng [2010]. *Efficient Unidirectional Proxy Re-Encryption*. In *Progress in Cryptology - AFRICACRYPT 2010*, pages 316–332.
- Clarke, Roger [1994]. *Human Identification in Information Systems: Management Challenges and Public Policy Issues*. *Information Technology & People*, 7(4), pages 6–37.
- Clauß, Sebastian and Marit Köhntopp [2001]. *Identity management and its support of multilateral security*. *Computer Networks*, 37, pages 205–219.
- Clercq, Jan De [2002]. *Single sign-on architectures*. In *Proceedings of the International Conference on Infrastructure Security*, pages 40–58.
- Clercq, Jan De and Jason Rouault [2004]. *An Introduction to Identity Management*. Technical Report, HP.
- Cloud Security Alliance [2011]. *SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0*. Technical Report, Cloud Security Alliance.
- Cock, Danny De, Brendan Van Alsenoy, Bart Preneel, and Jos Dumortier [2011]. *The Belgian eID Approach*. In Fumy, Walter and Manfred Paeschke (Editors), *Handbook of eID Security - Concepts, Practical Experiences, Technologies*, pages 117–153. Publicis Publishing, Erlangen.
- Cock, Danny De, Christopher Wolf, and Bart Preneel [2006]. *The Belgian Electronic Identity Card (Overview)*. In *Sicherheit 2006*, pages 298–301. Sicherheit der Gesellschaft für Informatik. Bonner Köllen Verlag.
- Cock, Danny De, Karel Wouters, and Bart Preneel [2004]. *Introduction to the Belgian EID card*. In *EuroPKI*, pages 1–13. Springer-Verlag Berlin Heidelberg.
- Commission of the European Communities [2002]. *eEurope 2005: An information society for all*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0263:FIN:EN:PDF>.
- Commission of the European Communities [2005]. *i2010 - A European Information Society for growth and employment*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF>.
- Commission of the European Communities [2009a]. *Final Evaluation of the eEurope 2005 Action Plan and of the multiannual programme (2003-2006) for the monitoring of eEurope 2005 Action Plan, dissemination of good practices and the improvement of network and information security (MODINIS)*.
- Commission of the European Communities [2009b]. *Final evaluation of the implementation of the IDABC programme*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0247:FIN:EN:PDF>.
- Council of the European Union and Commission of the European Communities [2000]. *eEurope 2002 - An Information Society For All - Action Plan*.
- Cox, Philip [2012]. *How to Manage Identity in the Public Cloud*. *InformationWeek reports*. <http://reports.informationweek.com/cart/index/downloadlink/id/8691>.
- Curphey, Mark, David Endler, William Hau, Tim Smith, Alex Russell, Gene McKenna, Richard Parke, and Kevin McLaughlin [2002]. *A guide to building secure web applications*. Technical Report, The Open Web Application Security Project (OWASP).

- Dabrowski, Marcin and Piotr Pacyna [2008a]. *Generic and Complete Three-Level Identity Management Model*. In *Second International Conference on Emerging Security Information, Systems and Technologies*, pages 232–237. IEEE.
- Dabrowski, Marcin and Piotr Pacyna [2008b]. *Overview of Identity Management*. Technical Report, chinacommunications.cn.
- Danek, Jirka [2009]. *Cloud Computing and the Canadian Environment*. Technical Report, Public Works Government Services Canada Opportunity. <http://www.cloudbook.net/directories/gov-clouds/public-works-and-government-services-canada--pwgsc>.
- Datacentres.com [2011]. *TDC gets Danish Cloud Computing framework deal*. <http://www.datacentres.com/news/tdc-gets-danish-cloud-computing-framework-deal>.
- Datatilsynet [2011]. *Processing of sensitive personal data in a cloud solution*. <http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/>.
- de Andrade, Norberto Nuno Gomes, Shara Monteleone, and Aaron Martin [2013]. *Electronic Identity in Europe: Legal Challenges and Future Perspectives (e-ID 2020)*. Technical Report, European Commission - Joint Research Centre - Institute for Prospective Technological Studies Contact.
- De Cock, Danny [2006]. *Modinis Overview*. http://www.sevecom.org/Presentations/2006-06_Paris/Sevecom_2006-06-26_GModinis-IDM.pdf.
- Denning, Dorothy E. [1984]. *Digital Signatures with RSA and Other Public-Key Cryptosystems*. *Communications of the ACM*, 27(4), pages 388–392.
- Derler, Andreas [2013]. *Secure cloud storage using Citizen Card Encrypted*. Bachelor thesis, Graz University of Technology.
- Deussen, Peter, Linda Strick, and Johannes Peters [2010]. *Cloud-Computing für die öffentliche Verwaltung*. Technical Report, Fraunhofer.
- Dhamija, Rachna and Lisa Dusseault [2008]. *The Seven Flaws of Identity Management*. *IEEE Security and Privacy*, 6(2), pages 24–29.
- Digital ID World Magazine [2002]. *What is Digital Identity?*
- dos Santos, Ernani Marques and Nicolau Reinhard [2011]. *Electronic Government Interoperability: Identifying the Barriers for Frameworks Adoption*. *Social Science Computer Review*, 30(1), pages 71–82.
- E-Government Innovation Center (EGIZ) [2013]. *PDF Signatur/Amtssignatur Spezifikation*. Technical Report, E-Government Innovation Center (EGIZ).
- Ebrahim, Zakareya and Zahir Irani [2005]. *E-government adoption: architecture and barriers*. *Business Process Management Journal*, 11(5), pages 589–611.
- Eichholz, Jan, Adrian Johnston, Herbert Leitold, Marc Stern, John Heppel, Tim Schneider, and Bernd Zwattendorfer [2010]. *D5.1 - Evaluation and assessment of existing reference models and common specs*. Technical Report, STORK Consortium.
- Elbadawi, Ibrahim [2011]. *Cloud Computing for E-Government in UAE: Opportunities, Challenges and Service Models*. In *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance*, pages 1–2.

- Emig, Christian, Frank Brandt, Sebastian Kreuzer, and Sebastian Abeck [2007]. *Identity as a Service - Towards a Service-Oriented Identity Management Architecture*. In *Dependable and Adaptable Networks and Services*, pages 1–8.
- ENISA [2010]. *Security Issues in Cross-border Electronic Authentication*. Technical Report, European Union Agency for Network and Information Security.
- Epractice.eu [2009]. *DK: Public discussion in implementing cloud computing services in the Danish public sector — ePractice*. <http://www.epractice.eu/en/news/292790>.
- EpSOS [2008]. *epSOS: About epSOS*. <http://www.epsos.eu/home/about-epsos.html>.
- Europe - Summaries of EU legislation [2003]. *eEurope 2002*. http://europa.eu/legislation_summaries/information_society/strategies/124226a_en.htm.
- Europe - Summaries of EU legislation [2005]. *Electronic interchange of data between administrations: IDA programme*. http://europa.eu/legislation_summaries/information_society/strategies/124147a_en.htm.
- European Commission [2000]. *eEurope - An Information Society For All*. <http://aei.pitt.edu/3532/1/3532.pdf>.
- European Commission [2004]. *European Interoperability Framework for Pan-European eGovernment Services*. <http://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529>.
- European Commission [2005]. *Ministerial Declaration approved unanimously on 24 November 2005, Manchester, United Kingdom*. <http://www.unic.pt/images/stories/noticias/051124declaration.pdf>.
- European Commission [2006]. *A conceptual framework for European IDM systems*. Technical Report, Modinis.
- European Commission [2009]. *Ministerial Declaration on eGovernment approved unanimously in Malmö, Sweden, on 18 November 2009*. <http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf>.
- European Commission [2010a]. *A Digital Agenda for Europe*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF>.
- European Commission [2010b]. *EIS - European Interoperability Strategy*. <http://ec.europa.eu/idabc/en/document/7772.html>.
- European Commission [2010c]. *Europe 2020 - A strategy for smart, sustainable and inclusive growth*. <http://ec.europa.eu/eu2020/pdf/COMPLETENBARROSO007-Europe2020-ENversion.pdf>.
- European Commission [2010d]. *European Interoperability Framework (EIF) for European public services*. http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf.
- European Commission [2010e]. *European Interoperability Strategy (EIS) for European public services*. http://ec.europa.eu/isa/documents/isa_annex_i_eis_en.pdf.
- European Commission [2010f]. *The European eGovernment Action Plan 2011-2015 - Harnessing ICT to promote smart, sustainable & innovative Government*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:EN:PDF>.

- European Commission [2011]. *The ISA programme - Overcoming eBarriers to European public services*. http://ec.europa.eu/isa/documents/isa_programme.pdf.
- European Commission [2012a]. *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of cri*. [http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0010/COM_COM\(2012\)0010_EN.pdf](http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0010/COM_COM(2012)0010_EN.pdf).
- European Commission [2012b]. *Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:PDF>.
- European Commission [2012c]. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
- European Council [2000a]. *Presidency Conclusions - Lisbon European Council*. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/00100-r1.en0.htm.
- European Council [2000b]. *Presidency Conclusions - Santa Maria da Feira European Council*. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/00200-r1.en0.htm.
- European Parliament and Council [1995]. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:pdf>.
- European Parliament and Council [1999a]. *DECISION No 1720/1999/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 1999 adopting a series of actions and measures in order to ensure interoperability of and access to trans-European networks for the electronic interchange of data between ad*. *Official Journal of the European Communities*, 203, pages 9–13. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1999:203:0009:0013:EN:PDF>.
- European Parliament and Council [1999b]. *DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures*. *Official Journal of the European Communities*, pages 1–9. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML>.
- European Parliament and Council [2004]. *DECISION 2004/387/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC)*. *Official Journal of the European Communitiesal Journal of the European*, 181, pages 25–35. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_181/l_18120040518en00250035.pdf.
- European Parliament and Council [2006]. *DIRECTIVE 2006/123/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2006 on services in the internal market THE*. *Official Journal of the European Union*, 376, pages 36–68. <http://www.djei.ie/trade/marketaccess/singlemarket/07serv005.pdf>.

- European Parliament and Council [2009]. *DECISION No 922/2009/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 September 2009 on interoperability solutions for European public administrations (ISA)*. *Official Journal of the European Union*, 260, pages 20–27. http://ec.europa.eu/isa/documents/isa_lexuriserv_en.pdf.
- European Parliament and Council [2012]. *REGULATION (EU) No 260/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009*. *Official Journal of the European Union*, 94, pages 22–37. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:094:0022:0037:EN:PDF>.
- Eurosmart [2008]. *Position Paper - European Citizen Card : One Pillar of Interoperable eID Success*. <https://www.eid-stork.eu/dmdocuments/public/ecc-position-paper-final.pdf>.
- Fang, Zhiyuan [2002]. *E-government in digital era: concept, practice, and development*. *International Journal of The Computer, The Internet and Management*, 10(2), pages 1–22.
- Fatema, Kaniz, Philip D. Healy, Vincent C. Emeakaroha, John P. Morrison, and Theo Lynn [2014]. *A User Data Location Control Model for Cloud Services*. In *4th International Conference on Cloud Computing and Services Science, CLOSER 2014*, pages 476–488.
- Federal Chancellery [2008]. *The Austrian E-Government Act*. *Austrian Federal Law Gazette I*, 7, pages 1–11. <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230>.
- Federal Chancellery [2010a]. *E-Government Equivalence Decree*. *Austrian Federal Law Gazette (BGBl)*, 170, page 1. <http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006801>.
- Federal Chancellery [2010b]. *General Administrative Procedure Act 1991 - AVG*. *Austrian Federal Law Gazette I*, 100, pages 1–49. https://www.ris.bka.gv.at/Dokumente/ErV/ERV_1991_51/ERV_1991_51.pdf.
- Federal Chancellery [2010c]. *Signature Act*. *Austrian Federal Law Gazette I*, 75, pages 1–13. <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10003685>.
- Federal Chancellery [2010d]. *Verordnung des Bundeskanzlers, mit der die Voraussetzungen der Gleichwertigkeit gemäß § 6 Abs. 5 des E-Government-Gesetzes festgelegt werden (E-Government-Gleichwertigkeitsverordnung) StF: BGBl. II Nr. 170/2010*. <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006801>.
- Federal Chancellery [2013]. *Federal Act on the Service of Official Documents (Service of Documents Act)*. *Austrian Federal Law Gazette I*, 33, pages 1–21. http://www.ris.bka.gv.at/Dokumente/ErV/ERV_1982_200/ERV_1982_200.pdf.
- Federal Ministry of Economics and Technology (BMWi) [2010]. *ICT Strategy of the German Federal Government: Digital Germany 2015*. Technical Report, Federal Ministry of Economics and Technology (BMWi). <http://www.bmwi.de/English/Redaktion/Pdf/ict-strategy-digital-germany-2015,property%3Dpdf>.
- Federal Ministry of Health [2013]. *Die e-card*. https://www.gesundheit.gv.at/Portal.Node/ghp/public/content/Die_e_card_HK.html.

- Ferdous, Md. Sadek and Ron Poet [2012]. *A comparative analysis of Identity Management Systems*. In *2012 International Conference on High Performance Computing & Simulation (HPCS)*, pages 454–461. IEEE.
- FIDIS [2004]. *About FIDIS*. <http://www.fidis.net/about/>.
- Frelle-Petersen, Lars, Timo Valli, Gudbjörg Sigurdardóttir, Katarina de Brisis, and Magnus Enzell [2011]. *Nordic Public Sector Cloud Computing - a discussion paper*. Technical Report, Nordon. http://www.norden.org/en/publications/publikationer/2011-566/at_download/publicationfile.
- Fromm, Jens and Petra Hoepner [2011]. *The New German eID Card*. In Fumy, Walter and Manfred Paeschke (Editors), *Handbook of eID Security - Concepts, Practical Experiences, Technologies*, pages 154–166. Publicis Publishing, Erlangen.
- Fumy, Walter and Manfred Paeschke [2011]. *Challenges in eID Security*. In Fumy, Walter and Manfred Paeschke (Editors), *Handbook of eID Security - Concepts, Practical Experiences, Technologies*, pages 14–22. Publicis Publishing, Erlangen.
- Furht, Borko and Armando Escalante (Editors) [2010]. *Handbook of Cloud Computing*. Springer New York Dordrecht Heidelberg London, 1–655 pages.
- Gallagher, Patrick [2012]. *FIPS PUB 180-4: Secure Hash Standard (SHS)*. Technical Report, National Institute of Standards and Technology (NIST).
- Gentili, Mario [2001]. *Italian Electronic Identity Card-principle and architecture*. In *Proceedings of the 27th VLDB*, pages 629–632.
- Gentry, Craig [2009]. *Fully Homomorphic Encryption Using Ideal Lattices*. In *STOC '09 Proceedings of the forty-first annual ACM symposium on Theory of Computing*, pages 169–178.
- Gentry, Craig, Shai Halevi, and Nigel P Smart [2012]. *Homomorphic Evaluation of the AES Circuit*. In *Advances in Cryptology - CRYPTO 2012*, pages 850–867.
- Glade, Britta [2009]. *Identity Assurance Framework: Assurance Levels*. Technical Report, Kantara Initiative.
- Goldkuhl, Göran [2008]. *The challenges of Interoperability in E-government: Towards a conceptual refinement*. *Proceedings pre-ICIS 2008 SIG eGovernment Workshop*, pages 1–6.
- Gongolidis, Evangelos, Christos Kalloniatas, and Evangelia Kavakli [2014]. *Requirements Identification for Migrating eGovernment Applications to the Cloud*. In *ICT-EurAsia 2014*, pages 150–158.
- Goodner, Marc and Anthony Nadalin [2009]. *Web Services Federation Language (WS-Federation) Version 1.2*. Technical Report, OASIS.
- Gopalakrishnan, Anu [2009]. *Cloud Computing Identity Management*. *SETLabs Briefings*, 7(7), pages 45–55.
- Górniak, Slawomir, John Elliott, Margaret Ford, Dave Birch, Rodica Tirtea, and Demosthenes Ikonomou [2011]. *Managing multiple electronic identities*. Technical Report, ENISA.
- Gorniak, Slawomir, Demosthenes Ikonomou, Panagiotis Saragiotis, Ioannis Askoxylakis, Petros Belimpasakis, Boldizar Bencsath, Matt Broda, Levente Buttyan, Gary Clemo, Piotr Kijewski, Alain Merle, Katerina Mitrokotsa, Alistair Munro, Oliver Popov, Christian W. Probst, Luigi Romano, Christos Siaterlis, Vasilios Siris, Ingrid Verbauwhede, and Claire Vishik [2010]. *Priorities for Research on Current and Emerging Network Technologies*. Technical Report, ENISA.

- Gottschalk, Petter and Hans Solli-Sæther [2009]. *Interoperability in E-Government: Stages of Growth*. In Chhabra, Susheel and Muneesh Kumar (Editors), *Integrating E-Business Models for Government Solutions: Citizen-Centric Service Oriented Methodologies and Processes*, pages 50–66. IGI Global.
- Goulding, J Tony [2010]. *identity and access management for the cloud: CA's strategy and vision*. Technical Report May, CA Technologies. http://www.ca.com/~/media/Files/whitepapers/iam_cloud_security_vision_wp_236732.pdf.
- Government Information Technology Services Board [1997]. *Access America: Reengineering Through Information Technology*. <http://govinfo.library.unt.edu/npr/library/announc/access/acessrpt.html>.
- Graux, Hans [2012]. *D.3.2 - QAA Status Report*. Technical Report, STORK 2.0 Consortium.
- Graux, Hans and Jos Dumortier [2009]. *Report on the state of pan-European eIDM initiatives*. Technical Report, ENISA.
- Graux, Hans and Jarkko Majava [2007]. *Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms*. Technical Report, IDABC.
- Graux, Hans, Jarkko Majava, and Eric Meyvis [2009a]. *eID Interoperability for PEGS: Update of Country Profiles study - Belgian country profile*. Technical Report, IDABC.
- Graux, Hans, Jarkko Majava, and Eric Meyvis [2009b]. *eID Interoperability for PEGS: Update of Country Profiles study - Estonian country profile*. Technical Report, IDABC.
- Graux, Hans, Jarkko Majava, and Eric Meyvis [2009c]. *Study on eID Interoperability for PEGS: Update of Country Profiles - Analysis & assessment report*. Technical Report, IDABC.
- Graux, Hans, Jarkko Majava, and Eric Meyvis [2009d]. *Study on eID Interoperability for PEGS: Update of Country Profiles - Memorandum of Understanding*. Technical Report December, IDABC.
- Green, Matthew and Giuseppe Ateniese [2007]. *Identity-Based Proxy Re-encryption*. In *Applied Cryptography and Network Security*, pages 288–306.
- Gronau, Norbert, Moreen Stein, Tanja Röchert-Voigt, Niels Proske, and Edzard Weber [2010]. *E-Government Anwendungen - Ein aktueller Überblick*. GITO-Verlag (Berlin), 264 pages.
- Guo, Xinghui [2011]. *Singapore govt to set up private cloud*. <http://www.futuregov.asia/articles/2011/jul/05/singapore-set-g-cloud/>.
- Gutierrez, Abraham and Ana Piñuela [2009]. *STORK Glossary and Acronyms*. Technical Report, STORK Consortium.
- Hallam-Baker, Phillip and Eve Maler [2002]. *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)*. Technical Report November, OASIS.
- Hammer-Lahav, E. [2010]. *RFC 5849 - The OAuth 1.0 Protocol*. Technical Report, Internet Engineering Task Force (IETF).
- Hansen, Marit, Andreas Pfitzmann, and Sandra Steinbrecher [2008]. *Identity management throughout one's whole life*. *Information Security Technical Report*, 13(2), pages 83–94.
- Hardjono, Thomas, Nate Klingenstein, and Scott Cantor [2012]. *SAML Version 2.0 Errata 05*. Technical Report May, OASIS. <http://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.pdf>.

- Hardt, D. [2012]. *RFC 6749 - The OAuth 2.0 Authorization Framework*. Technical Report, Internet Engineering Task Force (IETF).
- Harms, Rolf and Michael Yamartino [2010]. *THE ECONOMICS OF THE CLOUD FOR THE EU PUBLIC SECTOR*. Technical Report, Microsoft. http://www.microsoft.com/global/eu/RichMedia/eu_public_sector_cloud_economics_a4.pdf.
- Hayat, Amir [2007]. *A Pan European Interoperable Electronic Identity Management System*. PhD Thesis, Graz University of Technology.
- Hayat, Amir, Herbert Leitold, Christian Rechberger, and Thoms Rössler [2004]. *Survey on EU's Electronic-ID Solutions*. Technical Report, Secure Information Technology Center - Austria (A-SIT).
- Heck, Uwe and Willy Müller [2010]. *Vorstudie zu Cloud Computing in Schweizer Behörden*. Technical Report, Informatiksteuerungsorgan des Bundes (ISB).
- Heindl, Patricia [2003]. *Elektronische Demokratie - "Dienstleistungen" des Staates E-Voting, E-Legislation, E-participation*. In Prosser, Alexander and Robert Krimmer (Editors), *e-Democracy: Technologie, Recht und Politik*, pages 175–187. Oesterreichische Computer Gesellschaft.
- Helmbrecht, Udo [2010]. *Data protection and legal compliance in cloud computing*. *Datenschutz und Datensicherheit - DuD*, 34(8), pages 554–556.
- Helmbrecht, Udo and Ingo Naumann [2011]. *Overview of European Electronic Identity Cards*. In Fumy, Walter and Manfred Paeschke (Editors), *Handbook of eID Security - Concepts, Practical Experiences, Technologies*, pages 107–116. Publicis Publishing, Erlangen.
- Heron, Mike [2000]. *Q&A: Balancing the role of e-government*. <http://edition.cnn.com/2000/TECH/computing/11/13/qna.egov.idg/>.
- Hicks, Robin [2009]. *Thailand hatches plan for private cloud*. <http://www.futuregov.asia/articles/2009/may/25/thailand-plans-private-cloud-e-gov/>.
- Hollosi, Arno and Rainer Hörbe [2007]. *Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK)*. Technical Report, AG Bürgerkarte.
- Hollosi, Arno, Gregor Karlinger, Thomas Rössler, and Martin Centner [2014]. *Die österreichische Bürgerkarte*. <http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20140114/>.
- Hornung, Gerrit and Alexander Roßnagel [2010]. *An ID card for the Internet - The new German ID card with "electronic proof of identity"*. *Computer Law & Security Review*, 26(2), pages 151–157.
- Housley, R. [1999]. *RFC 5652 - Cryptographic message syntax (CMS)*. Technical Report, Internet Engineering Task Force (IETF).
- Huang, He Yuan, Bin Wang, Xiao Xi Liu, and Jing Min Xu [2010]. *Identity Federation Broker for Service Cloud*. *2010 International Conference on Service Sciences*, pages 115–120.
- Hughes, John, Scott Cantor, Jeff Hodges, Frederick Hirsch, Prateek Mishra, Rob Philpott, and Eve Maler [2009]. *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 - Errata Composite*. Technical Report, OASIS.
- Hühnlein, Detlef, Jörg Schwenk, Tobias Wich, Vladislav Mladenov, Florian Feldmann, Andreas Mayer, Johannes Schmölz, Bud Bruegger, and Moritz Horsch [2013]. *Options for integrating eID and SAML*. *Proceedings of the 2013 ACM workshop on Digital Identity Management - DIM '13*, pages 85–96.

- Hulsebosch, B., G. Lenzi, and H. Eertink [2009]. *D2.3 - Quality authenticator scheme*. Technical Report, STORK Consortium.
- Hurch, Martin and Gottfried Heider [2010]. *Deliverable: D3.6.2 Final identity management specification definition*. Technical Report, epSOS Consortium.
- IDABC [2009]. *The Programme*. <http://ec.europa.eu/idabc/en/chapter/3.html>.
- IDABC eGovernment Observatory [2006]. *eGovernment in the Member States of the European Union*. Technical Report, European Communities.
- Imamura, Takeshi, Blair Dillaway, and Ed Simon [2002]. *XML encryption syntax and processing*. Technical Report, W3C. <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>.
- Ingthorsson, Olafur [2010]. *How HTML5 advances Mobile Cloud Computing!* <http://cctooffice.com/2010/09/how-html5-advances-mobile-cloud-computing/>.
- Irish Government [2009]. *Technology Actions to Support the Smart Economy*. <http://www.dcenr.gov.ie/nr/rdonlyres/26c23436-e6b3-4842-95b3-20bd2af104d6/0/finalversiontechnologyactionsreportfinal210709.doc>.
- ISO/IEC JTC 1 [2011]. *ISO/IEC 24760-1: Terminology and concepts*. Technical Report, ISO/IEC.
- ISO/IEC JTC 1 [2012]. *ISO/IEC 29115 - Information technology - Security techniques - Entity authentication assurance framework*. Technical Report, ISO/IEC.
- Ivkovic, Mario and Manuel Preiteiro [2010]. *STORK Work Item 3.2.3 European Citizen Card*. Technical Report, STORK.
- Ivkovic, Mario and Klaus Stranacher [2010]. *Foreign Identities in the Austrian E-Government*. In *Policies and Research in Identity Management*, pages 31–40. Springer Berlin Heidelberg.
- Ivkovic, Mario and Bernd Zwattendorfer [2009]. *STORK Work Item 3.2.1 SAML*. Technical Report, STORK Consortium.
- Jain, Anil K., Arun A. Ross, and Karthik Nandakumar [2011]. *Introduction to biometrics*. Springer New York Dordrecht Heidelberg London, 1–328 pages.
- Jø sang, Audun, Muhammed Al Zomai, and Suriadi Suriadi [2007]. *Usability and privacy in identity management architectures*. In Brankovic, Ljiljana, Paul Coddington, John F. Roddick, Chris Steketee, James R. Warren, and Andrew Wendelborn (Editors), *ACSW '07 Proceedings of the fifth Australasian symposium on ACSW frontiers*, pages 143–152. Australian Computer Society, Inc. Darlinghurst, Australia.
- Jø sang, Audun, John Fabre, Brian Hay, James Dalziel, and Simon Pope [2005]. *Trust requirements in identity management*. *Proceedings of the 2005 Australasian workshop on Grid computing and e-research*, pages 99–108.
- Jø sang, Audun and Simon Pope [2005]. *User centric identity management*. In *AusCERT Asia Pacific Information Technology*, pages 1–13.
- Johnson, Don B. and Alfred J. Menezes [1998]. *Elliptic curve DSA (ECDSA): an enhanced DSA*. In *Proceeding SSYM'98 Proceedings of the 7th conference on USENIX Security Symposium*, pages 13–24.
- Johnson, Robert, David Molnar, Dawn Song, and David Wagner [2002]. *Homomorphic Signature Schemes*. In *Topics in Cryptology - CT-RSA 2002*, volume 28913, pages 244–262.

- Kaliski, Burt Jr. [2011]. *RSA Digital Signature Scheme*. In van Tilborg, Henk C. A. and Sushil Jajodia (Editors), *Encyclopedia of Cryptography and Security*, pages 1061–1064. Springer US.
- Keersebilck, Philip and Bert Dufraimont [2008]. *Belgian e-government Application: the eID Card*. In *9th International Conference on Development and Application Systems*, pages 196–199.
- Kessler, Gary C. [1997]. *PASSWORDS - STRENGTHS AND WEAKNESSES*. In Cavanagh, J.P. (Editor), *Internet and Internetworking Security*. January 1996, Auerbach.
- Kissel, Brian [2009]. *OpenID 2009 Year in Review*. <http://openid.net/2009/12/16/openid-2009-year-in-review/>.
- Knall, Thomas, Arne Tauber, and Thomas Zefferer [2011]. *Secure and Privacy-Preserving Cross-Border Authentication: The STORK Pilot 'SaferChat'*. In *Proceedings of the Conference on Electronic Government and the Information Systems Perspective (EGOVIS 2011)*, pages 94–106.
- Kolitsi, Zoi and Petra Wilson [2010]. *D2.1.2 Legal and Regulatory Constraints on epSOS Design - Participating Member States*. Technical Report, epSOS Consortium.
- Koper, Rob [2008]. *Open source and open standards*. In Spector, J. Michael, M. David Merrill, Jeroen van Merriënboer, and Marcy P. Driscoll (Editors), *Handbook of Research on Educational Communications and Technology*, 3rd Edition, pages 355–366. 1, Taylor & Francis.
- Körting, Stephan and Diana Ombelli [2011]. *Mapping security services to authentication levels*. Technical Report, ENISA.
- Kouloulias, V., A. Kountzeris, H. Leitold, B. Zwattendorfer, A. Crespo, and M. Stern [2011]. *STORK e-Privacy and Security*. *5th International Conference on Network and System Security*, pages 234–238.
- KPMG [2012]. *Exploring the Cloud*. Technical Report, KPMG. <http://images.forbes.com/forbesinsights/StudyPDFs/exploring-cloud.pdf>.
- Krontiris, Ioannis, Herbert Leitold, Reinhard Posch, and Kai Rannenberg [2011]. *eID Interoperability*. In Fumy, Walter and Manfred Paeschke (Editors), *Handbook of eID Security - Concepts, Practical Experiences, Technologies*, pages 167–186. Publicis Publishing, Erlangen.
- Kundra, Vivek [2011]. *Federal Cloud Computing Strategy*. Technical Report, The White House Washington. www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf.
- Lapon, Jorn, Markulf Kohlweiss, Bart De Decker, and Vincent Naessens [2011]. *Analysis of Revocation Strategies for Anonymous Idemix Credentials*. In *Communications and Multimedia Security*, pages 3–17.
- Lathrop, Daniel and Laurel R T Ruma [2010]. *Open Government. Transparency, Collaboration and Participation in Practice*. O'Reilly Media, 432 pages.
- Lawrence, Kelvin, Chris Kaler, Anthony Nadalin, Ronald Monzillo, and Phillip Hallam-Baker [2006]. *Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)*. Technical Report, OASIS.
- Layne, Karen and Jungwoo Lee [2001]. *Developing fully functional E-government: A four stage model*. *Government Information Quarterly*, 18(2), pages 122–136.
- Leitold, Herbert [2011]. *Challenges of eID Interoperability: The STORK Project*. In *Privacy and Identity Management for Life*, volume 6, pages 144–150.
- Leitold, Herbert, A. Hollosi, and Reinhard Posch [2002]. *Security architecture of the Austrian citizen card concept*. In *Proceedings of the 18th Annual Computer Security Applications Conference*, pages 391–400.

- Leitold, Herbert, Thomas Zefferer, Bernd Zwattendorfer, Manfred Pregartbauer, Robert Scharinger, Fabio Campari, and Roberto Zuffada [2011]. *D7.11 - Implementation Report on eHealth LSP*. Technical Report, STORK Consortium.
- Leitold, Herbert and Bernd Zwattendorfer [2011]. *STORK: Architecture, Implementation and Pilots*. In *ISSE 2010 Securing Electronic Business Processes*, pages 1–11.
- Lenz, Thomas, Bernd Zwattendorfer, Klaus Stranacher, and Arne Tauber [2014]. *Identitätsmanagement in Österreich mit MOA-ID 2.0*. *eGovernment Review*, 13, pages 20–21.
- Lenz, Thomas, Bernd Zwattendorfer, and Arne Tauber [2013]. *A Secure and Confidential Javascript Crypto-Framework for Cloud Storage Applications*. In *IADIS International Conference WWW/INTERNET*, pages 219–226.
- Linden, Mikael and Inka Vilpola [2005]. *An empirical study on the usability of logout in a single sign-on system*. In *Information Security Practice and Experience*, pages 243–254.
- Linn, John, Sharon Boeyen, Gary Ellison, Niina Karhuluoma, William Macgregor, Paul Madsen, Senthil Sengodan, Serge Shinkar, and Peter Thompson [2004]. *Trust Models Guidelines*. Technical Report, OASIS.
- Lockhart, Hal, Brian Campbell, Nick Ragouzis, John Hughes, Rob Philpott, Eve Maler, Paul Madsen, and Tom Scavo [2008]. *Security Assertion Markup Language (SAML) V2.0 Technical Overview*. Technical Report, OASIS.
- Lockhart, Hal and Thomas Hardjono [2010]. *SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0*. Technical Report, OASIS.
- Lörincz, Barbara, Dinand Tinholt, Niels van der Linden, Graham Colclough, Jonathan Cave, Rebecca Schindler, Gabriella Cattaneo, Rosanna Lifonti, Laurent Jacquet, and Jeremy Millard [2010]. *Digitizing Public Services in Europe: Putting ambition into action*. Technical Report, Capgemini, IDC, Rand Europe, Sogeti and DTi.
- Madsen, Paul, Eve Maler, Thomas Wisniewski, Tony Nadalin, Scott Cantor, Jeff Hodges, and Prateek Mishra [2005]. *SAML V2.0 Executive Overview*. Technical Report, OASIS.
- Majava, Jarkko, Eric Meyvis, and Hans Graux [2009]. *Study on eID Interoperability for PEGS: Update of Country Profiles - Quick Wins*. Technical Report, IDABC.
- Maler, Eve, Prateek Mishra, and Rob Philpott [2003]. *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1*. Technical Report, OASIS.
- Margraf, Marian [2010]. *The New German ID Card*. In Pohlmann, Norbert, Helmut Reimer, and Wolfgang Schneider (Editors), *ISSE 2010 Securing Electronic Business Processes*, pages 367–373. Vieweg+Teubner.
- Marketsandmarkets.com [2010]. *Cloud Computing Market: Global Forecast (2010 - 2015)*. <http://www.marketsandmarkets.com/Market-Reports/cloud-computing-234.html>.
- Martens, Tarvi [2010]. *Electronic identity management in Estonia between market and state governance*. *Identity in the Information Society*, 3(1), pages 213–233.
- Mazure, Drew, Susan Bramhall, Howard Gilbert, Andy Newman, and Andrew Petro [2005]. *CAS Protocol*. Technical Report, JASIG. <http://www.jasig.org/cas/protocol>.
- Meints, Martin and Marit Hansen [2006]. *D3.6 Study on ID Documents*. Technical Report, FIDIS.

- Mell, Peter and Timothy Grance [2010]. *The NIST definition of cloud computing*. Technical Report, National Institute of Standards and Technology.
- Meyer, Matthias, Rüdiger Zarnekow, and Lutz M. Kolbe [2003]. *IT-Governance Begriff, Status quo und Bedeutung*. *WIRTSCHAFTSINFORMATIK*, 45(4), pages 445–448.
- Millard, Jeremy [2011]. *2020 Vision: Eight megatrends in e-government for the next eight years*. <http://www.slideshare.net/smartcities/eight-mega-trends-in-egovernment-for-the-next-eight-years>.
- Mishra, Prateek, Phillip Hallam-Baker, Zahid Ahmed, Alex Ceponkus, Marc Chanliau, Jeremy Epstein, Chris Ferris, David Jablon, Eve Maler, and David Orchard [2001]. *Security Services Markup Language*.
- Mishra, Prateek, Krishna Sankar, Simon Godik, Tim Moses, Scott Cantor, Robert Philpott, Evan Prodromou, Chris Ferris, Jeff Hodges, Eve Maler, Bob Blakley, Marlena Erdos, and RL Morgan [2002]. *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)*. Technical Report, OASIS.
- Misuraca, Gianluca, Giuseppe Alfano, and Gianluigi Viscusi [2011]. *Interoperability Challenges for ICT-enabled Governance: Towards a pan-European Conceptual Framework*. *Journal of theoretical and applied electronic commerce research*, 6(1), pages 95–111.
- Modinis [2005]. *Common Terminological Framework for Interoperable Electronic Identity Management*. Technical Report, European Commission.
- Moon, M. Jae [2002]. *The Evolution of E-Government among Municipalities: Rhetoric or Reality?* *Public Administration Review*, 62(4), pages 424–433.
- Müller, Horst [2004]. *eGovernment 2004 Zeit zum Paradigmenwechsel*. Technical Report, MÜLLER + FORTMÜHLER.
- Müller, Thomas [2008]. *Trusted Computing Systeme*. Springer-Verlag Berlin Heidelberg.
- Myhr, Thomas [2005]. *Regulating a European eID - A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID*. Technical Report, Porvoo e-ID Group.
- Myhr, Thomas [2008]. *Legal and organizational challenges and solutions for achieving a pan-European electronic ID solution*. *Information Security Technical Report*, 13(2), pages 76–82.
- National Science and Technology Council (NSTC) [2008]. *Identity Management Task Force Report 2008*. Technical Report, National Science and Technology Council (NSTC) - Subcommittee on Biometrics and Identity Management.
- Naumann, Ingo and Giles Hogben [2008]. *Privacy features of European eid card specifications*. *Network Security*, 2008(8), pages 9–13.
- Naumann, Ingo and Giles Hogben [2009]. *Privacy Features of European eid Card Specifications*. Technical Report, ENISA.
- Neuman, C, T. Yu, S. Hartman, and K Raeburn [2005]. *RFC 4120: The Kerberos network authentication service (V5)*. Technical Report, Network Working Group.
- Next-generation Networks [2009]. *Recommendation ITU-T Y.2720 - NGN identity management framework*. Technical Report, International Telecommunication Union (ITU-T).

- Ng, Kelly [2009]. *Japan govt plots private cloud*. <http://www.futuregov.asia/articles/2009/may/18/japan-govt-plots-private-cloud/>.
- Nuñez, David and Isaac Agudo [2014]. *BlindIdM: A privacy-preserving approach for identity management as a service*. *International Journal of Information Security*, pages 1–17.
- Nuñez, David, Isaac Agudo, and Javier Lopez [2013]. *Leveraging Privacy in Identity Management as a Service through Proxy Re-Encryption*. In Zimmermann, Wolf (Editor), *Proceedings of the PhD Symposium at the 2nd European Conference on Service-Oriented and Cloud Computing*, pages 42–47.
- Nunez, David, Isaac Agudo, and Javier Lopez [2012]. *Integrating OpenID with proxy re-encryption to enhance privacy in cloud-based identity services*. In *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, pages 241–248. IEEE.
- OpenID Foundation [2007]. *OpenID Authentication 2.0 - Final*. http://openid.net/specs/openid-authentication-2_0.html.
- Orthacker, Clemens, Martin Centner, and Christian Kittl [2010]. *Qualified mobile server signature*. In *Security and Privacy - Silver Linings in the Cloud*, pages 103–111.
- Oxford Dictionaries [2014]. *identity*. <http://www.oxforddictionaries.com/definition/english/identity>.
- Paal, Stefan, Reiner Kammüller, and Bernd Freisleben [2003]. *Separating the Concerns of Distributed Deployment and Dynamic Composition in Internet Application Systems*. In *On the move to meaningful internet systems*, pages 1292–1311.
- Palfrey, John and Urs Gasser [2007]. *Digital Identity Interoperability and eInnovation*. *Berkman Publication Series*, pages 1–49.
- Pallis, George [2010]. *Cloud computing: The New Frontier of Internet Computing*. *IEEE Internet Computing*, 14(5), pages 70–73.
- Paquette, Scott, Paul T. Jaeger, and Susan C. Wilson [2010]. *Identifying the security risks associated with governmental use of cloud computing*. *Government Information Quarterly*, 27(3), pages 245–253.
- Pardo, Theresa A., Taewoo Nam, and G. Brian Burke [2011]. *E-Government Interoperability: Interaction of Policy, Management, and Technology Dimensions*. *Social Science Computer Review*, 30(1), pages 7–23.
- Parrilli, Davide M. [2012]. *D.3.3 - Mandate/Attribute Management Report*. Technical Report, STORK 2.0 Consortium.
- Parrilli, Davide M. and Hans Graux [2012]. *D.3.5 - Legal Entities Identification Report*. Technical Report, STORK 2.0 Consortium.
- Parycek, Peter, Johann Höchtel, Sylvia Purgathofer-Müller, and Johannes Weindl [2011]. *Kosten- & Entscheidungsmodelle für Cloud Computing in der öffentlichen Verwaltung*. Technical Report, Donau-Universität Krems.
- Pashalidis, Andreas and CJ Mitchell [2003]. *A taxonomy of single sign-on systems*. In *Information security and privacy - Proceedings of the 8th Australasian Conference, ACISP 2003*, pages 249–264.
- Pearson, Siani and Azzedine Benameur [2010]. *Privacy, Security and Trust Issues Arising from Cloud Computing*. In *IEEE Second International Conference on Cloud Computing Technology and Science*, pages 693–702. IEEE.

- Pearson, Siani and Marco Casassa Mont [2011]. *Sticky Policies: An Approach for Managing Privacy Parties*. *Computer*, 44(9), pages 60 – 68.
- Pérez San-José, Pablo, Susana de la Fuente Rodríguez, Laura García Pérez, Cristina Gutiérrez Borge, and Eduardo Álvarez Alonso [2012]. *Study on cloud computing in the Spanish public sector*. Technical Report, National Institute of Communication Technologies (INTECO).
- Pfitzmann, Andreas and Marit Hansen [2010]. *A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management*. Technical Report, TU Dresden.
- Pfitzmann, Andreas and M Köhntopp [2001]. *Anonymity, unobservability, and pseudonymity - a proposal for terminology*. In *Designing privacy enhancing technologies*, pages 1–9.
- Plattform Digital Austria [2008]. *Administration on the Net - The ABC guide of eGovernment in Austria New*. Technical Report, Plattform Digital Austria.
- Plattform Digital Austria [2014a]. *Digitale Agenda für Europa*. <http://www.digitales.oesterreich.gv.at/site/7436/default.aspx>.
- Plattform Digital Austria [2014b]. *eSENS*. <http://www.digitales.oesterreich.gv.at/site/6684/default.aspx#a6>.
- Poetzsch, Stefanie, Martin Meints, Bart Priem, Ronald Leenes, and Ranis Husseiki [2009]. *D3.12: Federated identity management - what's in it for the citizen/customer?* Technical Report, FIDIS.
- Pointcheval, David [2011]. *RSA Public-Key Encryption*. In van Tilborg, Henk C. A. and Sushil Jajodia (Editors), *Encyclopedia of Cryptography and Security*, pages 1069–1072. Springer US.
- Poller, Andreas, Ulrich Waldmann, Sven Vowe, and Sven Türpe [2012]. *Electronic Identity Cards for User Authentication - Promise and Practice*. *IEEE Security & Privacy*, 10(1), pages 46–54.
- Posch, Karl-Christian, Reinhard Posch, Arne Tauber, Thomas Zefferer, and Bernd Zwattendorfer [2011]. *Secure and Privacy-Preserving eGovernment - Best Practice Austria*. In *Rainbow of Computer Science*, pages 259–269. Springer Berlin Heidelberg.
- Posch, Reinhard [2008]. *A Federated Identity Management Architecture for Cross-Border Services in Europe*. In *BIOSIG*, pages 141–152.
- Posch, Reinhard, Clemens Orthacker, Klaus Stranacher, Arne Tauber, Thomas Zefferer, and Bernd Zwattendorfer [2010]. *Open Source Bausteine als Kooperationsgrundlage*. In Eixelsberger/Stember (Editor), *E-Government - Zwischen Partizipation und Kooperation*, pages 185–210. Springer Wien-New York.
- Prodromou, Evan, Darren Platt, Robert L. Grzywinski, and Eric Olden [2000]. *AuthXML: A Specification for Authentication Information In XML*.
- Ramsdell, B. and S. Turner [2010]. *RFC 5751 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification*. Technical Report, Internet Engineering Task Force (IETF).
- Reed, Drummond, Dave McAlpin, Peter Davis, Nat Sakimura, Mike Lindelsee, and Gabe Wachob [2005]. *Extensible Resource Identifier (XRI) Syntax V2.0*. Technical Report, OASIS.
- Reichstädter, Peter [2012]. *Cloud Computing - Positionspapier 2011*. Technical Report, AG-Cloud / BLSG.

- Relyea, Harold C. [2002]. *E-gov: Introduction and overview*. *Government Information Quarterly*, 19(1), pages 9–35.
- Repschlaeger, Jonas, Stefan Wind, Ruediger Zarnekow, and Klaus Turowski [2012]. *A Reference Guide to Cloud Computing Dimensions: Infrastructure as a Service Classification Framework*. *45th Hawaii International Conference on System Sciences*, pages 2178–2188.
- Rivest, Ronald L, Adi Shamir, and Yael Tauman [2006]. *How to Leak a Secret: Theory and Applications of Ring Signatures*. In Goldreich, Oded, Arnold L. Rosenberg, and Alan L. Selman (Editors), *Theoretical Computer Science*, pages 164–186. Springer Berlin Heidelberg.
- Robinson, Neil, Helen Rebecca Schindler, Jonathan Cave, and Janice Pedersen [2010]. *Computing in the public sector: rapid international stocktaking*. Technical Report, Netherland's Ministry of Internal Affairs and Kingdom Relations (BZK). <http://www.scribd.com/doc/40866691/Cloud-Computing-in-the-Public-Sector>.
- Rodriguez, Ricardo, John Warmerdam, and Claude Emmanuel Triomphe [2010]. *The Lisbon strategy 2000-2010. An analysis and evaluation of the methods used and results achieved*. Technical Report, European Parliament's Committee on Employment and Social Affairs.
- Roessler, Thomas [2010]. *E-Government und Cloud-Computing*. Technical Report, EGIZ.
- Roman, Ed, Rima Patel Sriganesh, and Gerald Brose [2005]. *Mastering Enterprise JavaBeans*. 3rd Edition. Wiley Publishing, Inc., 1–841 pages.
- Rössler, Thoms, Arno Hollosi, Michael Liehmann, and Rudolf Schamberger [2006]. *Elektronische Vollmachten Spezifikation 1.0.0*. Technical Report, IKT-Strategie des Bundes.
- Roth, Volker and Philipp Schmidt [2011]. *Pseudonymity and Anonymity*. In Fumy, Walter and Manfred Paeschke (Editors), *Handbook of eID Security - Concepts, Practical Experiences, Technologies*, pages 31–44. Publicis Publishing, Erlangen.
- RSA Laboratories [2009]. *PKCS #11 Base Functionality v2.30: Cryptoki - Draft 4*. <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30b-d6.pdf>.
- Sakimura, N., J. Bradley, M. Jones, B. de Medeiros, and C. Mortimore [2014]. *OpenID Connect Core 1.0*. Technical Report, OpenID. http://openid.net/specs/openid-connect-core-1_0.html.
- Sandhu, RS and Pierangela Samarati [1994]. *Access Control: Principle and Practice*. *IEEE Communications Magazine*, 32(9), pages 40–48.
- Schaffer, Henry E. [2009]. *X as a Service, Cloud Computing, and the Need for Good Judgment*. *IT professional*, 11(5), pages 4–5.
- Schüssel, Wolfgang and Franz Morak [2005]. *i2010 - Implementation*. <https://www.bka.gv.at/DocView.axd?CobId=16635>.
- Sen, Jaydip [2013]. *Security and Privacy Issues in Cloud Computing*. In Martínez, Antonio Ruiz, Rafael Marin-Lopez, and Fernando Pereniguez-Garcia (Editors), *Architectures and Protocols for Secure Information Technology Infrastructures*, pages 1–45. IGI Global.
- Senate of the United States [2001]. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*. <http://epic.org/privacy/terrorism/hr3162.pdf>.
- Shim, Simon S.Y., Geetanjali Bhalla, and Vishnu Pendyala [2005]. *Federated identity management*. *Computer*, 38(12), pages 120–122.

- Silcock, R. [2001]. *What is e-Government*. *Parliamentary affairs*, 54(1), pages 88–101.
- Slamanig, Daniel, Klaus Stranacher, and Bernd Zwattendorfer [2014]. *User-Centric Identity as a Service-Architecture for eIDs with Selective Attribute Disclosure*. In *ACM Symposium on Access Control Models and Technologies (SACMAT)*.
- Stefanova, Kamelia, Dorina Kabakchieva, and Lia Borthwick [2005]. *GUIDE Open Identity Management Architecture Design - Key Contribution to the Further Advancement of e-Government Throughout Europe*. In *ECEG*, pages 377–386.
- Stefanova, Kamelia, Dorina Kabakchieva, and Roumen Nikolov [2010]. *Design Principles of Identity Management Architecture Development for Cross-Border eGovernment Services*. *Electronic Journal of e-Government*, 8(2), pages 189–202.
- Stern, Marc [2011]. *D5.8.3d Security Principles and Best Practices*. Technical Report, STORK Consortium.
- STORK 2.0 Consortium [2013]. *STORK 2.0 Fact Sheet*. https://www.eid-stork2.eu/index.php?option=com_processes&controller=document&view=document&task=streamFile&id=17&fid=390.
- Stranacher, Klaus, Vesna Krnjic, Bernd Zwattendorfer, and Thomas Zefferer [2013a]. *Assessment of Redactable Signature Schemes for Trusted and Reliable Public Sector Data*. In *13th European Conference on e-Government*, pages 508–516.
- Stranacher, Klaus, Thomas Lenz, and Konrad Lanz [2013b]. *Trust-Service Status List Based Signature Verification*. In *Technology-Enabled Innovation for Democracy, Government and Governance*, pages 29–42.
- Stranacher, Klaus, Arne Tauber, Thomas Zefferer, and Bernd Zwattendorfer [2011]. *Grenzüberschreitendes E-Government in Europa*. *eGovernment Review*, 8, pages 8–9.
- Stranacher, Klaus, Arne Tauber, Thomas Zefferer, and Bernd Zwattendorfer [2013c]. *The Austrian Identity Ecosystem: An E-Government Experience*. In Martínez, Antonio Ruiz, Rafael Marin-Lopez, and Fernando Pereniguez-Garcia (Editors), *Architectures and Protocols for Secure Information Technology Infrastructures*, pages 288–309. IGI Global.
- Stranacher, Klaus and Bernd Zwattendorfer [2012]. *Ein interoperabler Container für elektronische Dokumente*. In *D-A-CH Security 2012*, pages 21–431. 2012.
- Stranacher, Klaus and Bernd Zwattendorfer [2013]. *Redigierbare Signaturen in e-Business Anwendungen*. In *D-A-CH Security 2013*, pages 19–30.
- Subashini, S. and V. Kavitha [2011]. *A survey on security issues in service delivery models of cloud computing*. *Journal of Network and Computer Applications*, 34(1), pages 1–11.
- Sumelong, Ivo, Armin Lunkeit, Bernd Zwattendorfer, and Tim Schneider [2011]. *D5.8.3e Software Design for MW architecture*. Technical Report, STORK Consortium.
- Suoranta, Sanna, Asko Tontti, Joonas Ruuskanen, and Tuomas Aura [2013]. *Logout in Single Sign-on Systems*. In *Policies and Research in Identity Management*, pages 147–160.
- Talamo, Maurizia, Franco Arcieri, Guido Maria Marinelli, and Christian H. Schunck [2011]. *The Italian eID Solution*. In Fumy, Walter and Manfred Paeschke (Editors), *Handbook of eID Security - Concepts, Practical Experiences, Technologies*, pages 140–153. Publicis Publishing, Erlangen.

- Tauber, Arne [2012]. *Cross-Border Certified Electronic Mailing*. PhD Thesis, Graz University of Technology.
- Tauber, Arne and Bernhard Karning [2013]. *Spezifikation Layout Amtssignatur*. Technical Report, PG Amtssignatur / AG ReSi.
- Tauber, Arne, Herbert Leitold, and Reinhard Posch [2011a]. *Online-Vollmachten - Spezifikation*. Technical Report, AG-II.
- Tauber, Arne, Thomas Zefferer, and Bernd Zwattendorfer [2012]. *Approaching the Challenge of eID Interoperability: An Austrian Perspective*. *European Journal of ePractice*, 14, pages 22–39.
- Tauber, Arne, Bernd Zwattendorfer, and Klaus Stranacher [2013]. *Elektronische Identität und Stellvertretung in Österreich*. In *D-A-CH Security 2013*, pages 1–9.
- Tauber, Arne, Bernd Zwattendorfer, and Thomas Zefferer [2011b]. *A Shared Certified Mail System for the Austrian Public and Private Sectors*. In *Electronic Government and the Information Systems Perspective*, pages 356–369.
- Tauber, Arne, Bernd Zwattendorfer, and Thomas Zefferer [2011c]. *Elektronisches Einschreiben im D-A-CH Raum*. In *D-A-CH Security 2011*, pages 510–521.
- Tauber, Arne, Bernd Zwattendorfer, and Thomas Zefferer [2011d]. *STORK: Pilot 4 Towards Cross-border Electronic Delivery*. In *Electronic Government and Electronic Participation - Joint Proceedings of Ongoing Research and Projects of IFIP EGOV and ePart 2011*, pages 295–301.
- Tauber, Arne, Bernd Zwattendorfer, Thomas Zefferer, Yasmin Mazhari, and Eleftherios Chamakiotis [2010]. *Towards interoperability: an architecture for pan-European eID-based authentication services*. In *Proceedings of the International Conference on Electronic Government and the Information Systems Perspective (EGOVIS)*, pages 120–133.
- Tinholt, Dinand, Graham Colclough, Sander Oudmaijer, Wendy Carrara, Trudy Tol, Mark Schouten, Niels van der Linden, Gabriella Cattaneo, Stefania Aguzzi, Laurent Jacquet, Hugo Kerschot, Roland van Gompel, Jo Steyaert, Jeremy Millard, and Rebecca Schindler [2012]. *Public Services Online 'Digital by Default or by Detour?' - Assessing User Centric eGovernment performance in Europe - eGovernment Benchmark 2012*. Technical Report, Capgemini, IDC, Sogeti, IS-practice and Indigov, RAND Europe and the Danish Technological Institute for the Directorate General for Communications Networks, Content and Technology.
- Tsolkas, Alexander and Klaus Schmidt [2010]. *Rollen und Berechtigungskonzepte: Ansätze für das Identity- und Access Management im Unternehmen*. Springer, 332 pages.
- UK Cabinet Office [2013]. *ICT strategy resources*. <https://www.gov.uk/government/collections/ict-strategy-resources>.
- Vaikuntanathan, Vinod [2011]. *Computing Blindfolded: New Developments in Fully Homomorphic Encryption*. In *IEEE 52nd Annual Symposium on Foundations of Computer Science*, pages 5–16. IEEE.
- von Lucke, Jörn and Heinrich Reineremann [2000]. *Speyerer Definition von Electronic Government*. Technical Report, Forschungsinstitut für öffentliche Verwaltung bei der Deutschen Hochschule für Verwaltungswissenschaften Speyer.
- Wauters, Patrick, Matthias Nijskens, and Jeroen Tiebout [2007]. *The User Challenge, Benchmarking The Supply Of Online Public Services*. Technical Report, Capgemini.

- West, Darrell M. [2010]. *Saving money through cloud computing*. Technical Report, The Brookings Institution.
- Wimmer, Maria a. [2002]. *A European perspective towards online one-stop government: the eGOV project*. *Electronic Commerce Research and Applications*, 1(1), pages 92–103.
- Windley, Phillip J. [2005]. *Digital Identity*. O'Reilly Media, Inc., 256 pages.
- WP2 Team [2012]. *D2.2 Existing attribute sources/sinks analysis*. Technical Report, STORK 2.0 Consortium.
- WP4 Core Team [2012]. *First version of process flows*. Technical Report, STORK 2.0 Consortium.
- WP4 Core Team [2013]. *D4.2 First version of Functional Design Deliverable*. Technical Report, STORK 2.0 Consortium.
- WP4 Core Team [2014]. *D4.4 First version of Technical Specifications for the cross border Interface*. Technical Report, STORK 2.0 Consortium.
- Wyld, David C. [2009]. *Moving to the Cloud: An Introduction to Cloud Computing in Government*. Technical Report, IBM Center for The Business of Government.
- Yildiz, Mete [2007]. *E-government research: Reviewing the literature, limitations, and ways forward*. *Government Information Quarterly*, 24(3), pages 646–665.
- Ylätupa, Tuomas [2011]. *CLOUD COMPUTING IN THE ICT OF FINNISH PUBLIC ADMINISTRATION*. Bachelor thesis, Saimaa University of Applied Sciences.
- Yuan, Eric and Jin Tong [2005]. *Attributed Based Access Control (ABAC) for Web services*. In *International Conference on Web Services, 2005. ICWS 2005*.
- Zacks Equity Research [2012]. *Accenture to Build French G-Cloud*. <http://www.zacks.com/stock/news/67978/Accenture+to+Build+French+G-Cloud>.
- Zefferer, Thomas [2010]. *STORK Work Item 3.3.5 Smartcard eID Comparison*. Technical Report, STORK Consortium.
- Zefferer, Thomas, Bernd Zwattendorfer, Arne Tauber, and Thomas Knall [2011]. *Secure and Reliable Online-Verification of Electronic Signatures in the Digital Age*. In White, Bebo, Pedro Isaías, and Flávia Maria Santoro (Editors), *Proceedings of the IADIS International Conference WWW/INTERNET 2011*, pages 269–276.
- Zhang, Qi, Lu Cheng, and Raouf Boutaba [2010]. *Cloud computing: state-of-the-art and research challenges*. *Journal of Internet Services and Applications*, 1(1), pages 7–18.
- Zissis, Dimitrios and Dimitrios Lekkas [2012]. *Addressing cloud computing security issues*. *Future Generation Computer Systems*, 28(3), pages 583–592.
- Zwattendorfer, Bernd and Daniel Slamanig [2013a]. *On Privacy-Preserving Ways to Porting the Austrian eID System to the Public Cloud*. In *28th IFIP TC-11 International Information Security and Privacy Conference (SEC 2013)*, pages 300–314.
- Zwattendorfer, Bernd and Daniel Slamanig [2013b]. *Privacy-Preserving Realization of the STORK Framework in the Public Cloud*. In *10th International Conference on Security and Cryptography (SECRYPT 2013)*, pages 419–426. SCITEPRESS Digital Library.

- Zwattendorfer, Bernd and Daniel Slamanig [2013c]. *Scalable and Privacy-Preserving Variants of the Austrian Electronic Mandate System in the Public Cloud*. In *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-13)*, pages 24–33.
- Zwattendorfer, Bernd, Klaus Stranacher, and Arne Tauber [2012a]. *Bürgerkarten-Authentifizierung zur Public Cloud*. In *D-A-CH Security 2012*, pages 136–147.
- Zwattendorfer, Bernd, Klaus Stranacher, and Arne Tauber [2013a]. *Towards a Federated Identity as a Service Model*. In *Technology-Enabled Innovation for Democracy, Government and Governance*, pages 43–57.
- Zwattendorfer, Bernd, Klaus Stranacher, Arne Tauber, and Peter Reichstädter [2013b]. *Cloud Computing in E-Government across Europe*. In *Technology-Enabled Innovation for Democracy, Government and Governance*, pages 181–195.
- Zwattendorfer, Bernd and Ivo Sumelong [2011]. *Interoperable Middleware-Architektur für sichere, länderübergreifende Identifizierung und Authentifizierung*. In *Tagungsband zum 12. Deutschen IT-Sicherheitskongress*, pages 175–189. SecuMedia.
- Zwattendorfer, Bernd, Ivo Sumelong, and Herbert Leitold [2012b]. *Middleware Architecture for Cross-Border eID*. In *Eighth International Conference on Information Assurance and Security (IAS)*, pages 303–308. IEEE.
- Zwattendorfer, Bernd, Ivo Sumelong, and Herbert Leitold [2013c]. *Middleware Architecture for Cross-Border Identification and Authentication*. *Journal of information assurance and security (JIAS)*, 8, pages 107–118.
- Zwattendorfer, Bernd, Bojan Suzic, Peter Teufl, and Andreas Derler [2013d]. *Secure Hardware-Based Public Cloud Storage*. In *Open Identity Summit 2013*, pages 43–54.
- Zwattendorfer, Bernd, Bojan Suzic, Peter Teufl, and Andreas Derler [2013e]. *Sicheres Speichern in der Public Cloud mittels Smart Cards*. In Schartner, Peter and Peter Trommler (Editors), *D-A-CH Security 2013*, pages 120–132.
- Zwattendorfer, Bernd and Arne Tauber [2012a]. *Secure cloud authentication using eIDs*. In *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, pages 397–401. IEEE.
- Zwattendorfer, Bernd and Arne Tauber [2012b]. *Secure cross-cloud single sign-on (SSO) using eIDs*. In *Internet Technology And Secured Transactions (ICITST)*, pages 150–155.
- Zwattendorfer, Bernd and Arne Tauber [2012c]. *The Public Cloud for e-Government*. In *Technology-Enabled Innovation for Democracy, Government and Governance*, pages 129–136.
- Zwattendorfer, Bernd and Arne Tauber [2013]. *The Public Cloud for e-Government*. *International Journal of Distributed Systems and Technologies*, 4(4), pages 1–14.
- Zwattendorfer, Bernd, Arne Tauber, Klaus Stranacher, and Peter Reichstädter [2012c]. *Cross-Border Legal Identity Management*. *Electronic Government 11th IFIP WG 8.5 International Conference, EGOV 2012*, pages 149–161.
- Zwattendorfer, Bernd, Arne Tauber, and Thomas Zefferefer [2011a]. *A privacy-preserving eID based Single Sign-On solution*. In *5th International Conference on Network and System Security*, pages 295–299. IEEE.
- Zwattendorfer, Bernd, Thomas Zefferefer, and Klaus Stranacher [2014]. *An Overview of Cloud Identity Management-Models*. In *10th International Conference on Web Information Systems and Technologies (WEBIST)*, pages 82–92. SCITEPRESS Digital Library.

Zwattendorfer, Bernd, Thomas Zefferer, and Arne Tauber [2011b]. *E-ID Meets E-Health on a Pan-European Level*. In *Proceedings of the IADIS International Conference e-Health*, pages 97–104.

Zwattendorfer, Bernd, Thomas Zefferer, and Arne Tauber [2012d]. *The prevalence of SAML within the European Union*. In *8th International Conference on Web Information Systems and Technologies (WEBIST)*, pages 571–576.