Electronic Voting over the Internet – an E-Government Speciality

by

THOMAS GERT RÖSSLER
Dipl.-Ing.

A dissertation submitted to the
University of Technology Graz, Austria

for the degree of
Doktor der Technischen Wissenschaften
(Doctor technicae)

accepted on the recommendation of
Univ.-Prof. Dr. Reinhard Posch, examiner
Univ.-Prof. Dr. Rüdiger Grimm, co-examiner

September 2007

Institute for Applied Information Processing and Communications (IAIK)
Faculty of Informatics
Graz University of Technology, Austria

Abstract

E-voting increasingly gains interest in e-Democracy and e-Government movements. Not only the technical security issues of electronic voting systems are of paramount importance, but also the necessity of following an all-embracing approach is challenging and needs to be addressed.

This thesis discusses e-voting as being a supreme discipline of e-Government. It tackles the question whether existing e-Government technologies and approaches are sufficient to serve e-voting requirements, and if so, discusses what an e-voting solution might look like. This work introduces an innovative e-voting concept using the Internet as the voting channel. The concept introduced is based on Austrian e-Government elements and the Austrian identity management concept in particular. Like any other e-Government application, e-voting requires a comprehensive handling of all legal, organisational and technical aspects. Therefore, this thesis treats e-voting on different abstraction layers.

As a result, this thesis introduces a novel approach of building an e-voting system relying on two core principles: strong end-to-end encryption and stringent identity domain separation. This theses finally reflects how this approach fits international standardization initiatives, such as the Council of Europe recommendations on e-enabled elections.

Zusammenfassung

E-Government und E-Voting verlangen hohe bzw. höchste Anforderungen an die IT-Sicherheit. Obschon der Entwicklungsgrad von E-Government Lösungen bereits ein hohes Maß erreicht hat, erfolgen konkrete Schritte in Richtung Aufgriff von E-Voting Lösungen nur spärlich. Nicht zu letzt das österreichische E-Government zeichnet sich durch einen hohen Entwicklungsgrad aus, wobei besonders das dem zu Grunde gelegte elektronische Identitätsmanagementkonzept dem Bürger ein Höchstmaß an Datenschutz gewährleistet.

Diese Dissertation stellt ein neues E-Voting Konzept vor, das besonders den Bedürfnissen österreichischer Wahlen zugeschnitten ist. Es bedient sich dabei im Kern der grundlegenden Technologien des österreichischen E-Governments, und wendet zur Gewährleistung der Anonymität, entgegen gängiger E-Voting Schemen, die Kombination aus starker Verschlüsselung und getrennten Identitätsdomänen an. Vor allem die Einführung getrennter Identitätsdomänen stellt eine Weiterentwicklung des österreichischen Identitätsmanagements dar. Darüberhinaus fasst diese Arbeit die Aussage, dass ausschließlich ein gesamtheitliches Sicherheitskonzept, das heißt nur ein koordiniertes Zusammenspiel technischer, rechtlicher und organisatorischer Sicherheitselemente, eine zufriedenstellende Lösung für Distanzwahlsysteme unter Verwendung des Internets realisierbar macht. Diese Arbeit skizziert ein solches vor dem Hintergrund einer konkreten, exemplarischen Wahl: der Hochschülerschaftswahl.

Contents

List of Figures

List of Tables

List of Acronyms

AA

Asserting Authority
The Asserting Authority confirms indirectly the voter's identity and blindly signs the whole ballot and all its elements to detect any latter modification.

CC

Common Criteria
International standard defining common criteria for information technology security evaluation.

CCE

Citizen Card Environment
The sum of all elements and components implementing the Citizen Card Concept is denoted as Citizen Card Environment.

CRR

Central Residents Register
The Central Residents Register is the register for all persons residing in Austria.

EA

Election Authority
The Election Authority is the authority legally carrying out the election and is usually overall responsible for the election.

e-ID

electronic Identity
An electronic Identity of an entity is the dynamic collection of all of the entity's attributes in an electronic form (definition taken from [7]).

EML

Election Markup Language
The Election Markup Language is a standardised XML language for the interchange of data among election services.

EVITA

Electronic Voting over the Internet - Tailored for Austria
EVITA is the name of the e-voting concept introduced by this thesis.

EVS

E-Voting Schema
The E-Voting Schema is the technical and mathematical core principle underlying an e-voting system.

HMAC

keyed-Hash Message Authentication Code
A keyed-Hash Message Authentication Code is a message authentication resulting from applying a cryptographic hash function in combination with a secret key.

HSM

Hardware Security Module
A Hardware Security Module is a device which securely creates and/or holds secrets—e.g. secret keys—and/or provides secret key operations for cryptographic applications.

OASIS

Organization for the Advancement of Structured Information Standards
The international Organization for the Advancement of Structured Information Standards hosts several committees developing technical standards.

PIN

Personal Identification Number
A Personal Identification Number is a number used to identify a person (within some context).

RA

Registration Authority
The Registration Authority is responsible for the whole registration phase of the proposed e-voting process.

SERVE

Secure Electronic Registration and Voting Experiment
The Secure Electronic Registration and Voting Experiment of the United States Department of Defense was intended to provide U.S. military staff abroad the possibility to vote electronically.

sPIN

Source Personal Identification Number
The Source Personal Identification Number is a person's very unique identification number.

SR

Supplementary Register
The Supplementary Register is an additional register for the purpose of electronic validation of entities' unique identity if they are not registered with other registers (e.g. Central Resident Register).

ssPIN

Sector Specific Personal Identification Number
The Sector Specific Personal Identification Number is a person's identifier for a specific sector of applications used to uniquely identify her within this specific sector.

TOE

Target of Evaluation
The Target of Evaluation is the subject of interest in a security evaluation process (e.g. this term TOE is defined in Common Criteria).

vPIN

Voting Personal Identification Number
The Voting Personal Identification Number is a special identifier representing a voter's identity with respect to electoral matters.

XML

Extensible Markup Language
The Extensible Markup Language is a general purpose language for interchanging and processing structured data.

Chapter 1

Introduction

Voting is the most important tool in democratic decision making. Therefore, elections and referenda should be accessible to as many people as possible. It is especially difficult for citizens living abroad to participate in elections. Thus, electronic elections, referred to as e-voting, is gaining more and more public interest.

The word e-voting is a general term that refers to any type of voting in electronical form. Thus, e-voting includes voting by telephone as well as electronic voting machines in voting booths. This work deals with e-voting in the sense of voting with the use of an ordinary computer via the Internet[1]. Irrespective of how the e-voting is carried out and what kind of technology is used, keeping the voter's decision represented by the voter's cast vote an inviolable secret is most essential.

This thesis treats e-voting as a special e-Government application and analyses whether the technologies and solutions provided by today's e-Government serve as a suitable basis for the development of an e-voting concept. This introductory chapter prefaces this thesis and explains the motives behind the work presented.

1.1 Motivation and Problem

E-Government is about the "*[..] modernisation of public administration bringing it closer to civil society and businesses through the use of information and communication technologies*"[2]. In other words, e-Government aims to reduce the barriers for citizens interacting with public administrations. E-Government has had a long successful history. From a European perspective, in order to foster e-Government within the European Union, the European Commission has launched action plans—the very first E-Government action plan "eEurope2005" was launched at the Seville summit 2000—and several collaborative initiatives and projects. As a result, the e-Government infrastructure is highly developed in many member states of the European Union. Austria in particular has actively pursued its e-Government strategy since the beginning and thus is today one of leading countries in Europe with respect to e-Government[3].

[1] This branch of e-voting is sometimes also denoted as *i-voting*.

[2] Taken from Council of Europe's definitions, http://www.coe.int/T/E/Com/Files/Themes/E-Voting/definition.asp, as seen on 29 July 2007.

[3] At the time of writing, the e-Government benchmark study 2006 of Cap-Gemini designates Austria as being the number one of the EU member states with respect to E-Government services.

Past and ongoing e-Government initiatives in Europe have had a lot of achievements at all relevant levels, at technical, organisational and legal levels, not only within member states but also in a Europe-wide dimension. Consider the achievements in the area of identity management, for instance, identity management is one of the most fundamental e-Government topics since almost any e-Government application dealing with citizens or enterprises draws on identities. Thus, most of the member states introduced electronic identity management concepts adapted to their national needs and suited to their national legislation and organisational requirements. Additionally, at the European level, the member states collaboratively addressed the interoperability of existing national identity management solutions in order to achieve seamless e-Government in a cross-border manner. The commission strongly supports these developments by launching funded projects in electronic identity related management and interoperability issues. As a result, many countries run sophisticated identity management systems and various studies and concepts on how to achieve interoperability at an international level have been developed. The example of identity management perfectly demonstrates the current status of e-Government developments: e-Government is much developed already and interoperability is subject of current developments. Thus, e-Government today seems to serve a sophisticated basis for applications.

The scope of e-Government is to bring public administrations closer to citizens. From this point of view, the next logical step ahead is to offer citizens active participation in democratic processes by electronic means. E-Government can be seen as one of the very first “e”-developments, but apart from e-Government, other disciplines related to the relationship between a country and its citizens exist. Therefore, the term “E-Governance” has been introduced as embracing the heading above, with e-Government as one of its sub-disciplines. The discipline related to active participation is denoted as “e-democracy”. A general definition of e-Governance and its sub-categories can be found at [8]. However, although e-Government is “only” a building block of e-Governance, it heavily influences all other elements since the fundamentals laid down by e-Government implementations act as the basis.

One of the most challenging topics in the area of e-democracy is e-voting. E-voting, as a special application of e-Government technologies, can be considered as being the supreme discipline of all e-Government applications due to its conflicting priorities of unique identification and perfect anonymity. In addition to the challenges caused by its technical nature, e-voting in general is of keen interest and currently heavily discussed, especially in Austria. Austrian citizens living abroad are adamant about asking for remote voting opportunities, since voting from abroad has proved to be quite difficult, depending on the country in which the citizen resides. The introduction of e-voting would not only be an improvement for voters living abroad but also for voters residing in Austria.

Thus, the overall question addressed by this thesis is whether or not existing e-Government elements serve a basis for the development of a remote e-voting solution. To be more precise, the work presented by this thesis tackles the problem of developing a remote e-voting concept using the Internet as a voting channel for major elections in Austria, whereby the conventional voting process should be kept in parallel. The resulting e-voting concept should be based on Austrian e-Government elements and should satisfy the requirements laid down by Austrian legislation. This aim implies the hypothesis, that a remote e-voting solution could intensely benefit from the Austrian e-Government framework.

Therefore, this thesis is not a pure e-voting thesis but also an e-Government thesis. In this work, the elements and methodology of e-Government are used to solve the problems of remote e-voting. Thus, this thesis follows an onionskin approach. It starts by discussing the stated problem at a highly abstract level by analysing the international and national legal situation, since the legal situation determines the playing field for any suitable solution. At the next level of abstraction, the thesis deals with an embracing

security analysis based on the requirements given by law. Based on the security objectives achieved, the thesis enters the next abstraction level and sketches the process model of the e-voting solution proposed. This step-wise methodology leads to an all-embracing understanding of the problem and finally examines an all-embracing problem solution. Furthermore, the solution presented in this thesis has been drawn up involving all these levels, since complex IT security problems in general, and e-Government and e-voting in particular, require a well concerted interaction of individual solutions at all these levels.

1.2 Concept of the proposed Solution EVITA

This thesis introduces a remote Internet e-voting concept that suits the needs of Austrian elections and is based upon Austrian e-Government components. The proposed e-voting concept draws upon two principles in order to protect the election secrecy. On the one hand, the proposed e-voting system makes use of strong end-to-end encryption between the voter casting her vote and the electronic device responsible for counting. Thus, the cast vote is immediately encrypted by the voter after she has filled in her decision and is only decrypted for the single moment of counting. On the other hand, the proposed e-voting concept introduces a stringent domain separation model that has to ensure unique identification of voters during registration, but also guarantee perfect anonymity of cast votes. A special case in the introduced e-voting concept is that although votes are cast anonymously it is still possible to determine whether a given voter has cast her vote already or not. This mechanism is available during the election event only. It enables a voter to cast her vote conventionally at a polling station although she has decided to vote electronically. This characteristic of the proposed e-voting concept faces problems in connection with the Internet and the voter's local infrastructure.

From a technical perspective, the proposed e-voting concept makes use of Austrian e-Government components such as the Citizen Card. Although the core principles of this e-voting concept are versatile, the resulting e-voting concept is tailored to a certain degree for Austrian elections. Thus, the proposed e-voting concept has been named "EVITA" which stands for Electronic Voting over the Internet - Tailored for Austria (EVITA) (figure 1.1 illustrates the EVITA project logo).

Figure 1.1: The EVITA project logo.

1.3 Structure of this Thesis

This thesis is organised as follows. After the introduction, chapter two discusses elections in general. It elaborates on the fundamentals of elections from a legal perspective by referring to international and national election fundamentals. The second chapter also analyses the legal situation with respect to

e-voting in Austria. Chapter three discusses e-voting from a scientific point of view. It discusses the three major types of e-voting schemes; homomorphic encryption schemes, schemes based on mixing nets and schemes based on blind signatures, and categorises e-voting concepts according to their underlying phase models. Thus first, second and n-th phase models are introduced. A survey of notable e-voting systems and projects is given in chapter four which complements the discussion on existing e-voting approaches. In the course of this survey, two existing e-voting projects are analysed in a more detailed way, namely the e-voting system of Estonia and the e-voting project developed by the University of Economics in Vienna. The former example was chosen since the Estonian system is one of the few Internet-based remote e-voting systems that have been used in real elections on a large scale already. The latter example was chosen because it claims to be an e-voting solution suitable for Austria. Based on the discussions held in the previous chapters, chapter five compiles a set of security objectives from the conclusions of the preceding discussions and existing national and international initiatives. The resulting security objectives provide a set of requirements for the EVITA e-voting concept. Since the proposed e-voting concept makes use of Austrian e-Government technology, chapter six briefly describes the most important elements of the Austrian e-Government framework. The subsequent chapters, seven and eight respectively, introduce the core principles of the EVITA e-voting concept and define its underlying processes in detail. In order to evaluate the developed e-voting concept from a practical point of view, the most important elements of the EVITA e-voting concept have been implemented in a prototype. Thus, chapter nine provides a brief overview of this prototype and discusses the lessons learned from it. Finally, chapter ten gives a short analysis of the proposed e-voting concept based on a comparison between the security objectives defined in chapter five and the fundamentals of the EVITA e-voting concept. Furthermore, this chapter summarizes the thesis and draws conclusions.

Chapter 2

Elections - a Democratic Obligation

Although this thesis is a technical treatise on e-voting, it is necessary to discuss e-voting from a legal perspective as well in order to understand and elaborate on the requirements for a technical e-voting solution. Thus, this chapter analyses elections from a legal perspective. It highlights international legal fundamentals and shows their influence on the Austrian national legislation. Furthermore, this chapter discusses remote e-voting and its legal basis.

2.1 International Fundamentals

> ***Article 3 - Right to free elections***
> *The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature. Council of Europe [9]*

Elections are the democratic obligation of states which operate under democratic fundamentals. The Convention for the Protection of Human Rights and Fundamental Freedoms [10] lays down the democratic fundamentals for the member states of the Council of Europe. In addition to the right of "freedom of expression", as stated in article 10 of [10], and the right of "freedom of assembly and association", as stated in article 11 of [10], the first additional protocol of this convention substantiates the "right to free elections". These three human rights are especially important with respect to democratic fundamentals. All member states of the Council of Europe which have agreed to uphold human rights as settled by the council's convention are required to hold *free* and *secret* elections regularly.

After the breakdown of the Soviet Union, a number of new independent states suddenly arose. All of them had to create their own legislations and constitutions based on democratic fundamentals. The Council of Europe recognised the need for supporting these new countries in creating their own democratic fundamentals. Thus, the Council of Europe founded the European Commission for Democracy through Law, called the *Venice Commission*, in the year 1990 as "*a tool for emergency constitutional engineering*"[1].

Since the Venice Commission aims to support states in adopting Europe's legal basis and democratic fundamentals, one of its main fields of interest is the electoral field. More than fifty years after the

[1] taken from the representation of the Venice Commission, as seen at http://www.venice.coe.int/site/main/presentation_E.asp, 25 May 2007.

settlement of the fundamentals for elections within the Convention for the Protection of Human Rights, the Council of Europe asked the Venice Commission to create a Code of Good Practice in Electoral Matters [11] in order to deepen the common understanding of free and secret elections.

This Code of Good Practice sets down the fundamental principles for democratic elections, based on the right to free elections defined within the Convention for the Protection of Human Rights and Fundamental Freedoms. It defines and addresses six principles:

1. universal suffrage
2. equal suffrage
3. free suffrage
4. secret suffrage
5. direct suffrage
6. frequency of elections

Although the Code of Good Practice has never been formally adopted as legally binding on the member states of the Council of Europe, it is considered as having set down the fundamental principles for elections. It has influence on the jurisdiction of the European Court of Human Rights as well. For example, the concurring opinion with respect to the judgment concerning application number 74025/01 (Hirst vs. the United Kingdom)[2], Judge Caflish explicitly names the Code of Good Practice on Electoral Matters as being meaningful:

> *[..] Two out of the above four elements are contained in the Code of Good Practice of the Venice Commission: I say this not because I consider that Code to be binding but because, in the subject-matter considered here, these elements make eminent sense.[..] [12]*

Based on this judgment and on the comment given within the concurring opinion, Christoph Grabenwarter[3] concludes in [13]:

> *[..] Im Einklang mit der Praxis des EGMR, zur Interpretation von Konventionsgarantien andere internationale Dokumente, insbesondere solche des Europarates, heranzuziehen [..], können der "Code of Good Practice" der Venedig-Kommission auch bei der Auslegung des Art 3 1. ZPEMRK dergestalt Berücksichtigung finden, dass er die Mindestbedingungen formuliert, die erfüllt werden müssen, damit die Vorgabe freier und geheimer Wahlen genüge getan ist. [..] [13]*

Grabenwarter states that the fact the European Court of Human Rights considers the Code of Good Practice of the Venice Commission in their judgments means that the Code of Good Practice is considered as having laid down the minimum requirements for free and secret elections as required by the first additional protocol of the Convention for the Protection of Human Rights and Fundamental Freedoms. Therefore, the Code of Good Practice is meaningful, not only from an academic perspective, but from a legal perspective as well. The following paragraphs briefly outline the six principles given within the Code of Good Practice and emphasize the implications it has on e-voting whenever meaningful.

[2]Hirst vs. the United Kingdom (no. 2), no. 74025/01 (Sect. 4) (Eng) - (30 March 2004)

[3]Univ.-Prof.DDr. Christoph Grabenwarter, Professor at the Department for Staats- und Verwaltungsrecht at the University Graz (Austria). He is currently a member of the Venice Commission

Universal Suffrage

> *Universal suffrage means in principle that all human beings have the right to vote and to stand for election. [11]*

This principle states that all human beings have the right to participate in elections, not only as a voter but also as a candidate. However, the Code of Good Practice also says that certain restrictions might be put in place that would be useful. The types of restrictions named by the Venice Commission are concerned with age, nationality, residence and deprivation of the right to elect and to be elected.

The right to elect and to be elected is usually bound to a certain age. The commission recommends that the minimum age to be allowed to elect and to stand for elections should be the same, but under certain circumstances they might differ (e.g. many states set the minimum age for presidential candidates higher than the age required to vote).

Another criteria for universal suffrage, which especially influences e-voting and remote voting in general, is the residence of a human being. The Code of Good practice states that a residence requirement might be imposed (the code makes some clear recommendations with respect to this), but "*the right to vote and to be elected may be accorded to citizens residing abroad*" [11]. So citizens who do not reside in their homeland on election day may still be allowed to vote.

Additional recommendations of the Venice Commission address electoral registers which are considered to be of paramount importance in order to maintain universal suffrage. Only if electoral registers are well maintained and up to date can the right to vote or to be elected be effectively enforced.

Equal Suffrage

This entails:

> *Equal voting rights: each voter has in principle one vote; where the electoral system provides voters with more than one vote, each voter has the same number of votes.*
> *[..] Equal voting power: seats must be evenly distributed between the constituencies.*
> *[..] Equality of opportunity*
> *[..] Equality and national minorities*
> *[..] Equality and parity of the sexes*
> *[11]*

This principle guarantees that each voter's decision influences the election result in the same way and with the same power. No voter is allowed to have more votes than other voters and also the voting power has to be equally distributed. This principle prompts governments to see that all parties and candidates have the same chance to be elected. Furthermore, the Venice Commission explicitly addresses national minorities, and thus recommends and permits special rules and exceptions for them.

From the perspective of e-voting, this right is very important but also carries with it an obligation that has been critically discussed. It is expected that the introduction of a new electronic channel for participating in elections might address a certain class of population more than others. This effect is called the "Digital Divide". Thus, it is expected that Digital Divide might doubtlessly influence the result of an election and might give an advantage to some parties and candidates more than others.

Klaus Poier[4] analysed voters' behaviour especially with regards to the introduction of remote voting mechanisms such as e-voting and postal voting. He addressed the aspect of the Digital Divide as well and states that different classes of population—different with respect to income, education as well as cultural and social heritage—might lead to a divide into "Users" and "Losers" and "Information Haves" and "Information Have-Nots":

> *Unterschiedliche Voraussetzungen (Einkommens- und Vermögensunterschiede, Bildungsniveau, generationsspezifische Kulturunterschiede) führen zu einer "digitalen Klassentrennung (Digital Divide)" in "User" und "Loser" bzw in "Information Haves" und "Information Have-Nots". [14].*

Based on surveys conducted in Germany and Austria, whereas in Germany postal elections are widely used, he concluded that significant differences between proportional results of remote voting and conventional voting might be expected as long as remote voting remains exotic. However, with increasing acceptance of remote voting mechanisms, the differences are expected to disappear. For instance in Germany, postal voting is an established way to vote; more than 20% of German voters make use of it regularly. Thus, the proportional result of remote voters is nearly the same as the proportional result of conventional voters.

So it is particularly important to address "equality" when introducing any new form of voting, such as e-voting. However, this aspect should not lead to hesitation about introducing new channels and mechanisms for elections. It should rather be seen as an encouragement to have targeted initiatives in order to increase awareness about new election mechanisms and to foster their acceptance.

Free Suffrage

This entails:

> *Freedom of voters to form an opinion*
> *[..]Freedom of voters to express their wishes and action to combat electoral fraud*
> *[11]*

This passage of the Code of Good Practice is a more detailed description of the right for free elections as stated in the first additional protocol of the European Convention for Human Rights and Fundamental Freedoms. It lays down a set of rules for governments and the authorities that conduct the election. For example, the authorities and the government have to be neutral with respect to the funding of candidates and parties, billposting and media presence. Furthermore, the authorities have to treat all candidatures equally and to make appropriate announcements of the lists and candidates to be elected. The form and the chosen languages of these announcements have to address national minorities as well.

In addition to the general requirements regarding the way a voter can form her opinion, the Code of Good Practice defines fifteen specific conditions that direct how a voter should be able to express her decision. To mention only a few of these conditions: the Venice Commission requests that the voting procedure must be simple, that a voter must always have the possibility to vote in a conventional polling station and it clearly defines how and under which circumstances other means of voting are acceptable.

[4] Univ.Ass.Dr. Klaus Poier, Department for Staats- und Verwaltungsrecht at the University Graz (Austria).

With regards to remote voting, the Code of Good Practice explicitly names e-voting as a possibility for free elections under certain circumstances:

> *[..]*
> *Freedom of voters to express their wishes and action to combat electoral fraud*
> *[..]*
> *iv. electronic voting should be used only if it is safe and reliable; in particular, voters should be able to obtain a confirmation of their votes and to correct them, if necessary, respecting secret suffrage; the system must be transparent;*
> *[..] [11]*

In addition to this claim, three more conditions are considered to be very relevant in terms of e-voting as they address counting and observation:

> *[..]*
> *vii. at least two criteria should be used to assess the accuracy of the outcome of the ballot: the number of votes cast and the number of voting slips placed in the ballot box; [..]*
> *x. polling stations must include representatives of a number of parties, and the presence of observers appointed by the candidates must be permitted during voting and counting; [..]*
> *xiii. counting must be transparent. Observers, candidates' representatives and the media must be allowed to be present. These persons must also have access to the records;*
> *[..] [11]*

These three conditions are particularly meaningful for e-voting systems, not only on an organisational level but also on a technical one. Condition (vii) suggests how counting should and could be observed at a minimum level and conditions (x) and (xiii) point out who should observe voting and counting. Since electronic voting systems do not appear to be very transparent to outside observers due to their technical nature, easily understandable metrics for observers must be considered from the very beginning when designing an e-voting system.

Secret Suffrage

This entails:

> *[..]*
> *a. For the voter, secrecy of voting is not only a right but also a duty, non-compliance with which must be punishable by disqualification of any ballot paper whose content is disclosed.*
> *b. Voting must be individual. Family voting and any other form of control by one voter over the vote of another must be prohibited.*
> *c. The list of persons actually voting should not be published.*
> *d. The violation of secret suffrage should be sanctioned.*
> *[..] [11]*

This condition of the Code of Good Practice is a more detailed expression of the human right to secret elections as stated in the first additional protocol of the European Convention for Human Rights and Fundamental Freedoms [9]. With respect to remote voting, this condition sets out clear requirements

with regards to “family voting”. Family voting occurs when members of a family are not free in their decision and/or cannot vote secretly (e.g. family members are influenced and observed by the father during voting). The problem of “family voting” is an imminent problem of remote voting at places that are not attended by election officials. Nevertheless, the Venice Commission does not explicitly prohibit remote voting due to this problem, it only requests governments to prohibit “family voting”, preferably by law, and to punish any violations.

For completeness, the term “remote voting” in general can be further broken down into “attended remote voting” and “unattended remote voting”. The former type of remote voting refers to remote voting in an attended environment. In this scenario, the voter is attended by another person or by any authority of public trust (e.g. by a mobile election commission). The latter form of remote voting is remote voting in the pure form, e.g. remote voting from home or from the office. The voter is not required to vote in front of any authority or third party.

Direct Suffrage

This entails:

> *[..]*
> *The following must be elected by direct suffrage:*
> *i. at least one chamber of the national parliament;*
> *ii. sub-national legislative bodies;*
> *iii. local councils.*
> *[..] [11]*

The requirement of direct suffrage is of fundamental importance in a country’s constitution and specifies what constitutes the country’s national bodies. This requirement claims that at least one chamber of the national parliament should be directly elected by voters. Other bodies, such as the head of state, can be—and are very often—indirectly elected through elected representatives of other bodies.

Frequency of Elections

This entails:

> *[..]*
> *Elections must be held at regular intervals; a legislative assembly’s term of office must not exceed five years.*
> *[..] [11]*

In addition to the other five principles, the Venice Commission additionally requires that elections should be held at reasonable intervals.

2.2 Austrian Adaption of International Fundamentals and its meaning to E-Voting

Austria "*is a democratic republic. Its laws proceed from the people.*"[5] As such, elections and democratic principles are of paramount importance in Austria's constitution and legislation. Furthermore, the "*European Convention for the Protection of Human Rights has been in force in Austria since 1958;*[6] *in 1964 it was incorporated entirely into the constitution.*"[7] This means that elections in Austria are based on the fundamentals given within the first additional protocol of the European Convention for the Protection of Human Rights.

The Austrian constitution defines democratic-political elections at several levels:

1. National Level
   - presidential election (defined in the Austrian constitution [15], Art 60 Abs 1 B-VG)
   - parliamentary election (defined in the Austrian constitution [15], Art 26 Abs 1 B-VG)
   - election of the Austrian representatives for the European Parliament (defined in the Austrian constitution [15], Art 23a Abs 1 B-VG)
2. Regional Level
   - election of regional parliaments (defined in the Austrian constitution [15], Art 95 Abs 1 B-VG)
3. Municipality Level
   - election of the municipal council (defined in the Austrian constitution [15], Art 117 Abs 2 B-VG)

With respect to the cardinal principles of elections, the Austrian constitution [15] requires more or less the same modus operandi for all these types of elections: the election must be secret and free, in accordance with the European Convention for the Protection of Human Rights. As an explanatory example, article 26 of the Austrian constitution requires for the election of the Austrian national parliament:

> *[..]*
> *Artikel 26*
> *(1) Der Nationalrat wird vom Bundesvolk auf Grund des* ***gleichen, unmittelbaren, persönlichen, freien und geheimen Wahlrechtes*** *der Männer und Frauen, die am Wahltag das 16. Lebensjahr vollendet haben, nach den Grundsätzen der Verhältniswahl gewählt.*
> *[..] [15]*

The emphasized text in article 26 requires equal, direct, personal, secret and free suffrage. The claims of equal, direct, free and secret suffrage are stated within the Code of Good Practice of the Venice Commission as well. The requirement of personal suffrage in this form is particular to the Austrian

[5] taken from "Parliamentary Democracy" as seen on the Website of the Austrian Foreign Ministry at http://www.bmeia.gv.at/view.php3?f_id=150&LNG=en&version=, 27 May 2007.

[6] European Convention for the Protection of Human Rights as well as its first additional protocol have been ratified through the national act BGBl. 1958/210 in 1958.

[7] taken from "Fundamental rights and freedoms" as seen on the Website of the Austrian Foreign Ministry at http://www.bmeia.gv.at/view.php3?f_id=150&LNG=en&version=, 27 May 2007.

constitution. It strongly expresses the requirement for a personal and uninfluenced decision by the voter. Thus, it might be comparable to the meaning of secret and free suffrage as required by the Venice Commission. In addition to the basic principles laid down by the constitution, each election event requires an additional statute that regulates the execution of the election. However, these additional statutes do not influence the cardinal principles of elections.

Amidst the background of these cardinal principles of Austrian elections the question arises: Is remote voting, especially in its electronic form, enabled by the Austrian law? This question is not easy to answer and it has to be discussed with respect to various aspects and at different levels.

In terms of the postal voting form of remote voting, this question can be easily answered, since postal voting is explicitly allowed by the Austrian constitution since 1 July 2007. This recent modification of the Austrian constitution anticipates of the outcome of the discussions of the past years regarding Austrian election fundamentals[8]. The following paragraphs discuss the possibility and the history of remote voting in Austria. The discussion starts by analysing Austrian election principles with respect to remote voting in general, and does not yet touch on explicitly allowing postal voting. This leads to interesting and notable opinions and interpretations of personal and secret suffrage. Finally, the discussion leads to the conclusion that any form of remote voting in Austria requires a modification of the constitution.

Before dealing with this question, the term remote voting has to be further clarified. According to the definitions given in section 2, different forms of remote voting have to be discussed separately. Remote voting under attendance—so called attended remote voting—is permitted by the Austrian law for most democratic political elections, i.e. presidential election, national parliamentary election, election of regional parliament, and under certain circumstances within the Austrian national territory. For national parliamentary elections and presidential elections, there are specific rules governing how and where remote voting may be conducted (even from abroad).

Considering attended remote voting within Austria, the law regulating the execution of elections for the Austrian national parliament [16] introduces in §73 (1) a "special election commission" (also called "flying election commission") which visits voters who are not able to come to a polling station (e.g. handicapped people or people in prison, hospital or similar institutions). This special election commission is available upon request and acts as an ordinary election commission of an ordinary polling station. Thus, there is no notable difference with respect to the election process apart from the location. On the other hand, if a voter is not able to vote in the election district of her polling station, the voter might apply for an "election card" which enables her to vote in any other election district in Austria, more precisely, at any other polling station.

However, both of these forms of remote voting are only applicable within Austrian territory. In July 2007, the Austrian law explicitly introduced postal voting, not only for voters abroad on election day, but also for voters in Austria. Since 2007, the applicable laws for conducting national parliamentary elections [16], presidential elections [17] and elections for the European parliament [18] clearly mention and regulate postal voting as an alternative form of voting.

Before the explicit introduction of postal voting in 2007, Austrian law only permitted a special variation of postal voting, called "qualified postal voting"[9], for voters abroad in the event of national parliamentary and presidential elections. Qualified postal voting refers to an attended form of remote voting but does

[8] Before July 2007, the Austrian constitution did not explicitly allow voting by mail. Furthermore, due to the election principles defined within the Austrian constitution, remote voting would not be allowed at all. The discussion held in this section points out that due to Austrian election principles, remote voting requires a modification of the constitution.

[9] "qualified postal voting" according to the statement of Dr.Thomas M. Buchsbaum in [19]

not necessarily mean in front of an election commission. So if the voter was not able to visit an Austrian embassy or consulate to cast her vote, the voter had to find a foreign notary or comparable institution or person, or at least another Austrian full-aged citizen to witness that she made her vote under the terms set down in Austrian law. The witness had to assert that the voter was not influenced and that the vote cast was her personal vote according to the requirement of personal suffrage. Finally, the voter had to put her vote into a prepared envelope—under the attendance of the witness—which had to be signed by both the voter and the witness. The voter had to send the envelope containing her vote to the election authority in Austria. Due to the required signature of a witness, this form of postal voting is referred to as qualified postal voting.

Austrian law offered this special form of postal voting to voters abroad only. This led to the remarkable situation that an Austrian citizen living abroad was able to cast a vote in the election for the regional parliament in Lower Austria, for example[10], since the law laying down the details for this election allows qualified postal voting from abroad. However, a citizen of the region of Lower Austria who was still in the country but not present in Lower Austria on election day was not able to vote; neither using an election card (due to the requirement that election cards can be cast in polling stations in Lower Austria only) nor by any other means[11].

Before the reformation of Austrian electoral law in 2007, an attempt to introduce postal voting in its unattended form had already taken place. The government of Lower Austria tried to extend the law in order to enable unattended postal voting for elections of municipality councils. However, this attempt failed due to a negative judgment by the Constitutional Court of Austria (Verfassungsgerichtshof - VfGH). The judges found on 16 March 1985 that unattended remote voting—in the form of postal voting—is incompatible with the requirements of secret, free and personal suffrage as required by the Austrian constitution. The most important statements of this judgment are discussed below, with the relevant parts having been translated.

> *[..] Die Bundesregierung macht - kurz zusammengefaßt - geltend, daß die angefochtene (Briefwahl-)Regelung zum einen dem Grundsatz der "geheimen" Wahl widerspreche, zum anderen das Prinzip der "persönlichen" Wahl verletze.*
> *[..]*
> *Sie ist nach beiden Richtungen hin im Recht.*
> *[..] [21]*

The judgment can be reduced to two sentences: the Constitutional Court agrees on the claim of the Federal Government (the Federal Government brought charges against Lower Austria) that postal elections are not in accordance with the requirements for elections as laid down by the Austrian constitution. The judges commented their decision as follows:

> *[..] "Geheim" in der Bedeutung des Art26 Abs1 B-VG und der [..] Norm des Art117 Abs2 Satz 1 B-VG ist ein Wahlrecht nur dann, wenn der Wähler seine Stimme derart abzugeben vermag, daß niemand, weder die Behörde noch sonst jemand, erkennen kann, wen er gewählt*

[10] Lower Austria: a state of the Federal Republic of Austria

[11] this example fits the commentary of Christoph Drexler: "*Das derzeitige Wahlrecht führt z.B. dazu, dass Wahlberechtigte bei Landtagswahlen, die sich am Wahltag nicht in ihrem Heimatbundesland aufhalten, nicht an der Wahl teilnehmen können, weildas Gesetz nur die Stimmabgabe vor einer Wahlbehörde erlaubt. Trotz Wahlkarte muss der Wähler in sein Bundesland reisen. Dies führt zur kuriosen Situation, dass man zwar bei Nationalratswahlen seine Stimme beispielsweise in Washington DC oder Ulan Bator abgeben kann, bei steirischen Landtagswahlen aber eine Stimmabgabe schon in Völkermarkt oder Klagenfurt unmöglich ist.*" in [20]

> *hat ([..]). Demgemäß verlangt der Grundsatz des geheimen Wahlrechts wirksame Vorkehrungen zur Geheimhaltung des Wahlverhaltens des einzelnen Wählers ([..]), der seinerseits zur geheimen Stimmabgabe verpflichtet und von der Wahlbehörde dazu anzuhalten ist. [..]*
> *[21]*

Secret suffrage—as defined in the Austrian constitution [15], in Art.26 Abs.1 B-VG—requires that a voter must be able to cast her vote in a way that neither the authority nor anybody else is able to learn her decision. Therefore, there is a need for effective provisions supporting the voter in keeping her vote secret. Keeping the vote secret is the obligation of both, the voter and the authority which has to encourage the voter to do so.

> *[..] Der Landesgesetzgeber wälzt die kraft Verfassungsrechtslage ihm selbst zukommende Aufgabe, dafür wirksam Sorge zu tragen, daß die Wahl (Stimmabgabe) geheim vor sich gehe, einzig und allein auf den - vor unzulässiger Einflußnahme auf seine Wahlentscheidung zu schützenden - Wähler ab; es fehlt nämlich [..] an Sicherheitsvorkehrungen, die dem Wahlberechtigten eine "geheime", das ist die unbeeinflußte und unbeobachtete Ausfüllung des Stimmzettels garantieren. [..]*
> *[..] Daß der Wähler nachträglich schriftlich bestätigen soll, er habe den Stimmzettel persönlich unbeobachtet ausgefüllt, ist aus der Sicht der Gewährleistung geheimer Wahlen im bereits dargelegten Sinn ungenügend. [..]*
> *[21]*

The Constitutional Court interprets the introduction of postal voting—as proposed by the electoral law of Lower Austria—as an attempt to transfer the responsibility of ensuring the secrecy of the vote to the voter. The court further claims that the authority has to protect the voter from being influenced or manipulated while casting her vote and thus has to ensure secret suffrage. Asking the voter to assert that she was not influenced or observed while casting her vote is not acceptable as a sufficient enough alternative.

> *[..] Im engsten Zusammenhang mit dem Grundsatz der "geheimen" Wahl steht das gleichfalls in Art117 Abs2 B-VG festgeschriebene Prinzip des "persönlichen" Wahlrechts. [..]*
> *[..] Das im B-VG (Art26 Abs1,95 Abs1 und 117 Abs2; 60 Abs1) für Wahlen zu allgemeinen Vertretungskörpern expressis verbis verankerte Persönlichkeitsprinzip gebietet die Schaffung von Wahlordnungen, die zwingend sicherstellen, daß alle zu zählenden Stimmen wirklich von jenen Personen stammen, die sie abgaben. Das bedeutet folgerichtig, daß ein "persönliches" Wahlrecht, wie es das B-VG festlegt, das persönliche Erscheinen, anders ausgedrückt: die physische Präsenz des Wählers, sei es im Stimmlokal, sei es vor einer sog. "fliegenden" oder sonst inner- oder außerhalb des Wahlgebiets amtierenden Wahlkommission oder einem die Aufgaben einer solchen Kommission adäquat besorgenden Staatsorgan, zur Teilnahme an der Wahl notwendig voraussetzt. [..]*
> *[21]*

The Constitutional Court further criticises postal voting against the background of personal suffrage as required by the Austrian constitution [15]. The Constitutional Court interprets the requirement of personal suffrage granted by the Austrian constitution as being satisfied only if the voter cast her vote while attended by an election commission (of any form) or by any other institution or person of public trust that may adequately act in place of an election commission.

To summarize the decision, the judges of the Constitutional Court in 1985 did not accept any form of unattended postal voting which made e-voting impossible, as both unattended postal voting and e-voting are similar remote voting mechanisms with respect to their legal aspects. The interpretation of personal and secret suffrage by the Constitutional Court heavily influenced the legal opinion on postal voting—or unattended remote voting in general—in Austria for many years. Moreover, this interpretation was remarkable especially in comparison to the international legal situation.

The Austrian constitution fully relies on the European Convention for Protection of Human Rights, thus it fully implements the requirements given by the first additional protocol with respect to elections. The fact that there are different interpretations of the requirement of secret suffrage amongst European countries shows that it is quite possible to reconcile secret suffrage and postal elections. For instance, both the Austrian constitution and the German constitution require secret suffrage. In contrast to the view of the Austrian Constitutional Court, the German courts do not see a contradiction between secret suffrage and remote elections in form of postal elections[12]. Furthermore, many other democratic states following the same democratic principles have effectively implemented postal voting. This illustrates a certain scope of discretion and margin of appreciation which is fully compliant with the European Convention. There is no normative interpretation of election principles; states are enabled to interpret these principles if they consider it necessary.

However, the European Convention for the Protection of Human Rights and its first additional protocol do not consider remote voting through postal voting as being not compliant with their cardinal principles[13]. Moreover, the Code of Good Practice in Electoral Matters [11] explicitly names postal voting as a mechanism for voting under certain circumstances:

> *[..]*
> *38. Postal voting and proxy voting are permitted in countries throughout the western world, but the pattern varies considerably. Postal voting, for instance, may be widespread in one country and prohibited in another owing to the danger of fraud. It should be allowed only if the postal service is secure - in other words, safe from intentional interference - and reliable, in the sense that it functions properly. [..]*
> *39. Neither of these practices should be widely encouraged if problems with the postal service are added to other difficulties inherent in this kind of voting, including the heightened risk of "family voting". Subject to certain precautions, however, postal voting can be used to enable hospital patients, persons in custody, persons with restricted mobility and electors residing abroad to vote, in so far as there is no risk of fraud or intimidation. This would dispense with the need for a mobile ballot box, which often causes problems and risks of fraud. Postal voting would take place under a special procedure a few days before the election.*
> *[..] [11]*

The legitimacy of postal voting may directly influence the legitimacy of e-voting since both forms of remote voting are an unattended form of remote voting. But even with respect to e-voting, the convention and its first additional protocol does not ban e-voting. In fact, the Code of Good Practice names electronic voting as a possibility under certain circumstances:

[12] This conclusion is in accordance with the statement of Univ.Prof.DDr.Christoph Grabenwarter as given in [13]

[13] See also Christoph Grabenwarter's statement in [13]: "*Eine explizite Vorgabe oder gar ein Hindernis hinsichtlich der Einführung von Briefwahlrecht oder e-voting lässt sich aus Art 3 1. ZPEMRK aber nicht ableiten.*"

[..]
3.2.2.3. Mechanical and electronic voting methods
42. Several countries are already using, or are preparing to introduce mechanical and electronic voting methods. The advantage of these methods becomes apparent when a number of elections are taking place at the same time, even though certain precautions are needed to minimise the risk of fraud, for example by enabling the voter to check his or her vote immediately after casting it. Clearly, with this kind of voting, it is important to ensure that ballot papers are designed in such a way as to avoid confusion. In order to facilitate verification and a recount of votes in the event of an appeal, it may also be provided that a machine could print votes onto ballot papers; these would be placed in a sealed container where they cannot be viewed. Whatever means used should ensure the confidentiality of voting.
43. Electronic voting methods must be secure and reliable. They are secure if the system can withstand deliberate attack; they are reliable if they can function on their own, irrespective of any shortcomings in the hardware or software. Furthermore, the elector must be able to obtain confirmation of his or her vote and, if necessary, correct it without the secrecy of the ballot being in any way violated.
44. Furthermore, the system's transparency must be guaranteed in the sense that it must be possible to check that it is functioning properly.
[..] [11]

Although the Venice Commission does not explicitly address remote e-voting, it names electronic voting methods as being adequate technical possibilities. This in connection with the fundamental position of the Venice Commission on remote voting—expressed in their position on postal voting—allows the conclusion that remote e-voting is not in conflict with European election fundamentals. To emphasise this, the European Council initiated an Multidisciplinary Ad Hoc Group of Specialists on Legal, Operational and Technical Standards for e-enabled voting[14] which created recommendations and standards regarding the legal, organisational and technical aspects of e-voting [3] [4]. These standards address the following (section 5.1 dissects these recommendations in detail):

[..]

- *The legal standards relate to the legal context in which e-voting is permitted.*
- *The operational standards relate to the manner in which e-voting hardware and software should be operated and maintained.*
- *The technical requirements relate to the construction and operation of e-voting hardware and software. The adoption of the technical requirements will ensure the technical security, accessibility and interoperability of e-voting systems.*
- *The three categories of standards all include provisions relating to all stages of elections and referendums, (i.e. the pre-voting stage, the actual casting of the vote, and the post-voting stage).*

[..] [4]

Although remote voting—postal voting or e-voting—is not banned by international law, the interpretation of the Constitutional Court of the Austrian election principles did not see any possibility for postal voting or any other form of unattended remote voting without changing the Austrian constitution.

[14] The author of this thesis contributed to the work of the technical sub-group.

However, due to increasing international acceptance of remote voting methods, a legal discussion about this topic has been started in Austria. Leading legal experts demanded more and more to modify the Austrian constitution in order to have a clear commitment to remote voting and e-voting in particular. On 30 June 2003, the Austrian Convention[15] was introduced. The convention aimed at discussing and elaborating on proposals for a reformed constitution. The convention sent its final report to the Austrian parliament on the 3 May 2005. Although election fundamentals have been heavily discussed, the final report addressed neither postal voting nor e-voting in particular. However, the discussions within the convention prompted a lot of further actions. The legal developments reached their height in July 2007: the modification of the Austrian constitution explicitly allowing postal voting was put into force. Now, the constitution makes a clear statement on postal voting.

In parallel with the Austrian Convention, the Austrian Ministry of the Interior initiated a working group which elaborated on the requirements for introducing e-voting in Austria. The working group was divided into three groups of experts: a sub-group for international influences of e-voting; a second sub-group for legal requirements and a third sub-group for technical requirements[16]. As an outcome, the working groups created a combined report [22]. The main statements and requirements for introducing e-voting in Austria—especially with respect to the legal perspective—can be summarized as follows [22][17]:

- E-voting, as well as postal voting, can be introduced as long as the Austrian constitution redefines the requirements of secret and personal suffrage.
- Any technical e-voting system has to ensure that election principles are complied with.
- Analogous to the conventional election system, an electronic voting system has to ensure that casting, opening as well as counting of votes can be easily observed by the members of the election commission. Furthermore, the cast votes must only be accessible after a collaborative action of the election commission.
- Before a nationwide deployment of e-voting within one of the major elections, e-voting should be "tried" on a smaller scale. Austrian law does not allow remote voting for political democratic elections in general, but it does allow e-voting for the election of the representation of interests (Austrian Chambers) and the Austrian National Union of Students. Both of these elections would prove excellent subjects for test elections.
- E-Voting should always remain as an alternative to conventional elections. There must always be the possibility to vote using paper ballots.

To summarize, e-voting in Austria is considered to be possible from a legal point of view, at least for some elections. There exists a common view amongst legal experts that the definition and interpretation of Austrian electoral principles, the principles of personal and secret suffrage in particular, as required for democratic political elections have to be reconsidered. Moreover, since the current interpretation of secret suffrage is much more stringent than is required by the European Convention for Protection of Human Rights, this interpretation should be eased. For example, German legislation requires secret suffrage as well, but in contrast to Austria, Germany has allowed remote voting through postal voting for years. Furthermore, German legislation considers that universal suffrage can be achieved as soon as

[15] See http://www.konvent.gv.at

[16] The author of this thesis was a member of the technical working group and assistant to the coordinator.

[17] Section 5.2 outlines this report and its sub-reports in more detail.

postal voting is fully deployed[18]. Considering the election turnout in Germany, more than 18 percent of German voters make use of postal voting.

Although the Constitutional Court's interpretation of the Austrian election principles does not give any room for unattended remote voting methods like e-voting within democratic political elections—such as parliamentary elections, presidential elections, elections for the European parliament, elections for the local government and elections of the municipality council—the explicit allowance of postal voting by the new modified constitution is trend-setting for e-voting.

However, an indication that e-voting is nevertheless an important issue to government and politics is that the current programme of the Austrian government [23] explicitly mentions further testing of e-voting methods[19] as an action point. For proving e-voting methods, real test elections using e-voting technologies would be promising, for example in the course of elections for the Austrian National Union of Students. The loosening up of the Austrian constitution towards postal voting is a step into the right direction.

Finally, e-voting could be introduced after some minor changes to the Austrian electoral law in accordance with European election principles are enacted, but it has to be kept in mind that in the end these election principles have to be guaranteed by (technical) security standards and mechanisms provided by the underlying e-voting system in an exhaustive and sufficient way[20].

2.3 E-Voting in Austria - a Legal Perspective

Although the Austrian constitution does not explicitly allow e-voting for democratic political elections—like parliamentary election at national or regional level, presidential elections or elections of municipality councils—it does allow for e-voting for specific types of elections.

Austrian law demands the regular election of representatives for various legally recognized unions and chambers. Although these elections do not directly influence the democratic processes of Austria, they are nonetheless still political in nature. However, elections of this kind are:

- Elections for Austrian Chambers
- Elections for the Austrian National Union of Students

Both of these types of elections are not regulated in detail by the Austrian constitution, thus personal suffrage is not required on the same stringent level as other elections. Moreover, the laws regulating the concrete execution of these elections explicitly define how to vote electronically.

Both elections have to be fully compliant with elections principles, especially with general election principles as stated within the Code of Good Practice of the Venice Commission. Since both are large scale elections, they touch on all aspects of democratic political elections, and thus are comparable with other

[18] See statement of Christoph Drexler: "*[..] der Überlegung folgte, dass das allgemeine Wahlrecht erst durch die Briefwahl vollständig verwirklicht wird.*" on p.122 in [20]

[19] See section "Staats- und Verwaltungsreform", sub-section 5 of [23]: "*[..] Prüfung der elektronischen Stimmabgabe (E-Voting) [..].*"

[20] See concluding statement of Christoph Grabenwarter in [13]: "*[..] Wenn nun [..] der zulässige Schluss gezogen wird, dass bestimmte Formen der Briefwahl und auch des e-voting nach europäischem Recht zulässig sind, darf nicht verkannt werden, dass diese Zulässigkeit stets unter dem Vorbehalt ausreichender Sicherheitsstandards im Wahlverfahren stehen.*"

elections at all levels. This was the reason why the final report of the working group of the Austrian Ministry of Internal Affairs recommended "testing" e-voting using one of these elections.

The e-voting system presented by this thesis was designed to be used within one of these elections. Not only due to the recommendation of the ministry's working group report but also due to the existence of clear legal regulations. The intention was to design an e-voting system in accordance with real requirements, thus the resulting e-voting system targets one of these elections. The design focused on the election for the Austrian National Union of Students since this election was judged most likely to occur first[21]. Although targeted at this specific election, the resulting e-voting system aimed to be fully compliant with the election fundamentals set out by the European Convention for the Protection of Human Rights and its first additional protocol, the Code of Good Practice of the Venice Commission and the Austrian constitution (but not following the interpretation of the requirements of secret and personal suffrage of the Austrian Constitutional Court). In other words, in the event the Austrian constitution becomes more relaxed toward the acceptance of e-voting, the e-voting system presented by this thesis is already designed to suit the need immediately.

In order to determine the requirements for the e-voting system to be developed, this section examines and discusses the regulative law in detail. The act regulating the Austrian National Union of Students (HSG98) [24] does not only define the foundation of the Austrian National Union of Students but also defines the legal basis as well as the fundamental process model for the election of representatives of the students union. In particular, §34 and §39 of [24] describe the election procedure in detail. The following segments cite and outline the most relevant parts of these paragraphs. Since the act is available in German only, here are the main statements of this paragraph.

Passages 1 to 7 of paragraph §34 define the requirements for conducting the election electronically in detail:

> *[..]*
> *§ 34 (1) Die Wahlen in die Bundesvertretung und die Organe gemäß § 12 Abs. 2 sind alle zwei Jahre durchzuführen, die Wahlen in die Studienvertretungen und die Universitätsvertretungen sind alle zwei Jahre für ganz Österreich gleichzeitig auf Grund des allgemeinen, gleichen und geheimen Verhältniswahlrechtes gesondert für jedes dieser Organe durchzuführen. Das Wahlrecht ist persönlich auszuüben.*
> *[..] [24]*

Passage (1) says that elections have to be conducted every two years at all universities in Austria at the same time. The principles of the election are:

1. universal
2. equal
3. free
4. secret
5. personal

[21] At the time of writing, concrete plans to deploy the e-voting system for the Austrian National Union of Students election existed

[..]
§ 34 (3) Bei Hochschülerschaftswahlen sind amtliche Stimmzettel zu verwenden. Für die Beurteilung der Gültigkeit von Stimmen und die Form der Stimmabgabe sind die Bestimmungen der Nationalrats- Wahlordnung 1992, BGBl. Nr. 471, anzuwenden.
[..] [24]

Passage (3) declares that the ballots used have to be official ballots. Furthermore, the verification of cast votes must happen in accordance with the legislation regarding national parliamentary elections.

[..]
§ 34 (4) Abweichend von Abs. 3 ist bei der Durchführung der Wahlen auf elektronischem Weg die Abgabe der Stimme den Wahlberechtigten auf elektronischem Weg zu ermöglichen. Das zum Einsatz kommende System muss den Sicherheitsanforderungen elektronischer Signaturen gemäß dem Signaturgesetz entsprechen und unter Berücksichtigung der Anforderungen des Datenschutzgesetzes 2000 an die Datensicherheit so ausgestaltet sein, dass die Einhaltung aller in Abs. 1 aufgezählten Grundlagen und die Erfüllung der in § 39 Abs. 1 festgelegten Aufgaben der Wahlkommission auch bei der elektronischen Wahl gewährleistet ist.
[..] [24]

Passage (4) allows electronic voting as long as the requirements stated in passage (2) are fulfilled. It requires that the technical systems used have to meet the requirements stated by the Data Protection Act [25] and the Act on Electronic Signatures [26]. Furthermore, the election commission must be able to carry out its duties as defined in paragraph §39 of [24].

[..]
§ 34 (5) Insbesondere ist folgendes durch geeignete Ausgestaltung des eingesetzen Verfahrens zu garantieren:

1. *Wahrung des Wahlgeheimnisses durch Methoden, die gewährleisten, dass die ausgefüllten Wahlformulare anonymisiert und nicht rückverfolgbar bei den Wahlkommissionen zur Auszählung gelangen; es darf zu keinem Zeitpunkt durch die Wahlkommission oder durch Dritte eine Zusammenführung der Identität der Wählerin oder des Wählers mit ihrem oder seinem Wahlverhalten möglich sein;*
2. *Verifikation der Identiät der oder des Stimmberechtigten gegenüber der Wahlkommission im Rahmen des Wahlvorganges vor der Übermittlung des Wahlformulars, damit die Stimmabgabe durch Nichtberechtigte und die Abgabe mehrerer Stimmen durch eine Person ausgeschlossen ist. Es dürfen nur jene personenbezogenen Daten verwendet werden, die zur Durchführung der Wahl notwendig sind;*
3. *Unverfälschtheit des ausgefüllten Stimmzettels durch den Einsatz elektronischer Signaturen und die Geheimhaltung der Wahldaten während der Übertragung zur Wahlkommission durch Verschlüsselung dieser Daten zur Sicherstellung des Wahlgeheimnisses;*
4. *Möglichkeit der Wahlkommission, alle ihr in diesem Gesetz übertragenen Aufgaben auch hinsichtlich der elektronischen Stimmabgabe durchführen zu können;*
5. *Berücksichtigung des Übereilungsschutzes für die Wählerin oder den Wähler wie bei der herkömmlichen Stimmabgabe;*

6. *Erfüllung aller an Wahlzellen gestellten Anforderungen auch durch die in universitären Räumlichkeiten aufgestellten technischen Komponenten zur Abgabe der Stimme und die Verpflichtung der Wahlberechtigten durch die Wahlordnung zum unbeobachteten, unbeeinflussten und persönlichen Ausfüllen der Wahlformulare.*

[..] [24]

Passage (5) further defines detailed requirements for the electronic election system used:

1. The cast ballots have to be anonymous. Neither the election commission/authority itself nor any other third party is able to reveal the identity of a voter by the cast ballot.
2. The voter has to be identified, authenticated and authorised to vote before casting her vote. The system must prevent unauthorised persons from voting as well as double-voting.
3. The system must protect filled in votes from being manipulated by applying electronic signatures. Furthermore, the election system has to encrypt votes before transmitting them from voters to the election commission.
4. The voting system must provide functionality to allow the election commission to carry out its duties.
5. The election system has to protect the voter against casting her vote precipitately.
6. If electronic voting components are put in place at the university, they must follow the same requirements as conventional voting booths. Electronic voting components have to guarantee that the voter can make her decision and cast her vote unobserved, uninfluenced, personally and secretly.

[..]
§ 34 (6) Die bei der Wahlkommission eingesetzten technischen Komponenten und die Komponenten, die unmittelbar zur Stimmabgabe und zur Verifikation der Identität verwendet werden, müssen nach dem Stand der Technik hinreichend und laufen geprüft sein. Die Erfüllung der Sicherheitsanforderungen muss von einer Bestätigungsstelle gemäß § 19 Signaturgesetz bescheinigt sein. Diese Bestätigungsstelle spricht auch Empfehlungen für die anderen technischen Komponenten aus, die bei der Abgabe der Stimme eingesetzt werden.
[..] [24]

Passage (6) requires that technical components used to identify voters and handle cast votes must be state of the art. Furthermore, this passage explicitly demands that the core components as well as the environmental elements of the voting system have to be verified by a confirmation body as defined by the Austrian Signature Act [26] to be adequately secure.

[..]
§ 34 (7) Nähere Bestimmungen über die Durchführung der Wahlen auf elektronischem Weg sind in der Verordnung gemäß § 48 (Wahlordnung) festzulegen.
[..] [24]

The last passage, passage 7, of the most relevant paragraph requires that any further requirements for conducting the election electronically have to be defined in detail and specify the administrative order

(each such election is accompanied by an administrative order which lays down the detailed regulations for conducting the election).

Considering §34 in all its aspects, most of the requirements stated in §34 are in full accordance with the common good practices for electronic elections. However, two issues are notable, issue 3 and issue 6 of passage (5). Issue 3 explicitly mentions electronic signatures as a technical measurement in order to prevent manipulation of (cast) votes. Although the use of electronic signatures seems to be obvious, to require its use by law would exclude alternative technologies. On the other hand, if this requirement leads to asking the voter to sign her vote before casting, the vote becomes branded with the voter's electronic signature and her certificate. However, the bottom line is that it is important to understand the principle behind this requirement. The issue is to prevent a vote from being tampered with after leaving the voter's environment. The use of electronic signatures makes sense for this purpose. Issue 6 requires that the e-voting system has to be verified by an independent confirmation body. The confirmation body should verify that the e-voting system is adequately secure and is compliant with the principles given by law. This requirement is very important as it leads to an independently approved voting system. An independently approved system is also more likely to be trusted.

A mandatory inspection in combination with a set of system-independent principles should be the legislative basis for any technical e-voting solution. Therefore, requiring certain technical measures by law, such as the use of electronic signatures as discussed before, might be too restrictive[22].

To define a set of technologically neutral requirements to verify whether a certain technical solution is in compliance is a standard instrument of risk management. Several well defined and standardised methodologies exist that do so, such as Common Criteria (CC)[23], ITSEC, etc. Common Criteria is one of the most used methodologies today. Protection Profiles are a speciality of Common Criteria. Protection Profiles are a standardised method for defining security objectives and requirements for a certain technical solution in a system independent way. By creating internationally standardised Protection Profiles, it is possible to ensure that all technical implementations/systems which are deemed to be compliant with a certain Protection Profile will fulfill the stated requirements. For example, the internationally accepted Protection Profile for Secure Signature Creation Devices (SSCD-PP) [27] [28] ensures that every smart card which is compliant with the SSCD-PP can be used to hold and create legally accepted secure electronic signatures according to the European Directive on Electronic Signatures [29]. Moreover, due to the Common Criteria schema and its international mutual recognition agreements (on a national level), it would be possible for an e-voting system developed by a vendor in the United Kingdom, which complies with a standardised Protection Profile for voting system as asserted by a German confirmation body, to be used immediately in Austrian elections if the Protection Profile applied covers all requirements stated by law. If a sufficiently standardised Protection Profile ever exists, it would be advisable to take it up and mention it in legislation.

In anticipation of the exhaustive discussion given in section 5, there is no fully complete Protection Profile for electronic voting systems available at the moment. The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI) developed a rudimentary Protection Profile for the core aspects of electronic election systems[24]. This Protection Profile is intended to be used to verify election systems for elections of board representatives of registered associations (for more

[22]The requirements given by law should be limited to claiming abstract objectives only. Preliminary technical decisions should be prevented; more detailed conditions could be formulated in the administrative order as required by passage (7) of §34 [24]

[23]Common Criteria; see http://www.commoncriteriaportal.org

[24]The author of this thesis was actively involved and a member of the advisory board.

information about this Protection Profile; see section 5.3). Although the core principles of elections have been addressed, the resulting Protection Profile lacks in completeness as it concentrates on the election phase only and makes assumptions which are indefensible with regards to large political elections. However, this Protection Profile can be seen as a good foundation; further and more comprehensive Protection Profiles have to be developed. In order to have a basis for a comprehensive Protection Profile, the Council of Europe[25] drafted the Security Recommendations and Best-Practices for e-enabled voting in the style of Protection Profiles. Thus, the technical security recommendations of the Council of Europe could be used to elaborate on the existing Protection Profile or to create a new one.

In addition to the definitions in paragraph §34, paragraph §39 of [24] defines the organisational duties and requirements for the election commission. The e-voting system has to comply these duties and requirements.

> *[..]*
> *§ 39 (1) Den Wahlkommissionen bei den Hochschülerinnen- und Hochschülerschaften an den Universitäten obliegen:*
>
> 1. *Feststellung der Zahl der für jedes Organ zu vergebenden Mandate,*
> 2. *Prüfung der Wahlvorschläge,*
> 3. *Leitung der Wahlhandlung,*
> 4. *Prüfung der Identität und der Wahlberechtigung der Wählerinnen und Wähler,*
> 5. *Entgegennahme der Stimmzettel und Entscheidung über die Gültigkeit der abgegebenen Stimmzettel,*
> 6. *Feststellung des Wahlergebnisses,*
> 7. *Zuweisung der Mandate an die wahlwerbenden Gruppen und die Kandidatinnen oder Kandidaten für die Studienvertretungen,*
> 8. *Verständigung der gewählten Mandatarinnen und Mandatare,*
> 9. *Verlautbarung des Wahlergebnisses,*
> 10. *bescheidmäßige Feststellung des Erlöschens von Mandaten gemäß § 43 und nachträgliche Zuweisung von Mandaten an Personen gemäß §§ 41 und 42,*
> 11. *Durchführung von Urabstimmungen gemäß § 50, wenn sie gemeinsam mit Hochschülerschaftswahlen stattfinden.*
>
> *[..] [24]*

Passage (1) of paragraph §39 enumerates the duties of the election commission in detail. With respect to the execution of the election, the relevant duties are:

1. determining the number of assignable mandates
2. proving of candidate nominations (election proposals)
3. steering of the whole election process

[25] The author of this thesis was actively involved in the Group of Specialists on core technical standards for e-enabled voting; a description of this work is given in section 5.1

4. proving the identity and right to vote of voters
5. collecting ballots and proving their validity
6. creating the election result
7. assigning mandates to the candidates and lists according to the result
8. notification of elected candidates
9. announcement of the result

These duties are the activities of the election commission for the election of the Austrian National Union of Students. Thus, the process model of the e-voting system has to be fully compliant with these required duties and has to provide all necessary functionality so that the election commission is able to carry out its duties.

> *[..]*
> *§ 39 (2) Der Wahlkommission bei der Österreichischen Hochschülerinnenund Hochschülerschaft obliegt: 1. Organisation und Durchführung der Wahl von Studierendenvertreterinnen und Studierendenvertretern in die Bundesvertretung (§ 35a), 2. Zuweisung der Mandate für die Bundesvertretung, Entscheidungen über Einsprüche gemäß § 45.*
> *[..] [24]*

Passage (2) gives the election commission of the Austrian Union of Students the legal right to conduct elections. In other words, the election commission is empowered to organise and hold elections for representatives of the Federal Assembly of the National Union of Students. Furthermore, the election commission is empowered to assign mandates for the Federal Assembly of National Union of Students and it decides in the event of protests.

> *[..]*
> *§ 39 (3) Die Wahlkommissionen haben spätestens am achten Tag vor der Wahl die zugelassenen gültigen Wahlvorschläge in der Reihenfolge ihres Einlangens zu verlautbaren. Die Verlautbarung erfolgt durch öffentliche Bekanntmachung in den Räumen der Österreichischen Hochschülerinnen- und Hochschülerschaft und der Hochschülerinnenund Hochschülerschaften an den Universitäten sowie an den in den Bildungseinrichtungen gemäß § 1 Abs. 1 zur Verfügung zu stellenden Plakatflächen. Bei der Durchführung der Wahlen auf elektronischem Weg erfolgt die Verlautbarung zusätzlich im Internet durch die Österreichische Hochschülerinnen- und Hochschülerschaft . Im Gegensatz zur gedruckten Verlautbarung ist die im Internet bereitgestellte Version nicht authentisch.*
> *[..] [24]*

This third passage of paragraph §39 regulates the announcement of the election. This passage contains a specific reference to e-voting. It requires that if e-voting is used, the election commission has to announce the election on the Internet as well. This requirement does not directly influence an e-voting system, but it strongly indicates that the lawmakers considered electronic voting over the Internet as well.

[..]
§ 39 (7) Die oder der Vorsitzende der Wahlkommission hat die elektronische Wahl abzubrechen, wenn die Sicherheit oder Funktionsfähigkeit der bei der Wahlkommission eingesetzten elektronischen Komponenten während der Wahl beeinträchtigt ist. In diesem Fall hat die Wahlkommission unter Beiziehung einer Bestätigungsstelle gemäß § 19 Signaturgesetz über die Gültigkeit der vor dem Abbruch abgegebenen elektronischen Stimmen zu entscheiden.
[..] [24]

Passage (7) directly addresses e-voting. It states that the head of the election commission becomes the authority to strike e-voting if the security or functionality of the e-voting system is impaired. In this event, the election commission has to consult a confirmation body[26] as defined within the Austrian act on electronic signatures [26] and both have to decide about the acceptance and validity of the votes cast before the election was aborted.

In addition to the requirements laid down in §34, paragraph §39 defines clear responsibilities and duties for the election commission. In general, the election commission is responsible for preparing and conducting the election. It is also in charge of nominating candidates, announcing the election event and releasing all relevant information (e.g. location and opening time of polling stations, list of candidates, etc.), identifying eligible voters and confirming their right to vote, collecting and verifying all cast ballots, tallying the election result and assigning mandates to the candidates and list standing for election. Moreover, the law gives the election commission the power to stop e-voting in the event of a malfunction or security risk.

The law itself only outlines the fundamentals of an election. More detailed instructions are written in a special additional administrative order (the current administrative order is from the year 2005 [30]). This order regulates the execution of the election in detail. Although the law considers e-voting as a possibility, the current administrative order does not address e-voting at all. Thus, there is a need to modify the administrative order before introducing e-voting.

To summarize, the law regulating elections for representatives of the Austrian National Union of Students explicitly regulates the use of e-voting technologies. Paragraphs §34 and §39 of [24] in particular define organisational and technical requirements for these elections. From this perspective there is a legal possibility to introduce e-voting in Austria, at least for the types of elections mentioned in this section. Therefore, the election for the Austrian National Union of Students has been taken to be the target use-case for the e-voting system presented through this thesis.

[26] At the time of writing, the only confirmation body according to §19 SigG [26] is the Secure Information Technology Center - Austria (A-SIT).

Chapter 3

Existing E-Voting Schemes

This chapter[1] provides an overview on existing e-voting approaches from a cryptographic point of view. The first section deals with election phases; the pre-voting phase, the voting phase and the post-voting phase respectively, and thus introduces a schema to categorise e-voting systems based on phases. It introduces the main actors used in e-voting scenarios as well.

The last section of this chapter describes the three common ways the technical core of e-voting can be implemented. So-called e-voting schemes represent a technical and mathematical model underlying every e-voting implementation. Most of the existing schemes can be divided into homomorphic schemes, mixing net schemes and blind signature schemes, which make use of cryptographic principles and mechanisms to meet the requirements of a democratic election.

3.1 Categories based on Phases

From a conceptional perspective, e-voting can be split up into three phases:

- Pre-Voting Phase
- Voting Phase
- Post-Voting Phase

Considering e-voting systems in this way follows the high level models of election systems given by the Organization for the Advancement of Structured Information Standards (OASIS). The OASIS consortium specifies a so-called Election Markup Language (EML) [1] especially for the exchange of data within e-voting processes. EML bases on the Extensible Markup Language (XML) and is useful in particular for interoperability reasons. At the bottom of the definition of EML, OASIS lays a high level overview and a high level model dealing with the human view and a high level model dealing with the technical view. Figure 3.1 depicts the human model of an e-voting system as seen by EML. In this chapter, mainly this human view is taken as a basis for talking about e-voting systems from the conceptual point of view. The

[1] As a spin-off of this thesis, this chapter has been published on the Internet already: "E-Voting: A Survey and Introduction" [31], at http://www.a-sit.at/pdfs/evoting_survey.pdf (as seen on 20 April 2007).

following sections briefly outline the phases of e-voting as defined within this human model in order to categorise e-voting systems according to phases.

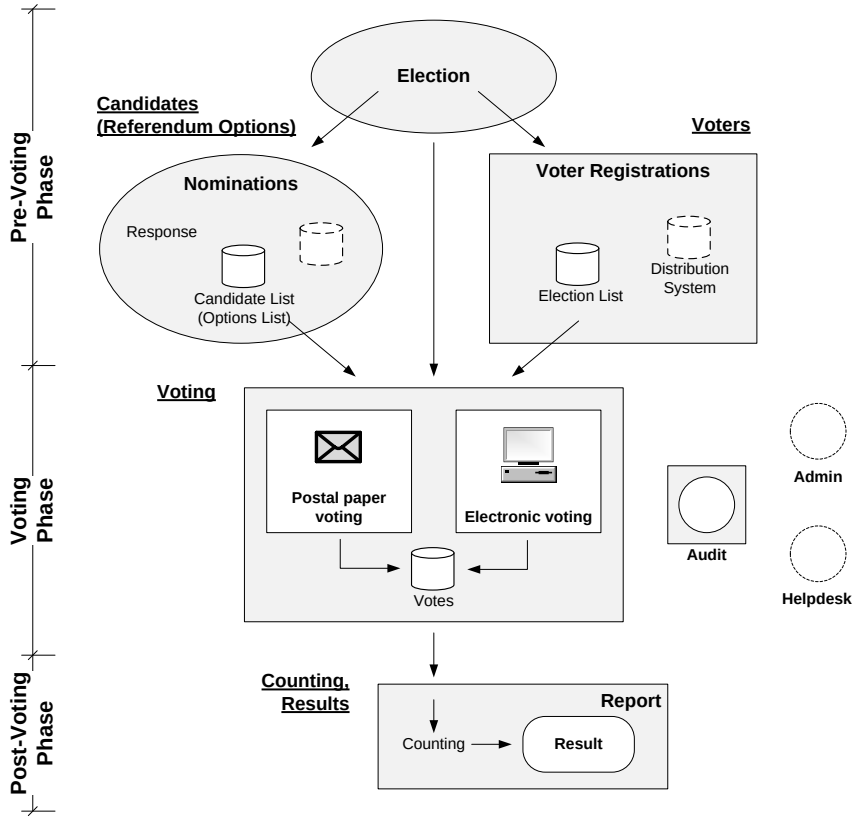

Figure 3.1: The human model stated by EML [1]

Pre-Voting Phase

As depicted in the human view of the OASIS high level model (see figure 3.1), the major tasks in this phase are:

1. Candidate Nomination Process
   - Candidate Nomination
   - Candidate Response
   - Generation of the Candidates List
2. Voter Registration Process
   - Voter Registration
   - Generation of the Election List

There may be various ways to become nominated as a candidate for election depending on the national legislative. A candidate has to meet some legal restrictions, e.g. she must be old enough, etc. The proposed candidate might have to accept her nomination. She has to decide whether to accept or decline her nomination. Finally, the nomination process results in a list containing all candidates, called the candidate list.

The EML model considers referenda as well. Thus, the model includes the referendum options nomination process in parallel to the candidate nomination process. In principle, they are quite similar despite the different legislative restrictions. Even the options nomination process leads to a resulting options list. In this chapter we limit our scope to elections only.

Depending on local law, voters may have to register to vote explicitly. In many countries citizens are registered for voting automatically. However, the result of this process is an election list containing all the persons that are allowed to vote.

Voting Phase

Based on the results of the pre-voting phase, the voting phase enables all eligible voters to make their decisions and cast their votes. Thus, by the use of the election list, the voter has to authenticate herself as an eligible voter and she has to cast her individual vote. The model presented in figure 3.1 does not limit voting to electronic voting only. It is the voter's decision to determine with which channel she prefers to cast her vote. However, the main scope in this thesis is the Internet as the electronic voting channel. Since the voter should have an alternative to e-voting and conventional voting with paper ballots must be provided in parallel, the model has to consider multiple possibilities. The interfaces and cutting edges between electronic and conventional elections have to be considered especially in the conceptual design.

Post-Voting Phase

The post-voting phase deals with the juicy parts of the e-voting process. This phase mainly covers counting and result reporting.

Counting is one of the most critical steps. Here, the possibility of recounting must be considered as well. Therefore, counting has to be able to be carried out multiple times and the input needed, such as the cast votes, has to be archived.

In addition to counting mechanisms, an analysis system is also needed. Such a system provides the auditing team and the election officials with various reports. One of the most important reports is of course the final result of the counting. The format and the precise schema of such reports is out of scope of the model provided by EML.

Audit, Administration

In addition to the phases and roles given above, there are some other important actors and elements in the model. Very important are the audit mechanisms that are needed along all phases of an election. On the one hand, it is important to have possibilities to prove the correctness of the process as such. On the other hand, it is crucial not to violate the main principles and security requirements, such as keeping a vote an inviolable secret in particular. However, auditing is necessary to prove the authenticity

of the result of the election. Thus, a special set of persons, e.g. election officials and the candidate's representatives, should be allowed to gain access to auditing information.

System administration is critical as well, since administrators are allowed to access the system. Nevertheless, administration is necessary and therefore the security concept of the e-voting system has to protect critical data and components, especially the secrecy of the ballots. This affects the organizational aspects of the security concept in particular. Technical security mechanisms cannot guarantee this by themselves. The administrative staff has to be chosen with respect to confidentiality as well.

3.2 Categories based on the Number of Rounds

Election systems can be categorized according to the number of rounds a voter has to pass while casting a vote. Most of the existing e-voting models can be classified into one-phase and two-phase models. Since a few models require additional phases, these models are called n-phase models.

Each phase represents a certain action required at a certain time. Thus, the phases are in a special order. The phases considered here are not necessarily the same as the ones defined within EML. Some of them may be similar, however a phase in the model view may cover several EML phases, and vice versa as well. For example, a voting model may require a user to register and vote in two distinct steps. Talking in EML, the pre-voting phase (voter-registration) is similar to phase one. The voting phase itself is phase two from the model's perspective. Post-electoral tasks as defined in EML are not considered here since they are not a part of the voters' business. This categorization is seen from the voter's view.

One-phase models are quite rare. Here, the voter casting a vote can be done in a one-step manner. This means that the voter is not required to register to vote in advance. Thus, from the voter's perspective, the voting process takes place in one phase.

However, most of the e-voting models available are two-phase models (see figure 3.2). Commonly, in the first phase the voter has to register to vote and she receives some sort of authentication credentials in exchange. With the use of these credentials, the voter is permitted to take part in the voting process in phase two (main phase).

Sometimes, a system may require some more steps between the first phase and the main phase. In an n-phase model, the voter is repeatedly asked to register to vote in two or more distinct steps at multiple authorities. In this case, from the voter's perspective, the pre-voting phase defined by EML is broken up into n phases.

3.3 Categories based on Schemes

E-voting systems consist of a conceptual design and a underlying e-voting scheme. Thus, an e-voting system is based on an E-Voting Schema (EVS). The scheme is the core of the system ensuring that requirements are met. Most of them use cryptographic mechanisms and principles. This chapter gives an overview and a survey of the most important classes of schemes used today. These can be grouped as follows:

- EVS based on Homomorphic Encryption [32] [33] [34] [35]

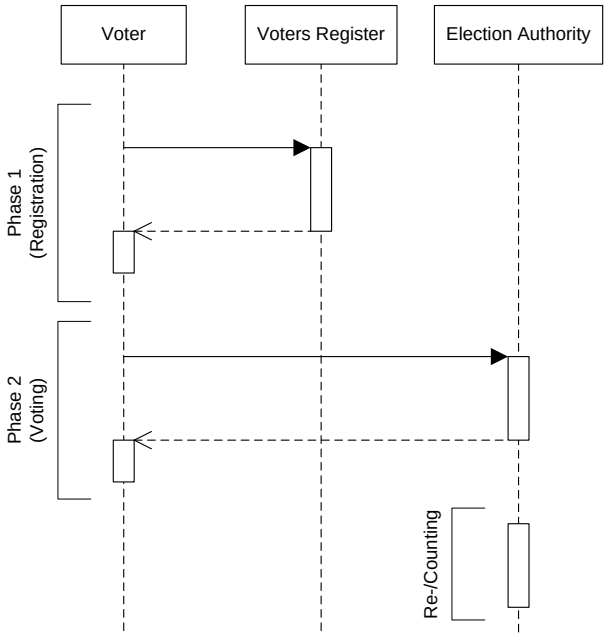

Figure 3.2: Sequence of a 2-phase voting model

- EVS based on Mixing Nets [36] [37] [38]
- EVS based on Blind Signatures [36] [39] [40] [41] [42] [43]

Of course, other schemes exist as well and the grouping can be done based on other objectives. However, here the most common approach was chosen.

The following sections do not describe the schemes in all details. The aim of this introduction is to outline the main ideas and principles only. Further descriptions can be found in [44] and in the referenced documents.

3.3.1 EVS based on Homomorphic Encryption

These schemes are based on the homomorphic properties of the encryption methods used. In the context of e-voting, all encrypted votes are collected and summed up. Finally, the sum of all encrypted votes is decrypted thus the result can be reconstructed. This works because of homomorphism.

To give a mathematical definition of homomorphism:

> A mapping $f : A \mapsto B$ is called a homomorphism of A into B if f preserves operations of A. That is, if $\circ$ is an operation of A and $\star$, an operation of B, then $\forall x, y \in A$ we have $f(x \circ y) = f(x) \star f(y)$. [45]

For instance, the ElGamal public key encryption [46] is homomorphic. Using it for encrypting votes would be a basis for a homomorphic voting scheme.

A scheme of this kind is the scheme proposed by Josh Benaloh [33]. Beside other cryptographic mechanisms, such as threshold cryptography, this scheme is based on homomorphic encryption. In order to

give an idea of the principles behind homomorphic encryption, we show an example based on a simple yes-no decision where 0 or 1 represent the available options.

The e-voting environment consists of M-authorities, A_1 to A_M. Each of them owns a public key pair. Authorities are closely bound to each other through the use of threshold cryptography requiring that at least t authorities are needed to decrypt the result of the election. The number of all voters is given by N, whereby every voter has got her very own public key pair.

To cast a vote, the voter has to split it up into M parts, one for each authority.

$$v_i \rightarrow s_{i,1}, ..., s_{i,j}, ..., s_{i,M} \tag{3.1}$$

Next, every part of the decomposed vote becomes encrypted with the public key of the authority for which the part of the vote is intended. One of the shares of a vote dedicated to an authority A_j look like this:

$$(g^{r_{i,j}}, \gamma_j^{r_{i,j}} g^{s_{i,j}}) \tag{3.2}$$

The notation used is quite common, but for this introduction it is not necessary to know all its details. Here, the tupel $(g^r, \gamma^r x)$ stands for the ElGamal encryption algorithm [46], where g denotes the generator function and r represents a random number. The random number is characteristic for the ElGamal encryption. This is why it is denoted as a randomized encryption algorithm. As a consequence, the variation of this random factor ensures that the encrypted messages will vary even if the plain text is the same. This is very important for this kind of e-voting scheme. Otherwise the voter's decision could be revealed by the form of the encrypted vote since there would only exist two different types of encrypted votes.

After the election is over, every authority collects the valid votes received and calculates the component-wise product of all of them without decrypting the particular votes. Due to the use of threshold cryptography, this is anyhow impossible.

Assume authority A_j receives N shares of votes, whereby all of them are proved for correctness, uniqueness and whether the voter is authorized to cast a vote:

$$(g^{r_{1,j}}, \gamma_j^{r_{1,j}} g^{s_{1,j}}), ..., (g^{r_{i,j}}, \gamma_j^{r_{i,j}} g^{s_{i,j}}), ..., (g^{r_{N,j}}, \gamma_j^{r_{N,j}} g^{s_{N,j}}) \tag{3.3}$$

Building the component-wise product of these encrypted shares leads to the following result:

$$(g^{\sum_i r_{i,j}}, \gamma_j^{\sum_i r_{i,j}} g^{\sum_i s_{i,j}}) \tag{3.4}$$

The component $S_j = g^{\sum_i s_{i,j}}$ is important. This component contains the resulting sum of all votes cast. Thus, by decrypting the result, authority A_j gains this component, and therefore the sum of the shares dedicated for it respectively, namely $g^{\sum_i s_{i,j}}$. Because of the use of threshold encryption, the components of t authorities are necessary at the very least to reconstruct the resulting sum according to all votes cast. Therefore, the overall result can be calculated by the *Lagrange-Interpolation* used within threshold cryptography systems:

$$\prod_j (g^{S_{ij}})^{\alpha_j} = g^{\sum_j S_{ij}\alpha_j} = g^S \tag{3.5}$$

Due to the difficulty of computing discrete logarithms, gaining S would be infeasible. Since the number of votes is limited by N, it is possible to calculate all possible results, such as $g^0...g^N$ reflecting $S = 0...S = N$. By comparing the result with these preprocessed values, the voter's decision can be easily determined.

The major principle in this scheme is that it is not necessary to decrypt each ballot and construct the result by the use of the encrypted votes. By using the homomorphic property of the encryption algorithm used, it is possible to compute a result by using the encrypted ballots and the homomorphic function adequate to addition. Threshold encryption used within this scheme brings an additional advantage to deal with malicious authorities, but it is not needed from the point of view of homomorphism. Reducing the number of authorities to one will lead to a scheme showing that the principle of homomorphic e-voting schemes works best.

This idea of this scheme is widely used. Many other existing schemes are built on this principle, [35] for instance. Once again, the big advantage is that no vote has to be decrypted, which is very helpful for keeping the voter's choice an inviolable secret. Thus, no authority is able to find out how any single person voted. The voter is authenticated using some credentials and her public key pair respectively. On the other hand, the encrypted vote given by a voter, which is in the case of a threshold cryptographic system a share of her original vote only, will be never decrypted. So, the vote remains hidden.

A mentionable drawback to schemes of this class is that the complexity of the scheme grows exponentially with the number of electable options. Most elections have more than only two options, thus election schemes based on homomorphic encryption might be hard to implement due to complexity reasons.

3.3.2 EVS based on Mixing Nets

The basic idea in this class of schemes is the use of mixing devices. A mixing device, a mixing net for instance, takes some input and scrambles it, and vice versa. Thus, the output corresponds to some permutation of the input. This mechanism can be used to scramble incoming votes in order to decouple the voter from her vote. On the other hand, mixing devices can also be used to scramble all possible votes a voter can cast from which the voter has to choose. As a result, the voter's choice becomes hidden and a secret. Many schemes use both principles.

David Chaum [36] first introduced the idea of mixing nets. He proposes using a cascade of several mixing devices. Each of these devices takes its input and produces an output corresponding to an arbitrary permutation of the input. Moreover, the mixing device knows the relationship between the input and the output only. However, in a cascade built of n mixing devices, since at least 1 of n mixing devices keeps the relationship between input and output a secret, the result of the whole mixing cascade remains a secret and will be unpredictable. This is one of the main advantages of mixing nets as proposed by David Chaum. On the other hand, this can also be a disadvantage at the same time. For instance, even if only 1 device fails, the whole mixing cascade will fail as well.

The voting scheme proposed by Martin Hirth and Kazue Sako described in their paper [38] uses this principle in addition to other cryptographic mechanisms such as the homomorphic property of encryption. However, the primary goal aimed at in their work is the use of mixing nets in order to decouple the voter and her vote. The basic workflow is as follows:

At first, assuming that for each vote possible, denoted by $v_i \in V$, there exists an encrypted counterpart using standard encryption, denoted by by $e_i^{(0)} \in E$. The encryption of all valid votes possible have to

be announced publicly, e.g. by the use of a bulletin board of some kind. Based on this assumption, the sequence of initial encoded votes ($e_1^{(0)}...e_L^{(0)}$) is taken as the input for the first mixing authority A_1. This authority takes this input, scrambles it and feeds it to the next authority A_2 as input sequence $e_1^{(1)}...e_L^{(1)}$. The relation between $e_1^{(0)}...e_L^{(0)}$ and $e_1^{(1)}...e_L^{(1)}$ produced by the randomness of authority A_1 is communicated to the voter via an untappable channel. In other words, the permutation π_M used to produce the output of the input sequence is known by the voter only. This untappable channel is of absolute importance in this scheme, which ensures that only the voter knows which element of the output corresponds to which element of the input. By cascading all the M-authorities step-wise in a sequence, whereby the output of the preceding authority is used as the input for the succeeding authority, the resulting sequence of encoded votes $e_1^{(M)}...e_L^{(M)}$ is totally mixed. Since the voter is informed about the relation between the input and the output sequence of every authority, she is the only one who can map an arbitrary element of the initial sequence to the according element of the final sequence. Therefore, it is essential in this situation to guarantee that the communication between every (or at least one) authority and the voter is kept secret and untappable. However, the voting process as such is that the voter points to the element of the resulting sequence which corresponds to the initial encrypted vote she wants to cast.

Mixing nets are often used in e-voting systems. Most commonly, mixing nets are used to send a sender-untraceable email. Therefore, messages are sent into a mixing net in order to lose the relation between the message and the sender. This mechanism is often used in e-voting systems in combination with other principles, such as blind signatures for instance. An example of an e-voting scheme that takes this approach is the collision-free secret ballot protocol proposed by Juang and Lei [37].

3.3.3 EVS based on Blind Signatures

The third major approach for realizing e-voting uses what is referred to as blind signatures. The idea of blind signatures was introduced by David Chaum in [36] [39]. Blind signatures initially were intended to be used within electronic cash systems (e-cash) to ensure the anonymity of its owner. Since the motivation to keep the voter anonymous is the same in e-voting schemes, this technique can be applied as well. The key technique of blind signatures allows a signer to sign a document without seeing it. This can be compared to giving a handwritten signature on a document wrapped in a flimsy paper. The wrapped document gets signed without being seen.

The following paragraph describes the mathematical principle used by blind signatures.

The authority's key is given as:

$$public : (n, e)$$
$$private : (n, d)$$

The voter wants the authority to sign the vote v without knowing what it is (blind signature). Thus, the voter generates a random value r satisfying:

$$\gcd(n, r) = 1 \tag{3.6}$$

By using the random value r and the authority's public key component e, the voter makes her vote blind

and creates a *blinded vote* x:

$$x = (r^e v) \bmod n \tag{3.7}$$

Now, the authority cannot derive any useful information from the message x. Therefore, the voter asks the authority to sign it using its private key:

$$t = x^d \bmod n \tag{3.8}$$

The authority returns the signed "vote" t to the voter.

$$\begin{aligned} t &= x^d \bmod n && (3.9)\\ &= (r^e v)^d \bmod n && (3.10)\\ &= (r^{ed} v^d) \bmod n && (3.11)\\ &= r \cdot v^d \bmod n && (3.12) \end{aligned}$$

Since the voter knows the random value r used for blinding, she can remove it from the signed vote to get:

$$\begin{aligned} s &= r^{-1} t && (3.13)\\ &= v^d \bmod n && (3.14) \end{aligned}$$

Finally, s is the vote v signed using the authority's private key which prevents the authority from learning the signed vote v.

In e-voting schemes, this principle is used in several occurrences. However, what is common to all of these occurrences is that a vote can be signed by an authority without reading the content, i.e. the voter's decision.

For example, prior to the voting process, a voter has to identify himself at the registration authority. After having been authenticated successfully, the voter sends her blinded vote carrying her decision to the registration authority to become signed. In consequence, the voter's vote is signed by the authority with the use of blind signature technology in order to assert that the voter is eligible to vote. Due to the blind signature, the content of the vote will not be revealed to the registration authority. After the vote has been cast, the election authority can prove every cast vote by verifying the blind signature. Thus, the election authority is able to decide whether a voter was eligible to cast a vote or not. The registration authority cannot find out the voter's decision during signing and the election authority cannot learn which voter a vote belongs to. The voter's identity remains a secret. However, the blind signature is used to prove that the voter is authenticated and authorized to cast a vote. So, the voter is authorized without revealing her identity.

In a scheme such as this, additional mechanisms should be implemented to ensure that every voter is only able to cast one valid vote. This can be achieved by including a unique random sequence with each vote. The sequence should be generated in such a way that the authority cannot learn which sequence is used by a particular voter. This could be ensured for example by preparing ballots in an anonymous process or by the voter himself locally.

Chapter 4

Notable E-Voting Projects

E-voting has been a challenging topic not only for academics but also for software vendors and governments as well. Thus, many notable e-voting projects and products exist already. Most of them follow one of the academic e-voting schemes described in section 3 from a technical point of view. From an organisational point of view, e-voting systems can be categorised as follows [1]:

- Local e-voting systems
- Remote e-voting systems
  - Remote e-voting in an attended (controlled) environment
  - Remote e-voting in any environment

Local e-voting systems are used within polling stations only. This term subsumes all kind of electronic voting machines and terminals which are used in polling stations as a replacement for paper ballots and conventional urn. Thus, local e-voting systems are only used in environments that are under the control of an election commission. Although these kinds of e-voting systems are widely-used internationally, e.g. in Brazil and in many US states, they are not in the focus of this thesis. Nevertheless, the use of local e-voting systems has its advantages. For example, an electronic terminal could aid handicapped people in casting their ballots by using special devices to display the ballot. Furthermore, with the use of local e-voting systems, counting could be done faster and would be more precise.

In contrast to local e-voting systems, remote e-voting systems are not limited to being used in a polling station only. Remote e-voting systems have to be further categorised into remote e-voting systems that are used within an attended (controlled) environment, and remote e-voting system that can be used anywhere. The former category of remote e-voting systems means that e-voting need not only take place in a polling station but can be in any controlled environment, e.g. having remote e-voting clients in police stations or in banks. In these scenarios, the e-voter does not visit an election commission but she votes in a controlled, attended environment. Many states only allow remote voting in controlled environments in order to protect the voter from being influenced by third parties.

The latter category of remote e-voting systems is the freest interpretation of e-voting since it stands for systems which allow e-voters to vote from anyplace[2], even from their homes.

[1] This categorisation is based on the categorisation proposed by Christoph Grabenwarter in [13]

[2] From a legal perspective, a further classification of these kinds of remote e-voting systems might be necessary since e-voting within a state and e-voting from abroad require different legal premises. Christoph Grabenwarter [13] discusses this legal issue in

Alternative categories of e-voting systems exist as well. For instance, in [47], e-voting systems are categorised into poll site e-voting systems[3], kiosk e-voting systems[4] and remote e-voting systems[5] which correspond to local e-voting systems, remote e-voting systems in a controlled environment, and remote e-voting systems in any environment respectively. Additionally, considering existing remote e-voting solutions, the use of the Internet as a voting channel might be used as an additional distinguishing characteristic from a technical perspective, though, this section as well as the whole thesis focus on e-voting over the Internet.

The e-voting system introduced by this thesis aims to be a remote e-voting system of the last kind. If an e-voting system enables voting from arbitrary locations, it can be used in all other scenarios as well. Thus, it can even be used as a local e-voting system within a polling station.

If we take e-voting to mean remote e-voting over the Internet, many countries are already experimenting with e-voting pilots but only a few have used e-voting systems in real elections. In Europe, several noteworthy e-voting systems have been used or were at least tested in various countries. The following list, sorted in alphabetical order, highlights a few of them[6]:

- **Austria**
  Austria has not yet conducted any legally binding e-voting pilots, however several e-voting trials have taken place already. The first non-binding e-voting trial was conducted in May 2003 in parallel with the Student Union election. Further non-binding e-voting tests have been conducted in parallel with the Austrian presidential election in April 2004 and the Austrian parliamentary election in October 2006. For a detailed description of the e-voting system used see section 4.2.

- **Estonia**
  Estonia was one of the very first countries in Europe to use remote e-voting over the Internet in real elections. Estonia had already started discussing e-voting in 2001 and successively created the legal basis for it and developed a technical e-voting solution. Since the e-voting solution of Estonia was developed in parallel to the e-voting solution introduced in this thesis and follows a similar approach, section 4.1 discusses the Estonian e-voting concept in more detail.

- **France**
  France started testing remote e-voting using the Internet in 2003. In June of that year, French citizens residing in the USA could elect their representative to the Assembly of the French Citizens Abroad (AFE) over the Internet. Apart from this legally binding test of remote e-voting using the In-

detail. With respect to the further technical discussion, this separation is not necessary.

[3] "*Poll site Internet voting* offers the promise of greater convenience and efficiency than traditional voting systems in that voters would eventually be able to cast their ballots from many polling places, and the tallying process would be both fast and accurate. Since election officials would control both the voting platform and the physical environment, managing the security risks of such systems is feasible." [47]

[4] "In *kiosk voting*, voting machines would be located away from traditional polling places, in convenient locations such as malls, libraries, or schools. The voting platforms would still be under the control of election officials, and the physical environment could be modified as needed and monitored (e.g. by election officials, volunteers, or even cameras) to address security and privacy concerns, and prevent coercion or other forms of intervention." [47]

[5] "*Remote Internet voting* seeks to maximize the convenience and access of the voters by enabling them to cast ballots from virtually any location that is Internet accessible. While the concept of voting from home or work is attractive and offers significant benefits (e.g., the ability to conduct online research on candidates prior to voting, and the empowerment of the disabled), it also poses substantial security risks and other concerns relative to civic culture." [47]

[6] This rudimentary overview is based on various sources; in addition to project and country specific sources, embracing and synoptic views can be found at http://aceproject.org/ or http://http://www.louiseferguson.com/resources/evoting-europe.htm

ternet, France has not taken any further actions with respect to the introduction of remote e-voting[7]. Today, France mainly focuses on using e-voting technologies at polling stations, and therefore concentrates their efforts on implementing local e-voting technologies (i.e. e-voting machines). Thus, during the recent presidential election in 2007, several polling stations tried various kiosk systems.

- **Germany**
  Germany is one of the pioneers with respect to e-voting, although e-voting systems are not yet widely in use. In 1999, Germany started a series of non-political test elections: Student Union elections at the universities of Osnabrück (2000) and Bremerhaven (2001), election of senior citizens councils (Brandenburg 2000), as well as elections of several public and private employees' councils.[8] The e-voting system used in these elections was the i-vote system developed by the German Research Group of Internet Voting[9]. However, for political elections, Germany only concentrates their focus on kiosk technologies.

- **Spain**
  E-Voting in Spain has had a long history. Since 1995, several pilots have been conducted, although most of them focus on local e-voting systems. In 2003, a non-binding remote e-voting test was conducted in parallel with the parliamentary election for Spanish citizens living abroad. Further non-binding e-voting trials followed at several municipalities using various technologies, e.g. SMS-voting or Internet voting-machines in the year 2003. In addition to national initiatives and trials, the city of Madrid launched its own e-participation initiative. The citizens of Madrid have the possibility to vote and participate in referendums electronically. The e-voting solution used in Madrid is the Pnyx-system [49] developed by the Spanish company Scytl[10]. This e-voting solution offers the use of multiple voting channels, e.g. mobile-phones and the Internet. In 2005, the Spanish government launched a large and nationwide remote e-voting pilot using the Internet in the course of the referendum on the European Constitution. This pilot was not legally binding; the system used was developed by the Spanish vendor Indra[11].

- **Switzerland**
  Switzerland has conducted several e-voting trials and legally binding e-voting pilots in the past. In 2001, the Swiss confederation mandated three states (cantons) to develop and test e-voting: Geneva, Neuchâtel and Zurich ([50] [51] [52]). The very first legally accepted e-voting test took place in January 2003 in Geneva. Since then, the state of Geneva offers e-voting as a legally accepted alternative to its citizens[12]. The Geneva e-voting system is of particular interest as it is intended to be conducted in parallel with conventional elections. Thanks to the special design of the ballot cards—ballot cards contain a secret e-voting code hidden under a rubber layer—the voter is free to choose whether she wants to vote electronically, through postal voting or at a conventional polling station. In the latter case, the officials at the polling station can easily determine whether

[7] The French Internet Rights Forum released a study on the use of Internet-based e-voting in France immediately after the first French e-voting trial. This study recommended against wider use of Internet based e-voting; Internet based e-voting should be offered only to French citizens residing abroad. [48]

[8] An exhaustive overview of e-voting pilots conducted in Germany can be found at http://www.isl.uni-passau.de/de/isl-home/about-us/mitarbeiter/melanie-volkamer/evoting.html (as seen on 15 July 2007).

[9] Information available at http://www.internetwahlen.de/ (as seen on 15 July 2007).

[10] Scytl, http://www.scytl.es

[11] INDRA, http://www.indra.es

[12] Further information of the e-voting solution of Geneva can be found at http://www.geneve.ch/evoting/english/welcome.asp (as seen on 15 July 2007), [53], [54].

the voter has tried to vote electronically by checking the rubber layer on the ballot card. If the rubber layer is untouched, the voter in question could not have tried to register for e-voting since the registration code is still hidden by the rubber layer. Just like Geneva, the canton of Zurich also successfully developed an e-voting system[13] [55] [56]. This e-voting system offers electronic voting via multiple channels, e.g. the Internet, SMS or even interactive TV. Recently, the e-voting system of Zurich has won an award from the United Nations; it was awarded the United Nations Public Service Award 2007 in the category for "Fostering Participation in Policy-making Decisions through Innovative Mechanisms"[14].

- **The Netherlands**
  In the Netherlands, e-voting mainly refers to e-voting using voting machines at polling stations. However, the possibility of remote e-voting using the Internet is still under discussion and is currently restricted to a limited number of voters living abroad [57] [58]. Voters abroad may use the so-called RIES (Rijnland Internet Election System; RIES was developed for the Rijnland District Water Board elections in 2004) remote e-voting system which uses the Internet as the voting channel[15]. In the last parliamentary elections of 2006, approximately 20,000 voters abroad used this system to cast their votes.

- **United Kingdom**
  The United Kingdom started testing electronic voting alternatives in 2000. Since then, several election districts in the United Kingdom have conducted e-voting pilots, in 2002, 2003, 2004, 2006 and 2007[16]. The United Kingdom's aim "[..] *that the General Election after next—possibly as soon as 2008, certainly by 2011—much of the ground should have been prepared for e-enabled election*" [60]. Thus, in this year's elections, various election districts have tested alternative voting technologies using multiple systems, e.g. kiosk systems at polling stations, remote e-voting systems, as well as various voting channels, such as telephone, Internet, etc. (a detailed announcement of the e-voting pilots used is given in [62]). However, the resulting recommendation of the Open Rights Group (ORG; a non-profit lobbying body for digital civil rights) is devastating; ORG concludes that "[..] *given the problems observed and the questions that remain unanswered, it cannot express confidence in the results declared in areas observed. Given these findings, ORG remains opposed to the introduction of e-voting and e-counting in the United Kingdom.*" [63].

In addition to national remote e-voting trials and projects, the EU Commission has funded an international e-voting research project called the CyberVote project[17]. CyberVote was launched on 1 September 2000 and was completed in September 2003. The scope of the project was to develop a remote e-voting system using the Internet for various types of elections. The resulting prototype was tested in a number of e-voting trials. The e-voting protocol and prototype that was developed allows a voter to securely cast her vote from multiple platforms, e.g. PC, mobile device, PDA, etc. From a cryptographical point of

[13] Website of the Zurich e-voting solution: https://evoting.zh.ch (as seen on 15 July 2007).

[14] The award was presented in Vienna, Austria, on 26 June 2007 during the seventh Global Forum on Reinventing Government; see http://www.unpan.org (as seen on 1 July 2007)

[15] The OSCE/ODIHR Election Assessment Mission Report [59] of the past parliamentary elections of 2006 discusses both forms of e-voting, local e-voting using voting machines and remote e-voting using RIES.

[16] Details on the e-voting trials conducted in the last few years can be found in [60] [61]; moreover, the UK Electoral Commission publishes detailed descriptions of past and upcoming electoral pilot schemes at http://www.electoralcommission.org.uk:80/elections/modernising.cfm.

[17] The project website contains further details and is available at http://www.eucybervote.org (as seen on 15 July 2007).

view, the resulting e-voting prototype makes use of a homomorphic encryption schema (for a general description and discussion of the principle of homomorphic encryption schemes see section 3.3.1) thus the encrypted votes are never decrypted. The result can be determined by summing up the encrypted votes. This prototype was tested with more than 1,000 voters during e-voting trials in Germany[18], France[19] and Sweden[20]. The CyberVote's final report [65] summarizes the project's achievements and outlines the main characteristics of the remote e-voting solution.

This thesis does not aim to present a comprehensive survey of all existing e-voting systems. Instead, the following sections describe two e-voting approaches which are notable with respect to the development of the e-voting system introduced in this thesis. The e-voting solution of Estonia seems to be remarkable since it is also based on the principle of postal voting and makes use of strong encryption to protect the election secrecy. Furthermore, the Estonian e-voting system is one of the few Internet voting systems which has already been used in real nationwide elections. The e-voting concept of the University of Economics Vienna (Austria) is also of special interest since it claims to be an e-voting system that is suitable for real elections in Austria. Both systems have been investigated and are outlined and briefly discussed in the following sections.

The last section of this chapter touches the Secure Electronic Registration and Voting Experiment (SERVE) of the United States Department of Defense. The SERVE e-voting system was intended to provide US military staff abroad with the ability to vote electronically. Before this system was put in place, a devastating report—the Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE) [66]—caused the immediate stop of this project. The SERVE report raised a number of points of criticism not only about the SERVE project itself but also about remote e-voting based on the Internet in general. Thus, the three most significant problems raised by the SERVE report will be discussed.

4.1 Remote E-Voting Solution of Estonia

Estonia is not only one of the leading countries with respect to e-Government but is also one of the first countries to have conducted e-voting over the Internet in real elections[21]. However, this is not the only reason why the Estonian e-voting model has been chosen to be discussed in this thesis. The Estonian e-voting solution is somewhat comparable to the proposed e-voting concept EVITA since it also maps a postal voting schema to e-voting. This section outlines the main characteristics of the Estonian e-voting model following [2], [67], [68], [69] and [70].

From an organisational and legal perspective, the Estonian e-voting scenario is an advance voting scenario in which e-voting takes place during a certain time before the election day of conventional elections[22]. Thus, e-voters are required to vote electronically in advance before the election day. This has two advantages. First, conventional polling stations can be easily equipped with current electoral rolls in which e-voters are marked in order to prevent double votes. Secondly, Estonian law enables advance voters to re-elect several times, either by voting electronically again or by voting in a conventional polling station on the election day. This is due to two reasons. First, in the event of a system failure, either in the

[18] Trial in Bremen (2-3 December 2002 and 13-15 January 2003): University of Public Administration, election of three university's representative bodies; the first trial in December was stopped due to an error in the candidates list [64].

[19] Trial in Issy-les-Moulineaux (11 December 2002): Election of the representatives of the city borough councils [64].

[20] Trial in Kista (27-31 January 2003): on-line referendum [64].

[21] In 2005, the first ever countrywide e-voting over the Internet took place.

[22] According to Estonian election legislation, e-voting takes place six to four days before election day. [2]

voter's equipment or infrastructure, or in the central e-voting infrastructure, e-voters have the possibility to vote again at a conventional polling station on election day. Secondly, Estonian law recognizes the "family voting" problem, or more generally speaking, the problem of having an e-voter who has been unduly influenced, and enables e-voters to cast her vote again[23]. As a result, the previously cast vote is replaced with the new one.

In contrast to many other voting scenarios, the Estonian voting system lacks a dedicated registration phase. Instead, voters who would like to vote electronically simply request the e-voting service offered during the advance voting phase. Thus, the voter is identified and authenticated by using her Estonian electronic identity[24].

The core principle is depicted in figure 4.1. From a technical perspective, the Estonian e-voting solution maps a generic postal voting schema to e-voting by applying asymmetric cryptography (public key cryptography). The vote is put into an inner envelope which itself is wrapped by an outer envelope that contains additional identifying information about the voter. Mapping this principle to e-voting leads to the application of encryption and electronic signatures. The inner envelope is substituted by encrypting the vote for the appropriate electronic urn, referred to as the Vote Counting Application. The outer envelope bearing the voter's identity information is substituted by the voter's electronic signature. Thus, the election process consists of the following steps (this description touches on the most relevant steps only):

1. Voter accesses the e-voting service provided by the Estonian election authority. The e-voting front-end is denoted as the Vote Forwarding Server since it forwards all received votes to the storage system, called the Votes Storage Server, located in the back office area. The voter has to identify and authenticate herself using her Estonian electronic identity.

2. The Vote Forwarding Server verifies the voter's identity as well as her eligibility to vote, it determines her election district by querying the voters registry and finally checks whether or not the voter has already cast a vote by querying the Votes Storage Server. As a result, the Vote Forwarding Server displays the resulting list of candidates according to the voter's election district. In the event that the voter has already cast a vote, the Vote Forwarding Server informs her that she is going to delete her previously cast vote.

3. The voter is requested to make her decision. In an additional step the service requests the voter to confirm her decision.

4. After the voter has confirmed her decision, the voting application—i.e. a signed applet presented in the voter's browser by the Vote Forwarding Server—encrypts her decision by applying the public key of the Vote Counting Application. This encryption represents the inner envelope as in conventional postal voting.

5. Furthermore, the voter signs her encrypted vote using her electronic identity card. This signature represents the outer envelope as in conventional postal voting wearing the voter's identity.

6. The voter transmits her signed and encrypted vote to the Vote Forwarding Server which verifies the vote with respect to the outer signature. It verifies whether the voter who signed the vote is the same as the one who requested to vote.

[23] The voter is able to vote several times electronically.

[24] The Estonian electronic identity is the major e-ID document used in Estonia. It also provides electronic signatures for authentication purposes.

7. The Vote Forwarding Server forwards the received vote to the Vote Storage Server which stores all incoming votes. If the vote is able to be stored successfully, the Vote Storage Server returns a confirmation message to the voter via the Vote Forwarding Server.

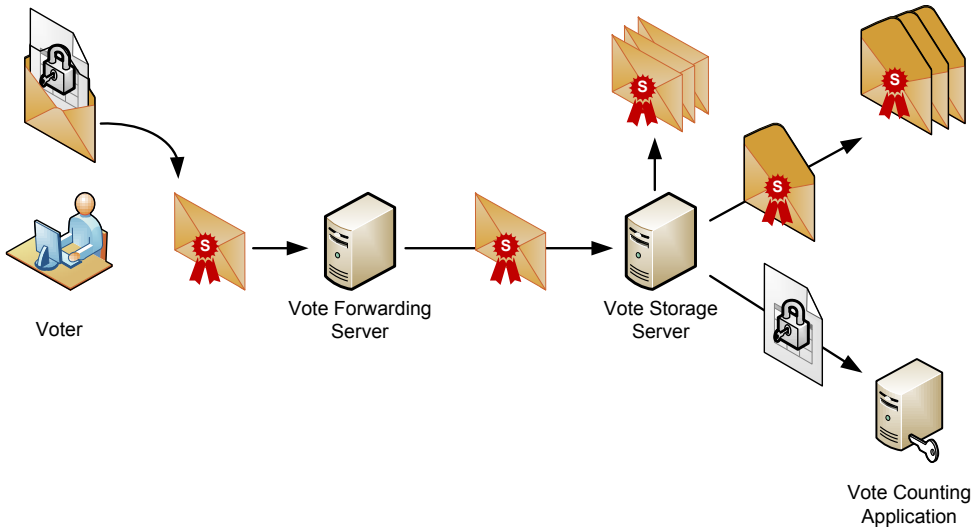

Figure 4.1: The core principle of the Estonian e-voting solution as described in [2].

After the election phase, the Vote Storage Server holds all votes cast. Before counting, cast votes have to be sorted and double votes have to be eliminated. Since the Estonian e-voting systems allows e-voters to cast multiple votes electronically, whereby the only very last vote is of relevance, the sorting algorithm has to find the very last vote and cancel all others. As a result of this sorting and cancellation algorithm, the Vote Storage Server holds a set of sorted and unified votes. The succeeding counting algorithm takes this sorted set of votes as input:

1. Votes become sorted according to the election district. This is done by taking the outer signature of the cast vote to identify the voter. The election district is determined by querying the voters list.
2. The outer envelope, the electronic signature, is removed from the cast votes. The remaining signatures without content are held separately as the final list of e-voters (i.e. list of voters who have cast their votes electronically).
3. The remaining encrypted votes—without the enveloping signature identifying the voter—are fed to the Vote Counting Application. The Vote Counting Application securely holds the private key used to decrypt votes. Then, the Vote Counting Device decrypts all cast votes and counts them.

The key element of the Estonian e-voting solution is the private key used to decrypt all cast votes. Therefore, a stringent key management is required and the private key should be securely held, preferably using a Hardware Security Module (HSM). With respect to encryption, the Estonian e-voting system is comparable with the e-voting system proposed in this thesis. However, in some issues, the Estonian approach seems not to be satisfying. One of the most important issues, the obligation for voters to sign their vote using their personal electronic identity card, leads to cast votes which are permanently branded with

their unique electronic identity. Although their signature becomes separated from their cast vote before counting, the concept does not provide any possibility to break the link between a vote and the voter's identity before casting. Moreover, the Estonian e-voting solution creates logging information consisting of the voter's unique identifier and a hash value of her cast vote at several stages due to auditing purposes. This logging information is critical as well since it serves as an additional link between the voter's unique identity and her cast vote.

Therefore, as a requirement, the proposed EVITA e-voting schema introduces a stringent domain separation concept in order to achieve unique, repetitive identification of the voter's cast vote without revealing the voter's unique identity. Furthermore, to prevent voters from signing their votes personally, an independent asserting authority will be introduced. From an organisational perspective, the advance vote model followed by the Estonian e-voting solution is also not directly applicable to Austria. However, this issue is not that restrictive.

To summarize the Estonian solution, the core principles used are comparable with the proposed EVITA concept up to a certain extent. Also the main workflow process makes use of comparably clear steps. Its main drawback is the lack of being able to separate the voter's unique identity from her cast ballot. On the other hand, the Estonian e-voting project is successful as it has already been put in place and used. For example, during the parliamentary elections of March 2007 more than 30.000 voters decided to vote electronically[25].

4.2 E-Voting System of the University of Economics Vienna

Austria does not yet have an e-voting system that is used in real elections. Nevertheless, three e-voting trials have been conducted by the University of Economics and Business Administration Vienna. The last e-voting test was conducted in 2006 in parallel with the Austrian presidential election, whereby this e-voting test did not influence the result of the real election. Since the core system used in all three e-voting tests is the same, this section reflects the latest state of development. The description given here is based on [71], [72], [73], [43], [74] and [75].

From a technical perspective, the e-voting concept of the University of Economics relies on blind signatures. From an organisational perspective, it follows the principle of ballot cards whereby the voter receives a ballot card during the registration phase for which she then receives a blank ballot during the election phase. The following paragraphs outline both the registration and the election phase of this voting system separately.

The registration phase is shown in figure 4.2. Before accessing the e-voting system for registration, the voter has to generate a random string that represents her ballot card. This ballot card—technically a token—becomes blindly signed by two distinct authorities, namely by a registration authority and an additional trust center. The voter uses this blindly signed ballot card during the election phase to prove her eligibility to vote. The registration process at a glance is as follows:

1. In the first step, the voter generates her own ballot card. The ballot card consists of a random string created by the voter. The random string generator has to guarantee that the generated string is unique amongst all voters. The voter then blinds her ballot card and thus prepares it to be blindly signed by the registration authority and the trust center.

[25] Taken from [68]; percentage of e-voters amongst votes collected through remote voting: 18%.

2. Before the voter requests the registration authority to sign her ballot, she has to identify and authenticate herself. With respect to voter identification and authentication, this e-voting concept does not make further assumptions and thus it does not necessarily require the use of the Austrian Citizen Card. At any rate, the voter has to prove her identity so that the registration authority is able to determine her eligibility to vote. If the voter's right to vote can be positively verified, the registration service signs the voter's blinded ballot card and returns it to the voter.

3. Next, the voter presents the blindly signed ballot card to the trust center. The trust center again checks the voter's eligibility to vote and signs the blinded ballot card. The trust center returns the signed ballot card to the voter.

4. Finally, the voter un-blinds the received ballot. As a result, she holds a ballot card which has been blindly signed by both the registration authority and the trust center. The voter needs her ballot card in order to authenticate herself anonymously during the succeeding election phase.

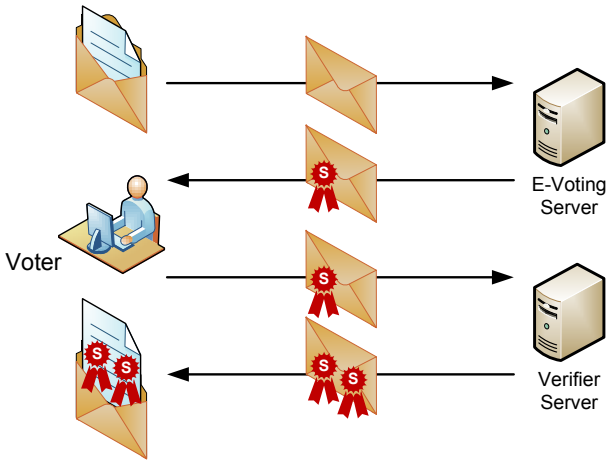

Figure 4.2: The registration process of the e-voting system of the University of Economics.

After the registration phase, the registration authority generates electoral rolls for polling stations. These rolls do nothing more than hold a list of voters who have been registered for e-voting in order to prevent double votes. On the other hand, the voter holds a double signed ballot card as a kind of anonymous proof that she is eligible to vote. Anonymity is ensured by blinding the ballot card before signing. By introducing an additional trust center to verify and assert the voters eligibility to vote a second time, the concept aims to prevent a bogus registration authority from creating ballot cards. In fact, if a bogus authority is able to create illegal ballot cards, this e-voting concept would allow them to be used for casting valid votes due to the authority's signature on ballot cards. Therefore, the e-voting concept of the University of Economics introduces an additional trust center to re-sign the voter's ballot card. So neither a bogus registration authority nor a bogus trust center would be able to create illegal ballot cards. Illegal ballots can only be created if both authorities are bogus and work together. From a systematical point of view, this threat is still possible, however.

The voter has to securely store the ballot card. To do so, this e-voting concept requests that the voter encrypts her vote using a simple password-based encryption method at the very least. On election day—or during the election period—the voter is asked to present her ballot card to the e-voting server in order

to authenticate herself as eligible voter. The core principle of the election phase is illustrated in figure 4.3; its main activities are:

1. The voter decrypts her ballot card (if necessary). She provides her decrypted ballot card to the e-voting server in order to authenticate herself as an eligible voter. Since the ballot card does not contain any identifying information—the ballot card is a randomized string—the voter remains anonymous.
2. In response, the e-voting server returns a blank ballot and the public key of the electronic urn.
3. The voter makes her decision and fills in her vote. She immediately encrypts her vote by applying the urn's public key provided by the e-voting server. Thus, this e-voting concept relies on public key cryptography in order to protect cast votes, but encryption is not needed to keep the vote anonymous. The voter finally submits her encrypted vote to the e-voting server which stores it and responds with a confirmation.

As a result, the e-voting server holds all encrypted cast votes. Since the cast votes do not contain any identifying information—all cast votes are of the same structure, depending on the voter's election district—the counting procedure is obvious and simple. The e-voting server simply encrypts all cast votes and produces the result by considering all decrypted votes.

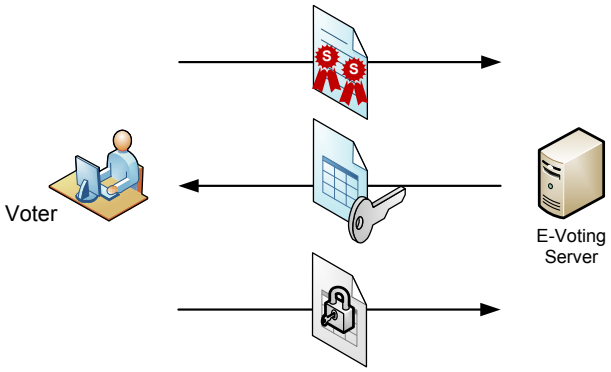

Figure 4.3: The election process of the e-voting system of the University of Economics.

Considering the core principles of this e-voting system, there are some systematical drawbacks worth discussing. One issue is the requirement of needing an additional trust center. This concept suggests having a trust center in order to prevent a bogus registration authority from creating illegal ballot cards. However, even having a second authority cannot entirely eliminate this threat. There still exists the possibility that both authorities are bogus and cooperate with each other. Thus, having an additional trust center is only able to reduce the risk. Another issue is the ballot card itself. This e-voting concept asks the voter to generate a randomized string which is blindly signed by two authorities and is finally used to anonymously authorise the voter to vote. This means that every issued ballot card—or to be more precise, every ballot card structure signed by both authorities—can be used to vote. There is no way to invalidate an issued ballot card or to sort it out during the election phase. In the event that a voter loses her ballot card, there is no possibility to reissue a second ballot card since the old one still would be usable for voting. Although a technical implementation of this e-voting concept could offer voters

the possibility to store their encrypted ballot card securely on the e-voting server[26], if a voter loses her key or password needed to decrypt her ballot card she would be excluded from the election as well. Furthermore, in the event of technical failure or a break-down either on the voter's local computer or at the e-voting system, there is no possibility for the voters affected to vote conventionally at a polling station. An e-voting solution should especially take a break-down of the server side infrastructure of the e-voting system into consideration, e.g. if the e-voting server goes down as a result of a successful denial-of-service attack. However, this e-voting concept provides no conventional alternative for such a worse case scenario. This problem also precludes re-voting being considered as a possibility to protect against "family voting" as this e-voting concept would not be able to offer it.

To summarize, the e-voting concept of the University of Economics Vienna is a two-phase concept requesting voters to register in advance for e-voting. In order to keep the voter's identity anonymous, it relies on the use of blind signatures. Although the introduction of the Austrian Citizen Card is possible[27] and would improve the concept in some aspects, e.g. the Citizen Card would serve as unique identification and a strong authentication of voters as well as strong encryption of the voter's ballot card, the concept may only be limitedly suitable for a national election on a large scale.

4.3 Secure Electronic Registration and Voting Experiment (SERVE)

For many ongoing projects concerned with voting via the Internet, the SERVE report [66] seems to be a disaster. In this report, a group of well known e-voting researchers—D.Jefferson, A.D.Rubin, B.Simons and D.Wagner—stated their doubts on the Internet-based e-voting project developed by the United States Department of Defense (DoD). As a consequence, the DoD's SERVE project was stopped immediately following the recommendations given in the report. The most important arguments in the SERVE report can be summarized as follows:

- the system (especially the software) is totally closed and proprietary
- the system has no voter-verified audit trails
- an Internet and PC based system is vulnerable to various types of cyber attacks (e.g. denial-of-service attacks, spoofing, viral attacks, etc.)

The SERVE report raises these issues and some other problems as well, however these are the main problems. Since the e-voting system proposed in this thesis uses the Internet as a voting channel, these criticisms cannot be ignored. Thus, this section shortly discusses the three major problems and emphasises their meaning with respect to the work presented by this thesis.

A Closed and Proprietary System

Election systems should be evaluated by some independent authority. E-voting systems should be proven to be compliant with standardised protection profiles, although exhaustive protection profiles for e-voting systems are not available yet. Thus, such protection profiles have to be developed.

[26] The implementation of this e-voting concept as it was used for the test election in 2006 offered this service to voters.

[27] The concept is intended to be used in connection with the Citizen Card although the e-voting test conducted in 2006 does not make use of the Citizen Card.

Whether or not the system and in particular the software should be opened to the general public is a difficult question. On the one hand, giving the public a look at the software increases the chance of somebody detecting vulnerabilities and reporting them. On the other hand, instead of reporting the error, they may compromise the election by using this knowledge. However, it is not the intention of this work to provide a clear answer to this question.

A possibility for evaluating the system is to use standardised interfaces for the modules of the election system. By splitting the e-voting system into modules as proposed in the definition of the EML [1] and by applying EML at the interfaces, the e-voting modules of different vendors can be interchanged arbitrarily. Doing so enables proving the system by using different components. In other words, if the behavior of the system changes when using modules from different vendors, it is a strong indication that something is working not correctly. On the other hand, the introduction of standardised interfaces means that an election result can be verified by doing a re-count on a totally different and independent e-voting system. From the technical point of view, it would even be imaginable that the results of an election could be proven by using a compatible voting system from another country (e.g. in the EU: results of elections for the EU parliament)—however, the political and legal aspects remain unaccounted for.

The e-voting system introduced in this thesis makes use of the EML model and the election markup language. This means that the system and its components are not bound on a set of proprietary implementations.

Voter Verified Audit Trails / Audit in General

To provide the voter with an audit trail is quite reasonable. The e-voting concept presented in this thesis provides the user with the ability to audit the ballot until it is encrypted and signed. From this moment on, any alteration of the voter's ballot will be detectable. As will be shown in the following chapters, using the Austrian Citizen Card to encrypt the voter's ballot and to prepare it for being signed, the voter can be ensured that her decision is under her control until she sends it to the electronic ballot box. The voter can audit her ballot until it is encrypted using her certified Citizen Card software which includes a secure viewer to display the ballot. This approach is somewhat comparable to paper based voter-verified audit trails which, for instance, display the ballot to the voter through a glass window before it falls into the ballot box.

Auditing in general is of paramount importance. The voting system has to be designed to enable auditing at every stage and during every process. Since the ballots used in the e-voting system proposed in this thesis are encrypted, it is possible to monitor every single vote during the whole election process. Even the hardware security module will be designed to be auditable in order to prove that it is working correctly (e.g. by including counters at relevant stages).

Using the Internet

Up to a certain extent, the statement of the authors of the SERVE report is correct: the security problems of today's Internet are enormous. These problems are difficult and some of them are still impossible to solve in a technical way alone. Therefore, e-voting systems have to be complex enough to include a technical perspective, an organisational perspective and as a legal perspective as well. When following an all-embracing security concept that is comparable to that of the Common Criteria methodology, it is necessary to realize that technical countermeasures alone cannot eliminate all threats. Therefore there

is an urgent need for additional organisational and non-technical measures to combat these threats.

For example, in the Internet today it is impossible to fully protect a server from denial-of-service attacks which threaten any Internet based e-voting system. Instead of technical countermeasures, the e-voting concept proposed in this thesis deals with this problem by requiring an organisational measure. For instance, enabling voters to cast their votes at conventional polling stations even though they registered for e-voting leads to having conventional voting as a fall-back system, thus allowing the voter can participate in the election anyway. Furthermore, due to the proposed e-voting schema based on strong encryption, it would even be possible for the voter to print her encrypted ballot on paper and send it to the election authority by postal mail. However, understanding e-voting as an all-embracing system allows many problems to be solved, especially those related to the Internet which cannot be handled by IT technology alone.

Chapter 5

Requirements for Electronic Voting using the Internet

Lorrie Cranor and Ron Cytron define requirements desirable in e-voting systems from an scientific point of view in [76] and [77]. They give the following ”desirable characteristics of a good electronic voting system”:

Accuracy, Democracy, Privacy, Verifiability, Convenience, Flexibility, Mobility

At first sight, the most important characteristics are accuracy, democracy, privacy and verifiability. Cranor and Cytron define them in [77] as follows:

Accuracy: *A system is accurate if*

1. *it is not possible for a vote to be altered,*
2. *it is not possible for a validated vote to be eliminated from the final tally, and*
3. *it is not possible for an invalid vote to be counted in the final tally.*

In the most accurate systems the final vote tally must be perfect, either because no inaccuracies can be introduced or because all inaccuracies introduced can be detected and corrected. Partially accurate systems can detect but not necessarily correct inaccuracies. Accuracy can be measured in terms of the margin of error, the probability of error, or the number of points at which error can be introduced. [77]

Democracy: *A system is democratic if*

1. *it permits only eligible voters to vote,*
2. *it ensures that each eligible voter can vote only once. [77]*

Privacy: *A system is private if*

1. *neither election authorities nor anyone else can match any ballot to the voter who cast it, and*

2. *no voter can prove that he or she voted in a particular way.*

The second privacy factor is important for the prevention of vote buying and extortion. Voters can only sell their votes if they are able to prove to the buyer that they actually voted according to the buyer's wishes. Likewise, those who use extortion to force voters to vote in a particular way cannot succeed unless they can make the voters to prove that they voted as requested. [77]

Verifiability: *A system is verifiable if voters can verify independently that their votes have been counted correctly.*

The most verifiable systems allow voters to verify their votes and correct any mistakes they might find without sacrificing privacy. Less verifiable systems might allow mistakes to be pointed out, but is not able to correct them, or they might allow verification of the process by party representatives but not by individual voters. [77]

The most important characteristic of an e-voting system mentioned by Cranor and Cytron is to keep the voter's decision an inviolable secret. Therefore, the protection of cast votes is essential. This is difficult because on the one hand, it must be ensured that no cast vote carrying the voter's decision can be mapped to the voter's identity, but on the other hand, voters have to be uniquely identified and authenticated for the election. These two requirements seem to be contradictory but both have to be satisfied. This is what makes electronic election systems so challenging to design.

The general requirements for any kind of election and for e-voting as stated by the Venice Commission's Code of Good Practice [11] are[1]:

- universal suffrage
- equal suffrage
- free suffrage
- secret suffrage
- direct suffrage.

The desirable characteristics given by Cranor and Cytron are a subset of these cardinal principles. Thus, the cardinal principles have to be considered as the base requirements for any e-voting system used for political democratic elections. Therefore, the discussion on e-voting requirements starts at these cardinal principles.

A number of initiatives—driven by multi-national consortia, such as the Council of Europe, as well as by national organisations, such as the German Bundesamt für Sicherheit in der Informationstechnologie or the Austrian Ministry of Internal Affairs—have been launched to draft detailed requirements for e-voting systems based on these cardinal principles. The following sections discuss these initiatives and specify the requirements for the e-voting system EVITA.

[1] A detailed discussion on the Venice Commission's Code of Good Practice is given in section 2.

5.1 Recommendations for e-enabled Voting of the Council of Europe

The Council of Europe initiated an ad-hoc group of experts and charged them to create recommendations for legal, operational and technical standards for e-voting systems. The recommendation report of this working group contains 112 detailed requirements and aims to raise the standards for the creation and introduction of e-voting systems. The ministerial committee of the European Councils adopted these recommendations on 30 September 2004.

The recommendation is structured into three categories: legal, operational and technical requirements (standards). The basis for these requirements are election fundamentals as laid down by international conventions and documents, such as the European Convention for the Protection of Human Rights and Fundamental Freedom or the Code of Good Practice in Electoral Matters of the Venice Commission. The recommendation should therefore help in designing an e-voting system that is compliant with existing election fundamentals.

The Council of Europe aims to foster common understanding and to create an established set of requirements for e-voting systems. This recommendation is not legally binding, although it is expected to influence upcoming as well as existing e-voting systems in the near future. The Committee of Ministers summarizes the recommendation as follows:

> *[..]*
> *i. E-voting shall respect all the principles of democratic elections and referendums. E-voting shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means. This general principle encompasses all electoral matters, whether mentioned or not in the Appendices;*
> *ii. the interconnection between the legal, operational and technical aspects of e-voting, as set out in the Appendices, has to be taken into account when applying the Recommendation;*
> *iii. member states should consider reviewing their relevant domestic legislation in the light of this Recommendation; iv. the principles and provisions contained in the Appendices to this Recommendation do not, however, require individual member states to change their own domestic voting procedures which may exist at the time of the adoption of this Recommendation, and which can be maintained by those member states when e-voting is used, as long as these domestic voting procedures comply with all the principles of democratic elections and referendums;*
> *v. in order to provide the Council of Europe with a basis for possible further action on e-voting within two years after the adoption of this Recommendation, the Committee of Ministers recommends that member states:*
>
> - *keep under review their policy on, and experience of, e-voting, and in particular the implementation of the provisions of this Recommendation; and*
> - *report to the Council of Europe Secretariat the results of their reviews, who will forward them to member states and follow up the issue of e-voting.*
>
> *[..] [3]*

The recommendation does not aim to require member states to change their existing election processes

or e-voting systems, as long as they are compliant with established election fundamentals, but if election systems or processes are subject to changes, governments should consider this recommendation. This recommendation requires taking legal, operational and technical requirements into consideration as a solid combination. Only all three aspects together will yield an e-voting system that would satisfy the recommendation.

The Committee of Ministers aims to review the recommendation in regular intervals as e-voting is based on rapidly evolving technologies. The first review took place in November 2006, two years after the recommendation had been adopted. The experts group did not see the need for updating the recommendation at that time and suggested leaving the recommendation unchanged.

The recommendation contains three appendices which give detailed requirements with respect to legal, procedural and technical issues. The following paragraphs emphasize the most important requirements for the e-voting system to be introduced and designed throughout this thesis. Since legal requirements have been already elaborated on in chapter 2 and due to the fact that this thesis focuses on presenting a technical solution, the technical requirements are of interest. The recommendation itself also focuses on technical requirements, which can be seen by comparing the number of legal, operational and technical requirements[2]. A full description of all requirements and further detailed explanations are given in the final recommendations of the Committee of Ministers [3] and in the explanatory memorandum [4].

Legal Requirements

The legal requirements address those voting principles of the Code of Good Practice of the Venice Commission which directly affect an e-voting system. These principles are universal suffrage, equal suffrage, free suffrage and secret suffrage. The principle of direct suffrage is not addressed as it does not influence the design of an e-voting system but instead concerns itself with the organisational and legal background of an election. (see requirements 1. to 19. of the recommendation [3] and [4])

Furthermore, the legal appendix defines procedural requirements as well. It claims that an e-voting system has to be transparent and understandable for voters in order to foster voters' confidence in the e-voting system. It is also recommended to give voters a chance to practice e-voting using a test system prior the actual election event. (see requirements 20. to 23. of the recommendation [3] and [4])

The recommendation asks electoral authorities to charge an independent body with the duty of verifying and proving the e-voting system to confirm that it functions correctly. Moreover, this body should confirm that the e-voting system is compliant with the required security measures. (see requirements 24. to 25. of the recommendation [3] and [4])

Re-counts are also addressed by the legal requirements. It is explicitly required that an e-voting system shall not prevent re-counts. Even a partial or complete re-run of the election shall be possible. (see requirements 26. to 27. of the recommendation [3] and [4])

Finally, the section on legal requirements addresses reliability and security aspects. In this section, the election authority is asked to ensure the reliability of the e-voting system and verify that it functions correctly. It must be ensured that the e-voting system remains available throughout the election event. Furthermore, the election authority has to properly select the persons who access or operate the e-voting system. Critical actions should be conducted by teams of at least two or more persons only. Accurate

[2]The Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting [3] contains 36 legal requirements, 25 operational requirements and 52 technical requirements.

monitoring and reporting is required. (see requirements 28. to 33. of the recommendation [3] and [4])

The last two requirements are especially relevant for the EVITA voting system. Requirement 34 requires that the e-voting system should keep the votes sealed and confidential—and under certain circumstances encrypted—until the counting process. It is further required that the voter's data (her identity, authentication information, etc.) should remain sealed and kept separate as long as it can be linked to the voter's decision. Voter information and the cast vote should be separated at a certain stage of the election. Both of these requirements coincide with the basic principles of the EVITA voting system, thus, the recommendation of the Council of Europe explicitly affirms the general principle of the EVITA voting system. (see requirements 33. to 35. of the recommendation [3] and [4])

Operational Requirements

Operational standards address the way in which an election event should be organised. For example, the operational standards require that a clear timetable is given and that all relevant periods and timelines have to be announced in clear and understandable language. (see requirements 36. to 38. of the recommendation [3] and [4])

The existence of a voters' register is recommended, and if possible, it should be an electronic register. If a voter has to apply for e-voting, an electronic application should be provided to voters. The standard also recommends considering an electronic process for candidate nomination. (see requirements 33. to 35. of the recommendation [3] and [4])

Electronic elections and conventional elections may take place in parallel. This means that polling stations may be open during the period of e-voting. The operational standards specify that the e-voting period may start and/or end before the period of conventional voting at polling stations, but e-voting should not be possible after polling stations have closed. Furthermore, if e-voting and conventional voting are conducted at the same time, appropriate measures have to be taken in order to prevent double voting. (see requirements 44. to 45. of the recommendation [3] and [4])

When displaying voting options to the voter, the e-voting system has to ensure that all options are displayed equally. No candidate or list standing for election must be discriminated against. The system should clearly and equally display all options without any other kind of information which might influence the voter. Furthermore, while casting her vote, the voter should be notified that she is casting her vote in a real election. If any test or demonstration systems are in place—either before or in parallel to the real election event—the voter must be made very aware whether she is using the test system or the real e-voting system. (see requirements 46. to 50. of the recommendation [3] and [4])

Giving the voter proof of her vote is a topic that has been heavily discussed. The operational standards of this recommendation address this issue and recommends not giving the voter any kind of proof of voting, especially any proof that contains the voter's decision or gives an indication of the voter's decision. (see requirements 51. to 52. of the recommendation [3] and [4])

The e-voting system should not start the counting process before the voting period ends. The operational standards further states that the e-voting system should not reveal any information indicating the result before the election period ends. The counting procedure should be observable and auditable by the election commission and external observers as well. Counting should result in a detailed report documenting the start and end time of the counting process, the persons involved, etc. The counting process should prevent uncover votes by choosing an arbitrary small set of votes, thus stringent rules have to be put in

place. (see requirements 53. to 60. of the recommendation [3] and [4])

Technical Requirements

The technical requirements address several aspects of e-voting systems, such as accessibility, interoperability, system operation and security. With respect to accessibility, the design of the e-voting system should follow all-embracing accessibility considerations. The hardware and/or software of an e-voting system, especially the components used at the client side, should be easy and intuitive to use and should provide easy access to handicapped people. Thus, users should be involved in the development of the e-voting system from the very beginning and common accessibility recommendations (such as given by the Web Accessibility Initiative) should be considered. Furthermore, voters should be supported by all means if necessary. (see requirements 61. to 65. of the recommendation [3] and [4])

When designing an e-voting system, technologies based on open standards and open specifications should be preferred whenever possible. For example, OASIS[3] hosts the development of EML which is an open standard for "*enabling the exchange of data for public and private election services*"[4] and should preferably be used for creating XML interfaces and document formats. If local and national circumstances require customization, open standards and specifications should be localised to suit these needs. However, by using open standards and specification as the basis at least, the design of an e-voting system reaches a maximum of interoperability. (see requirements 66. to 68. of the recommendation [3] and [4])

The e-voting system and its hardware and software components should be well-documented and regularly verified. It should be checked whether any security updates or bug fixes for the components exist before the system is used again in an e-election. In other words, the election officials should ensure that the e-voting system is up-to-date with respect to security and error patches. Furthermore, it is recommended to have a contingency plan for the e-voting system. This implies that backup procedures/systems, emergency and incident handling strategies, and a disaster recovery plan are required. An incident handling strategy should instruct election officials—or the persons who run the e-voting system—about how to react in the event of an incident so that the election is not affected by it or have to be interrupted or aborted. Furthermore, it should be defined in advance who is to be informed in the event of an incident and how they can be reached. In addition to incident-handling procedures, verification and control procedures should be defined in order to prove, monitor and verify the proper functioning of the e-voting system before, during and after an election event. The e-voting system should be located and run within a secure area. (see requirements 69. to 76. of the recommendation [3] and [4])

With respect to information security, the technical requirements point to all phases of an election separately; the pre-voting phase, the voting phase and the post-voting phase. However, with respect to all voting phases, the e-voting system should (see requirements 77. to 85. of the recommendation [3] and [4]):

- ensure that no data or information becomes permanently lost even if some event occurs, such as a break down of the system, etc.
- ensure the privacy of individuals, i.e. votes, candidates, etc.
- be regularly checked and monitored with respect to availability and correct functioning

[3] see http://www.oasis-open.org

[4] taken from the EML website at http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=election as seen on 6 June 2007.

- identify and authenticate any person or user accessing the system
- protect authentication data from being modified, spied on or deleted
- provide observation data in an accurate and sufficient form; authenticity, integrity, availability and timely accuracy should be guaranteed
- make use of accurate—and preferably synchronised—time sources; this is important not only to determine the exact start and end time of the e-voting period but also to create accurate observation and audit information
- be under the responsibility of the election commission with respect to compliance with security requirements

An additional major requirement for an e-voting system is to uniquely identify voters and candidates with the use of an adequate electronic identification schema in order to prevent any kind of confusion or impersonation. (see requirement 82. of the recommendation [3] and [4])

For the pre-voting phase, the recommendation requires that the authenticity and integrity of the data stored in the voters' register and candidate list should be ensured. Furthermore, the voters' register and the list of candidates should be available during the election event or at least as long as required. The information provided by the voters' register and the list of candidates provides the data source for the whole e-voting system. Thus, the data to be fed into the voters' register and list of candidates has to be authentic in order to achieve a sufficient level of data quality. Furthermore, data protection measurements have to be taken. If voters can register for e-voting by electronic means, the registration service has to record the time of registration so that it is evident that the voter has applied for e-voting within the defined registration period. The registration system should deny registrations that occurred before or after the registration period. (see requirements 86. to 88. of the recommendation [3] and [4])

Since data transfer from the pre-voting phase to the voting phase is necessary, data origin authentication is required. The e-voting system should ensure the integrity of data. This is not just a requirement for the communication between pre-voting phase and voting phase but rather a general requirement for most data flows between different phases and entities. The voter should also be able to verify the authenticity of the ballot she receives from the voting system. (see requirements 89. to 90. of the recommendation [3] and [4])

The voter is allowed to cast her vote within a certain period of time only. Thus, the e-voting system should accurately record the time that the voter cast her vote. The system should take sufficient measures to prevent a voter's vote from being modified or deleted both during and after casting. This requirement has an effect on the central components of the voting system as well as on the components on the client side, i.e. voter side. If some form of client software is needed, measures should be taken to delete any remaining (cached) information that could reveal a voter's decision. Voters should at least get sufficient information instructing them how to delete and prevent unintentionally remaining data on the client (e.g. Web browsers usually cache contents which could be used to spy on a voter's choice or decision). (see requirements 91. to 93. of the recommendation [3] and [4])

Before the voter casts her vote, the e-voting system should require the voter to sufficiently identify and authenticate herself. The e-voting system also has to confirm whether or not the voter is eligible to vote. The vote cast by the voter should accurately and unambiguously represents the voter's decision. After the period for casting votes is over, the e-voting system should not accept any more cast votes.

Attention should be paid to cast votes which are in transfer at the moment of the closing of the system. This is especially relevant for remote e-voting over the Internet, as there may be delays when sending information. Thus the e-voting system should accept incoming cast votes for a certain period of time longer. (see requirements 94. to 96. of the recommendation [3] and [4])

With respect to communication between the voting phase and post-voting phase, the recommendation report requires once again that the authenticity and the integrity of the data be confirmed. Furthermore, the availability and integrity of all cast votes—e.g. stored within an electronic ballot box—should be maintained as long as necessary, at least until counting or as long as a re-count might be expected. The counting of the votes should be accurate and reproducible. (see requirements 97. to 99. of the recommendation [3] and [4])

The last portion of the technical recommendations addresses audit functionality. In general, auditing should be considered in the very first phase of implementing an e-voting system on all levels: on a logical level, on a technical level and on an application level. Comprehensive auditing should include recording, monitoring and verification facilities:

- Recording:
  - record potential issues and threats, e.g. any attacks or attempts to attack the system or its affiliated components, system failures and malfunctions, etc.
  - record times, events and actions
  - record voting-related information, e.g. number of eligible voters, number of cast votes, number of valid and invalid votes, counts and re-counts, etc.
- Monitoring:
  - provide functionality to oversee the election
  - provide a way to verify that the election is conducted in accordance with given laws and defined procedures
- Verifiability:
  - E-voting systems should provide the possibility of proving the accuracy of the election result with the use of cross-checks
  - it should be verifiable that all votes are authentic, that all votes have been counted and that the result is an accurate representation of all valid cast votes

Disclosure of audit information to unauthorised persons should be prevented. The voter's anonymity must remain protected despite the introduction of a transparent and comprehensive audit system. Thus, the audit system itself should be protected against attacks and misuse of any kind. (see requirements 100. to 110. of the recommendation [3] and [4])

In order to ensure that the e-voting system is compliant with the technical security requirements stated in this recommendation, the e-voting system or the components used should be certified and accredited. Certification and accreditation processes are common practice in IT security. The certification process is the evaluation of the security features of components and systems. Internationally accepted certification schemes have already been established, e.g. the Common Criteria schema. The Common Criteria

schema defines the certification process as "[..] *the independent inspection of the results of the evaluation leading to the production of the final certificate or approval, which is normally publicly available*" [78]. The accreditation process is used to verify that a given (certified) system meets specified security requirements and thus is approved to be put into service. Although Common Criteria does not address accreditation directly, it states system accreditation as "*[..] the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts*" [78].

Member states are encouraged to expand on and perhaps even localise the security requirements given in this recommendation in accordance with the organisational needs of the certification schema. In terms of Common Criteria for instance, member states could develop a detailed protection profile so that e-voting systems can be certified and accredited according to a well-defined set of requirements by an independent certification authority. Having this in mind, the structure of the explanatory memorandum of technical requirements has been borrowed from the structure of a Common Criteria protection profile as a basis for future works. (see requirements 111. to 112. of the recommendation [3] and [4])

5.2 Requirements for E-Voting in Austria

In 2004, the Austrian Ministry of the Interior launched an initiative in order to answer the question about how e-voting could be introduced in Austria. Three working groups have been set up to tackle this question with respect to the legal, technical[5], and international aspects. These working groups were requested to[6]:

- investigate and analyse e-voting projects (in Austria and abroad)
- analyse discussions on e-voting abroad (especially within Europe)
- verify the adaptability of the recommendation of the Committee of Ministers of the Council of Europe on legal, operational and technical standards for e-voting
- determine legal, technical and economical requirements for the introduction of e-voting in Austria

As a result, the working groups prepared a combined report [22] giving a summary of their findings along with three additional detailed reports: on the international situation [79], on legal aspects [80] and on technical issues [81].

Although these working groups elaborated on the current situation and identified things to do on the way towards introducing e-voting in Austria, the conclusions of these working groups can be interpreted as requirements. This section provides an excerpt of the conclusions of these working groups as presented to the Ministry of the Interior in November 2004[7]. The main conclusions have been presented in section 2.2 on page 17 already.

[5] The author of this thesis was a member of the technical working group and assistant to the coordinator.

[6] taken from the preamble of [22]

[7] The concluding report of the working group "E-Voting" has been presented to the Ministry of the Interior, Dr.Ernst Strasser, on 15 November 2004.

International Situation of E-Voting

Although the survey on the international situation was conducted in 2004, the major statements are still valid. This excerpt emphasises the major statements only; the in-depth report of this working group [79] gives a detailed overview of the international situation as seen in 2004.

The report of the working group on international aspects (UAG-3) concluded that e-voting is a topic of emerging interest. E-voting has been addressed by several states, institutions and organisations of different kinds. The internationally common main objectives of e-voting are:

- to ease execution of elections for both, public administration and voters
- to ease access to elections for voters, especially for a wider range of voters
- to provide access to elections by using communication channels which are commonly used by citizens today, e.g. the Internet
- to increase quality, in general, but especially with respect to counting
- to prevent the accidental or unintentional cast of invalid votes

From an international perspective, two different forms of e-voting exist: e-voting at polling stations (attended e-voting) and remote e-voting (e.g. e-voting using the Internet). The former form of e-voting is already widely in use, e.g. in Belgium, the Netherlands, United States of America, Russia, Azerbaijan, Brazil, Paraguay, India, Germany, Canada, Portugal, Denmark and Australia. Several other countries are also considering introducing this form of e-voting. The latter form of e-voting—which is also the one of interest with respect to the introduction of e-voting in Austria—is not yet widely in use, although several countries have tested remote e-voting, e.g. France, Italy, Denmark, Portugal, or already conducted test elections, e.g. United Kingdom, Switzerland, Japan, the Netherlands and Spain).

Many countries interested in introducing e-voting (remote e-voting) aim to provide their citizens living abroad an easy and efficient way to participate in elections. However, these countries are faced with challenges of different kinds, i.e. in legal, technical, political and socio-cultural perspectives. Furthermore, any e-voting system to be introduced has to be fully compliant with existing voting fundamentals, the most important of which being secret and personal suffrage. Moreover, questions such as how to uniquely identify and authenticate voters and how to guarantee election secrecy throughout the election and beyond have to be addressed.

International experience with e-voting shows that many questions and aspects have been intensively discussed and solved already, although problems remain that are still waiting to be tackled. Another important lesson learned through the international experience is that the introduction of e-voting should take place step by step in order to familiarise both voters and governments with it. Only a stepwise procedure is considered to be successful for reducing doubt and increasing trust in e-voting[8]. Therefore, it is recommended to introduce e-voting by having practice tests, followed by smaller test elections and ending with nationwide elections on a large scale.

[8] See also statement of Thomas M. Buchsbaum in [19]: "*[..] Alle Länder, die sich mit der Entwicklung von E-voting beschäftigen, haben [..] ein vorsichtiges Vorgehen eingeschlagen: Schritte von kleinen zu größeren Zahlen von Testpersonen, von unverbindlichen Wahltests zu rechtsgültigen Testwahlen, von überwachter zu nicht-überwachter Stimmabgabe, von Briefwahl zu Distanz-E-Voting. Wobei [..] sowohl bei Politikern als auch bei der Bevölkerung Verständnis und Vertrauen zu jedem Schritt aufgebaut werden muss. [..]*" He states that having a stepwise introduction of e-voting allows users to build up trust in it. Thus, an introduction should start with noncommittal tests and proceed on to conducting small test elections.

Legal Requirements for the Introduction of E-Voting in Austria

The legal working group (UAG-1) analysed the legal situation in 2004 with respect to the introduction of remote e-voting in Austria and has described their findings in a detailed report [80]). The working group came to a similar conclusion as described in the discussion in section 2.3: the introduction of e-voting in Austria requires a legal redefinition of secret and personal suffrage. In other words, the Austrian constitution has to be modified so that it explicitly allows the casting of votes outside a polling station, and thus not observed by an election commission. This must be possible not only for voters abroad (they already have this possibility) but also for voters within Austria.

The working group on legal aspects further identifies that the allowance of remote e-voting is directly bound to the general allowance of postal voting since both forms of remote voting go against the Austrian constitution and its interpretation. The concluding report of the legal working group recommends amending the Austrian constitution. A modified constitution should also contain regulations on the duties and the responsibilities of the election commission with respect to relevant steps of e-voting processes, e.g. registration process, cast-vote process and counting process[9].

The discussion about the legal acceptance of remote e-voting leads to the discussion of how to face the problem of voters who might be influenced or controlled by others. In order to tackle this fundamental problem—which is common to all forms of remote voting—the working group recommends to have polling stations within a reasonable distance of every voter as a requirement in the constitution. This should prevent the situation in the future that some voters do not have the possibility to vote conventionally (e.g. in outlying areas). For this reason, the legal working group recommends creating the fundamental right of being able to vote in front of an election commission. Thus, voters who are afraid of being influenced or controlled must have the possibility to consult an election commission in their local area.

In addition to legal changes on constitutional level, the working group requires regulating all other elements and processes of e-voting by extending the existing laws and administrative orders, whereby e-voting has to be always considered as an additional form of voting. The e-voting elements and processes recommended to be legally regulated are, for instance, the existence of a central electronic electoral roll and a registration procedure for e-voters.

The registration of voters for e-voting in advance is currently considered to be the only possibility for conducting e-voting and conventional voting in parallel, not only due to legal reasons but also due to economic aspects. The working group recommends that the registration period should end at a certain time before the election day so that the registration authority has time provide current electoral rolls to the polling stations (thus eliminating the need for providing online access to the central electoral roll at every polling station). However, online access at every polling station to the central electoral register should be envisaged for the future so that advance registration is not required.

The concluding report of the working group recommends starting e-voting prior to election day; preferably on the last working day before the election day. Thus, voters who do not have Internet access in their home might still be able to vote electronically from their office.

In general, the legal working group recommends adhering to the recommendations for e-enabled Voting of the Council of Europe [3] as the minimum standard for e-voting in Austria. The concluding remarks of the working group's report explicitly refer to the recommendation of the Council of Europe with respect to the appearance of the electronic ballot. The working group requires that all options on the ballot should

[9] Since July 2007, postal voting is allowed by the Austrian constitution; see also section 2.2 discussing Austrian adaption of international election fundamentals.

be displayed equally—as far as possible due to technical reasons—and security measures should be taken to prevent printing the ballot or the vote, as it is suggested by the recommendation of the Council of Europe as well.

Technical Requirements for the Introduction of E-Voting in Austria

The technical working group discussed various approaches for implementing e-voting from a technical perspective. The full report of this working group [81] describes all considerations in detail whereas the recommendations given in this report are technology-independent in order not to recommend any specific technologies or concrete solutions.

The working group considers the existing e-Government infrastructure as a sufficient basis for the introduction of e-voting. The Austrian Citizen Card in particular is considered to be the key element for voters as it provides unique identification and strong authentication of voters as well as other security functions, e.g. electronic signatures and encryption. Thus, the use of existing e-Government infrastructure is advisable not only due to the high level of security provided through e-Government infrastructural components but also due to economic reasons. In fact, the Citizen Card is not only adequate for identification and authentication of voters or candidates; it is also a comprehensive vehicle for providing anonymity and secrecy of votes through strong encryption.

In order to prevent double votes, the working group recommends two different approaches. The first approach is to hold e-voting at a different time than conventional voting, whereby e-voting would take place a certain time before conventional voting (advance voting). Conventional polling stations could be provided with current electoral rolls in which those voters are marked who already cast their vote by e-voting. This approach does not require any additional equipment for polling stations and does not necessarily require voters to register for e-voting in advance. The other approach is to conduct e-voting and conventional voting in parallel and require voters to register in advance if they want to use e-voting.

In order to enable e-voters to cast their vote conventionally, e.g. in the event of technical problems, some polling stations at least should be equipped with some form of access to the electoral register in order to determine whether or not the voter in question has already cast her vote (depending on the e-voting system used). Access to the electoral register could be implemented in different ways, e.g. by a full online access or by introducing some kind of call center, etc. If voters who originally registered to vote electronically are free to choose to vote conventionally instead on election day, it is necessary to equip the most of the polling stations with online access to the electoral register. If voters who have registered to vote electronically are allowed to vote conventionally only under extenuating circumstances, it would be sufficient to equip only a few selected polling stations with online access to the electoral register or with a call center providing “access” to the electoral register. However, in the long term, having full online access to the electoral register at each polling station seems to be desirable.

The technical working group further concludes that there is no technical measurement that can guarantee personal suffrage. The possibility of a voter being influenced or controlled by third parties is technically unsolvable and thus has to be accepted as a characteristic of remote elections. This problem has to be addressed by other methods, i.e. by legal and/or organisational measures.

Any technical implementation of an e-voting system should carefully consider the role of the election commission. The election commission should be an indispensable actor in the system. For instance, counting should only be started by a collaborative act of the members of the election commission. Furthermore, it should not even be possible to commence counting unless a collaborative act is started by

the members of the election commission. Additionally, the voting system should provide the election commission with the possibility to observe the election, to control counting and to enable the opening of the electronic ballot box (if this is required due the design of the e-voting system).

The technical working group also highlights in its report that the electronic form of voting provides plenty of possibilities which are not possible within conventional elections. For example, an e-voting system could prevent a voter from casting an invalid or blank vote. On the other hand, this kind of "help" would only be available for e-voters and thus would discriminate against conventional voters. Furthermore, if the voter wants to willfully cast an invalid vote, she has the right to do so. Thus, the working group concluded that the variety of additional "features" of e-voting should be well considered and the consequences carefully weighed.

Finally, the working group sketches out a conceivable e-voting scenario using existing e-Government technologies in order to give an idea of what is possible today. This example scenario requires the introduction of a central electoral register and takes the model of postal voting as the basis for the example. Within this scenario, voters should explicitly register for e-voting in advance. After being registered for e-voting, a voter is no longer allowed to vote conventionally. As a result of registration, voters receive some kind of electronic ballot card. The Citizen Card is used as key element in order to ensure confidentiality and secrecy of cast votes.

5.3 Common Criteria Protection Profile of the BSI

The German Federal Office for Information Security (BSI) took up the initiative to create a set of requirements, called a protection profile, for electronic voting systems following the Common Criteria methodology [10]. The Target of Evaluation (TOE) of this protection profile is an online e-voting system for elections within registered associations according to the German law. At the same time, it aims to lay down fundamentals applicable for any online e-voting system. The resulting protection profile addresses the voting phase only.

The recommendations of the Council of Europe [3] served as the basis for this protection profile. Since the protection profile is especially intended to be used for elections of registered associations, the authors drew on existing descriptions of requirements for these particular types of elections. Two sets of requirements have been considered: the e-voting requirement catalogue of the German PTB [83] and the e-voting requirement catalogue of the German GI [84].

The former requirement catalog was created by the Department of Metrological Information Technology of the German Physikalisch-Technische Bundesanstalt (PTB). The PTB created a catalogue of requirements for online voting systems for non-parliamentary elections [83], however it does not address remote e-voting systems specifically. The analysis presented in this catalogue assumes that voters only use networked polling stations. However, the basic principles and requirements are valid for and applicable to remote e-voting systems as well. This catalogue outlines the functions required at every stage of an election and further defines a set of requirements to be met by these functions. In this catalogue, an abstract e-voting system was divided into a number of functional units at a low abstraction level. The requirements were created according to these functional units. In contrast to the protection profile created by the BSI,

[10] "Basissatz von Sicherheitsanforderungen an Onlinewahlprodukte" [82]; the author of this thesis is a member of the advisory board supporting the development of this protection profile.

this catalogue of requirements considers an election throughout all of its stages. However, this catalogue lacks a standardised methodology, although it contains a comprehensive summary of requirements.

The latter description is the catalogue of requirements for Internet-based elections for registered associations created by the German Gesellschaft für Informatik e.V. (GI) [84]. This catalogue of requirements is based on both the Council of Europe's recommendation and the catalogue of requirements of the German PTB. Although this catalogue addresses e-voting in a very useful and simple way, it touches on issues related to remote elections over the Internet as well. Thus, it expands on the considerations given in [83] to some extent, however, it is not very detailed.

Using these two catalogues of requirements as a basis, the BSI working group followed the Common Criteria methodology for creating a protection profile for an online e-voting system suitable for remote elections. Since the level of detail was chosen to be quite low, the resulting protection profile only provides a bare minimum for a set of requirements. However, the Common Criteria methodology applied leads to systematically elaborated security considerations which could and should be further developed and extend to be also usable for large scale elections.

The protection profile serves two purposes. Vendors and developers of an e-voting system can use it as a catalogue of security requirements for design and development. In addition, a vendor might ask an independent evaluation authority to evaluate whether the vendor's e-voting system is compliant with the protection profile (to a certain degree). Only those e-voting systems which pass the evaluation are marked as evaluated components and are of certified quality. With respect to this, the technical recommendations given by the Council of Europe [3] require in line 111 that a certification procedure should be introduced in order to attest that it is in conformity with the required security standards:

> *111. Member states shall introduce certification processes that allow for any ICT (Information and Communication Technology) component to be tested and certified as being in conformity with the technical requirements described in this recommendation.*
> *[3]*

Additionally, the explanatory memorandum of the Council of Europe's recommendation [4] specifically suggests developing a protection profile based on the Council of Europe's recommendation and to require an independent assessment:

> *[..]*
> ***O.Assessment** Independent Assessment*
> *Election authorities have overall responsibility for compliance with these security requirements which shall be assessed by independent bodies. Application note: In case evaluated and certified CC / ISO 15408 Protection Profiles are developed based on this security recommendations, independent assessment is given under the CC scheme.*
> *[..] [4]*

Thus, the protection profile created by the BSI is a very important step toward designing an exhaustive protection profile for online elections. Before it can be applied to e-voting systems for real democratic elections on a large scale, it has to be extended to cover all phases of an election and its level of detail has to be expanded. The following paragraphs raise three issues to show the boundaries and the intention of the current version of the protection profile, thus highlighting future work which should be done.

The current version of the protection profile deals with a very limited set of roles and subjects. For example, the role of an election observer is neither defined nor addressed. This seems to be a valid decision for rudimentary elections, but with respect to "real" democratic political elections on a large scale and/or at a high level this role is essential. The current protection profile requires auditing and observation functionality for the election commission at the very least, although the observer role and the role of the election commission have to be strictly separated.

Furthermore, the assumptions with respect to the election commission made by the protection profile might be suitable for small elections but are unacceptable for others. The protection profile widely assumes that the election commission is not attacking the e-voting system. For instance, consider an election of members of the executive board of a registered association. In such a scenario, those persons who are members of the election commission are usually standing for election as well, thus they could have a potential interest in manipulating the election. In other words, the election commission should be considered as a potential attacker. This would be especially important since election observers are not yet considered in this protection profile.

In general, the protection profile does currently not assume having high potential attackers with sophisticated skills. The current version of the profile assumes having only four types of attackers—the network attacker, the voter without the right to vote, the voter without the permission to vote, the attacker aiming to access TOE data after voting phase—with very low skills (except network attacker; the network attacker is assumed to have professional skills) which is not sufficient.

Finally, the evaluation assurance level (EAL) aimed for in this protection profile—currently defined with EAL 2+ —seems to be adequate for elections under certain circumstances only, however, for real elections a significantly higher level should be required. Choosing an appropriately high evaluation assurance level is important. Having too low of a basis level and hoping that vendors would voluntarily apply for evaluation at a higher level will fail. If the protection profile itself does not require a sufficient evaluation assurance level—in order not to hinder smaller e-voting systems from being evaluated—additional policies or at least legal requirements should define an appropriate higher level.

To summarise, the existing protection profile is very important and is a useful basis for future work. It outlines the fundamental methodological framework and thus can be adopted and extended if required for other election scenarios. However, the intention of this protection profile was to serve small elections only. Furthermore, it was never intended to address more than the voting phase. Having this in mind, it can be concluded that the present protection profile is valuable, especially as a basis, and should be further developed in order to meet the needs of "real" elections as well.

5.4 Summary of Requirements for "EVITA"

This section sketches out the most important requirements with respect to technical security—the security objectives—for an e-voting system that would be suitable for Austrian elections. The following list of security objectives has been created by considering the requirements discussed in the previous sections. The resulting e-voting system presented in this thesis is aimed at addressing these requirements and objectives. In the final analysis section of this thesis, the presented e-voting system is compared against these objectives in order to verify whether or not it meets the claimed requirements.

In order to create a list of security objectives, it is advisable to follow some established methodology.

For example, the Common Criteria methodology provides logical procedures to analyse ICT systems as well as their environments with respect to assets and threats to find suitable security objectives (risk analysis). The Common Criteria methodology has also been chosen for creating the technical security recommendations of the Council of Europe [3] [4].

The risk analysis given in the technical part of the recommendations for e-enabled Voting of the Council of Europe is taken as the basis for the rudimentary risk analysis outlined in this section. This is not only due to the methodology used but also since the group of experts of the Austrian Ministry of the Interior has recommended create an Austrian e-voting system that is based on the recommendations of the Council of Europe[11].

The risk analysis given in the recommendation of the Council of Europe addresses conceptional and procedural aspects of e-voting but does not address certain technologies or solutions. Figure 5.1 depicts all assets and threats identified in the report of the technical experts group of the Council of Europe's initiative as well as the corresponding security objectives at a glance. The assets given in the recommendation are exhaustive and taken as the basis for these considerations. The election fundamentals stated by the Venice Commission [11] lay down the basis for all democratic elections. The following table 5.1 relates the assets to the election fundamentals. Table 5.1 gives a summary of assets separated into general assets and assets of the pre-voting phase, voting phase and post-voting phase (assets that appear in several voting phases are marked with a $^{*)}$). All fundamental rights except the right of direct suffrage can be associated with a corresponding asset. The fundamental right of direct suffrage is not a requirement for a technical solution, but rather is an organisational and legal issue. Thus, the corresponding column in table 5.1 is left blank.

For the full definition of all assets and threats as well as for a complete description of all security objectives, see the explanatory memorandum to the Council of Europe's recommendation [4] (appendix A of this thesis holds a copy of the relevant security objectives of the Council of Europe's recommendation).

The recommendations of the Council of Europe concentrate on election fundamentals and remain generic with respect to many details. So some recommendations could and should be more precisely defined according to the specific needs of Austrian elections. The protection profile developed by the BSI working group is of limited scope only, although a few elements of the BSI protection profile should be considered. Thus, in order to create an applicable risk analy sis, the Council of Europe's recommendation, or more precisely the risk analysis given in the technical appendix of the recommendation, was inspired by the requirements stated by the working group of the Austrian Ministry for the Interior's initiative and has been extended by selected elements in the BSI protection profile. The resulting list of security objectives is suitable as a set of minimum security requirements for the technical e-voting solution presented by this thesis. Figure 5.2 gives a summarised illustration of the compiled risk analysis (additions are marked with '**O**'). The following paragraphs explain the changes made.

The assets defined in the Council of Europe's security analysis remain unmodified as far as possible. From an abstract point of view, they seem to be suitable for Austrian elections. However, the security threats described in this recommendation are not exhaustive and additional threats need to be discussed. By following the reports of the working groups of the Austrian Ministry for the Interior and by considering the BSI protection profile, the introduction of further threats and security policies is needed. The following list only outlines the threats and security policies that were added. For an exhaustive description of inherent threats see the explanatory memorandum to the Council of Europe's recommendation [4].

[11] The author of this thesis was involved in both initiatives. He especially contributed to the work of the technical experts group of the Council of Europe with respect to risk analysis.

		Fundamentals				
	Assets	Universal Suffrage	Equal Suffrage	Free Suffrage	Secret Suffrage	Direct Suffrage
General	Authentication Data				X	
	Verifiabi./Observab.			X	X	
	System integrity	X	X	X	X	
Pre-voting	Candidate decision	X				
	List of candidates *)	X	X	X		
	Voters register *)	X		X	X	
	Nomination process	X	X			
	Nomination period	X	X			
	Privacy *)				X	
	Registration process	X	X	X	X	
	Registration period	X	X	X		
	Right to vote *)	X	X			
Voting	Ballot		X	X		
	List of candidates *)	X	X	X		
	Voters register *)	X	X	X	X	
	Right to vote *)	X	X	X		
	Vote *)		X	X	X	
	Voter’s decision *)			X	X	
	Voter’s privacy				X	
	Voting period	X	X	X		
	Casting of a vote	X		X	X	
Post-Voting	List of candidates *)	X	X	X		
	Counting process		X	X	X	
	Counting result		X		X	
	Election report		X		X	
	Vote		X	X	X	
	Reporting process		X		X	

Table 5.1: Summary of assets and their relations to election fundamentals.

1. **General Threats (T) and Policies (P):**

- *T.SystemMisuse* 1)
  Any form of accidental misuse, for example due to bad user interface design or lack of clear instructions, may lead to unintended results. For example, a voter might not understand how to use the user interface thus might not be able to cast her vote correctly. Or, an attacker could purposely aim to misguide a voter using forged user instructions thus might influence the voters’ behaviour or prevent voters from casting their intended votes.

- *T.UnauthorisedVoter* [2)]
  An unauthorised voter (an attacker) aims to cast a vote and influence the result. If there are a large number of unauthorised votes, an attacker could influence the election result significantly.
- *P.Accesibility* [1)]
  This policy requires the e-voting system to provide easy accessibility for everyone, but especially for people with disabilities. Here electronic voting offers a variety of possibilities for providing easier access to voting, e.g. by supporting special output equipment. Therefore, the e-voting system has to be compliant with existing accessibility guidelines, such as those provided by W3C consortium[12].

2. **Threats/Policies of the Pre-voting Phase:**
   No additional threats or policies required.

3. **Threats/Policies of the Voting Phase:**

   - *T.VoteProof* [1) 2)]
     Any information that might be usable for providing proof of a voter's decision could be used by the voter as an aide in selling her vote. The voter could use the information as proof to third parties that she voted in a certain way.
   - *P.VoteObligation* [1)]
     This policy requires the e-voting system to support enforcement of a legal obligation to vote. Thus, an e-voting system should record (upon request) which voter has cast her vote. The e-voting system should identify the voter while casting her vote, either directly through an explicit identification procedure or indirectly through her cast vote/ballot. However, the identity data collected by the system has to be able to identify voters uniquely. The identity data must be accessible by authorised persons only (e.g. election commission, etc.).
   - *P.VoterAbort* [2)]
     This policy requires an e-voting system to provide an abort function to the voter that can be used at any stage of the voting procedure. The voter should be able to cancel the procedure at any time.
   - *P.Overhaste* [2)]
     This policy requires an e-voting system to protect voters from casting her vote in haste. Additional confirmation should be requested from the voter before casting her vote.
   - *P.Correction* [2)]
     This policy requires an e-voting system to provide voters the possibility of correcting their vote before casting it.
   - *P.Acknowledgement* [2)]
     This policy requires an e-voting system to provide a clear and unambiguous acknowledgement to the voter that her vote has been successfully cast. The voter must be sure about this. (see also T.VoteProof).

[12] W3C Recommendation "Web Content Accessibility Guidelines", as seen at http://www.w3.org/TR/WAI-WEBCONTENT/ on 10 June 2007.

4. **Threats/Policies of the Post-Voting Phase:**

   - *P.ElectionCommission* [1)]
     This policy requires an e-voting system to consider the role of the election commission with regards to the counting procedure. Counting should be explicitly started by the election commission. Usually, the election commission consists of a number of representatives, thus the e-voting system should require a collaborative action of a representative number of members of the election commission.

Threats and policies marked with [1)] are adopted from the considerations in the e-voting study of the Austrian Ministry of the Interior [81]; threats and policies marked with [2)] have been taken from the BSI protection profile [82].

Due to the additional threats and policies defined, a number of additional security objectives are required. These security objectives are (sorted according to voting phases):

1. **General Security Objectives:**

   - *O.Usability*
     The e-voting system shall address usability starting from the very stage of design. The e-voting system should follow an intuitive and state-of-the-art usability schema. The design of the e-voting system should address a wide range of user groups.
   - *O.Accessibility*
     An electronic voting system should address the needs of users with disabilities. The system should adhere to existing accessibility guidelines.
   - *O.ElectionCommission*
     The election commission plays a special role which should be explicitly addressed by the e-voting system. Due to legal requirements, the election commission usually consists of a number of representatives. The e-voting system should require a collaborative activity of all—or at least of a specified number—of representatives.
     Application Note: For example, the e-voting system should require that all representatives of the election commission have to be present in order to start the counting process. This could be technically ensured by requiring all representatives to enter their personal secret code (e.g. password or cryptographic key).

2. **Security Objectives of the Pre-voting phase:**
   No additional security objectives are required.

3. **Security Objectives of the Voting phase:**

   - *O.Proof*
     The e-voting system should not provide any information to the voter which she could use as proof of her vote to third parties. Furthermore, all possible technical measurements should be taken to hinder voters from making screenshots or printouts of their vote.

4. **Security Objectives of the Post-Voting phase:**
   No additional security objectives are required.

The compiled catalogue of threats, policies and objectives is still very generic and thus has to be put down in concrete terms with respect to a dedicated election (depending on the election's specific needs). However, this compiled catalogue should provide a rudimentary basis for all types of Austrian elections.

The e-voting system presented in this thesis takes the security objectives drafted in this section as requirements so far as applicable. Some requirements—assets, threats, policies and objectives—address elements of an election which are not addressed by this e-voting system EVITA, e.g. candidate nomination is out of scope of EVITA.

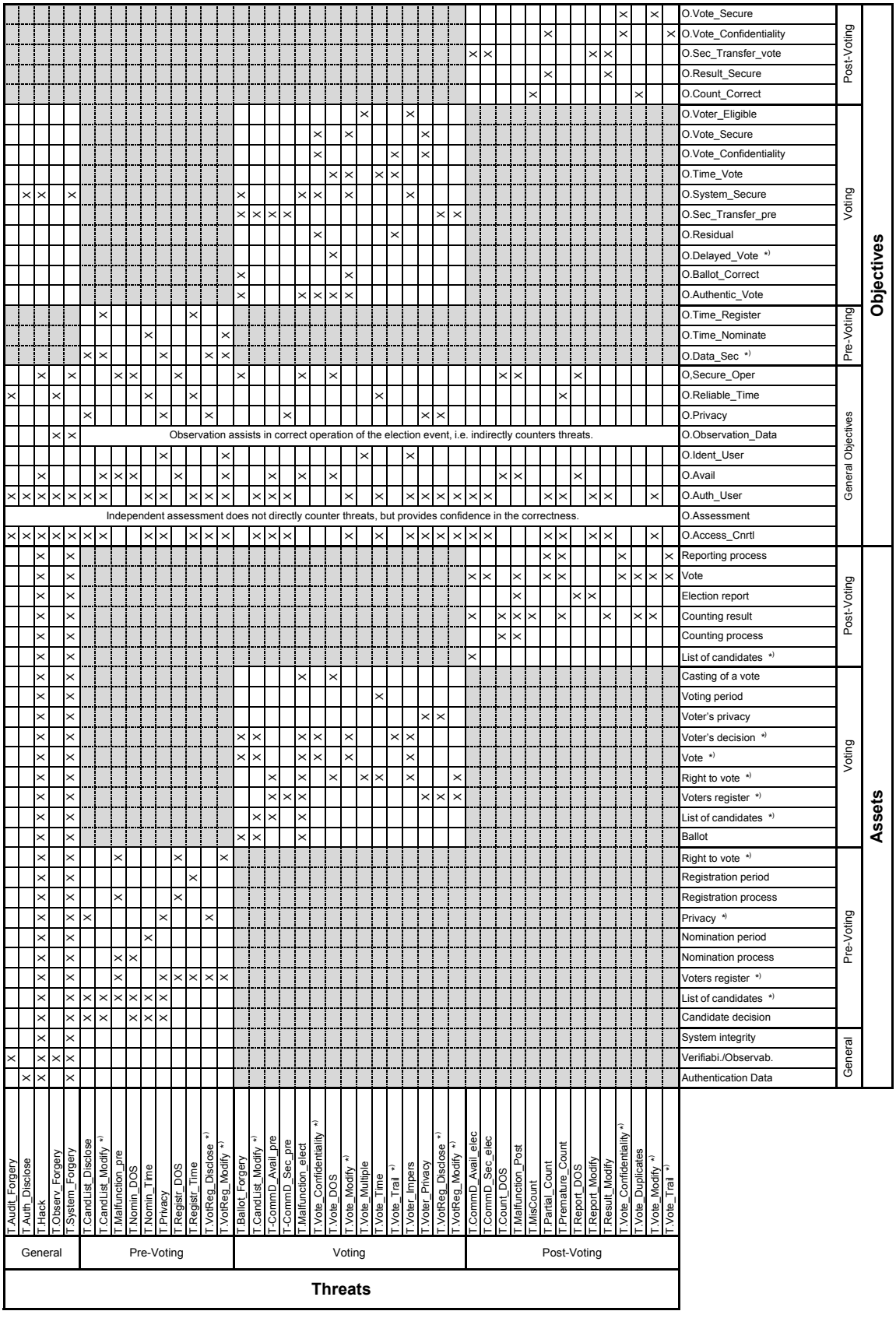

Figure 5.1: Summary of assets, threats and security objectives of the technical security recommendations of the Council of Europe [3] [4].

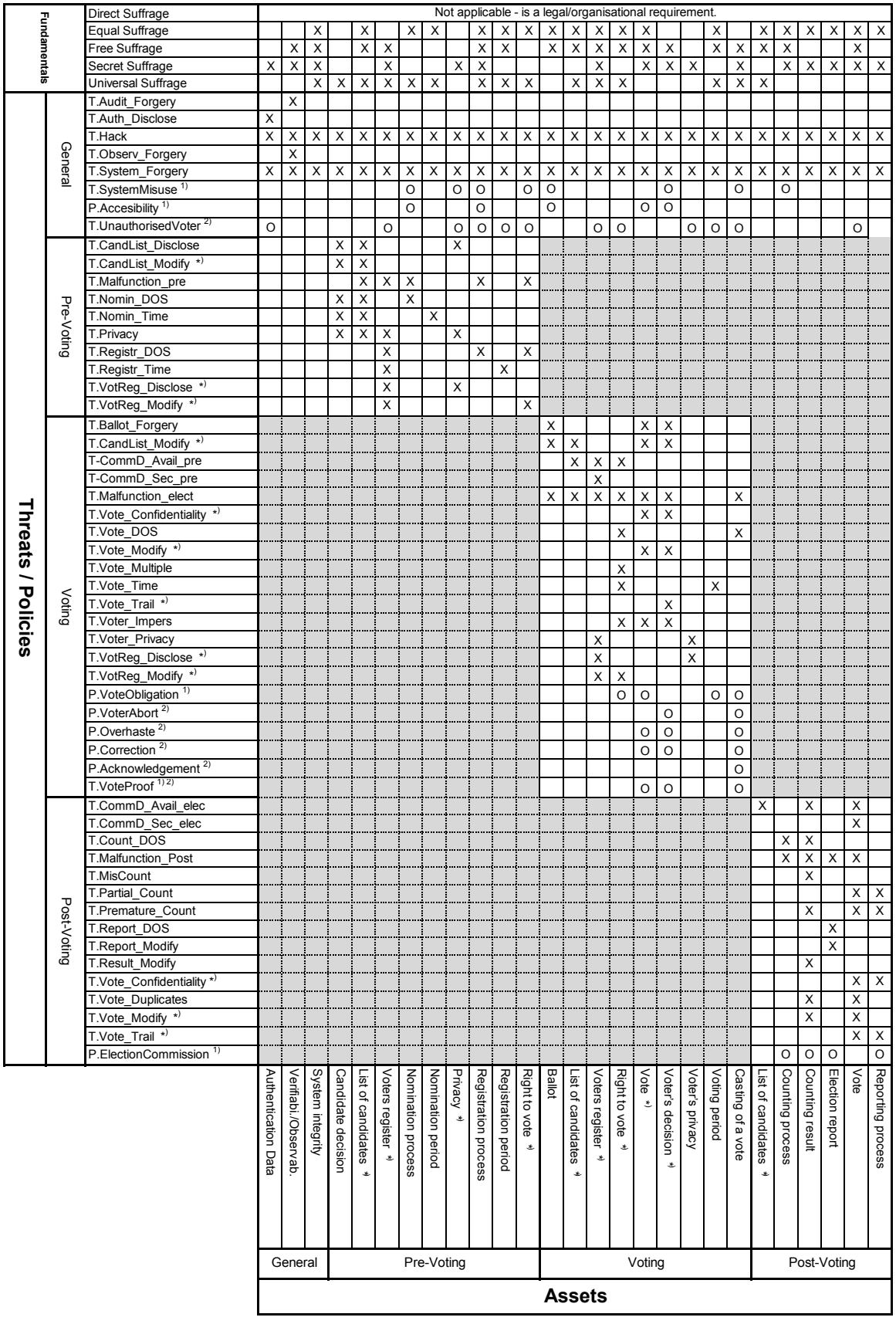

Figure 5.2: Summary of assets, threats and security objectives for the technical e-voting solution presented by this thesis.

Chapter 6

E-Government in Austria

E-Government is not only a technical framework but also covers an embracing legal and organisational framework. Therefore, Austria, as one of the leading member states of the European Union with respect to e-Government[1], has put a number of laws in place regulating e-Government issues. The most important law with respect to e-Government is the E-Government Act [85]. It lays down all necessary regulations for e-Government and defines fundamental concepts such as the Austrian electronic identity management system.

Identity management (i.e. how can a person can be identified uniquely[2]) and electronic identities in general affect all e-Government applications that deal with people (as well as legal entities). Thus, electronic Identity (e-ID) is a key enabler for e-Government and e-Government applications.

Austria started developing an all-embracing electronic identity management system that aimed from the very beginning to identify persons uniquely and also to protect a maximum of privacy. As a result, Austrian e-Government is based on the award-winning[3] e-ID concept, represented by the Austrian Citizen Card, which heavily influences other countries as well as the European movement toward building an interoperability framework.

Since the E-Voting solution presented in this thesis is based on the core concepts of Austrian e-Government, this chapter introduces its most important elements. The following sections explain the Austrian e-ID and the Austrian Citizen Card concepts in detail and discusses some additional, notable e-Government components.

[1] At the time of writing, the e-Government benchmarking study 2006 by Cap-Gemini designates Austria as being number one amongst EU member states with respect to e-Government services.

[2] The terminology paper [7] provided by the **modinis**^{idm} study defines "Identity Management" as follows: "*Identity Management is the managing of partial identities of entities, i.e., definition, designation and administration of identity attributes as well as choice of the partial identity to be (re-) used in a specific context.*"

[3] The Austrian Citizen Card concept received first prize at the Second European Seminar on Best Practices in Data Protection in Public Administrations in Madrid in December 2005. Furthermore, Univ.Prof.Dr. Reinhard Posch, Chief Information Officer of the Austrian Federal Government, received the "ID Community Award" 2006 for "[..] *driving the issues surrounding eID security to the forefront of the EU community and encouraging other Member States to begin discussions on eID interoperability.*", taken from http://www.idworldonline.com/index.php?id=idpa06winners as seen on 6 July 2007.

6.1 Electronic Identity Management in Austria

This section introduces the Austrian electronic identity management system and describes the basic mechanisms used. The Austrian identity management concept lays out a good base for enabling unique identification while maintaining a maximum of privacy. However, providing sufficient identity management makes e-voting one of the most challenging e-Government applications. The citizen has to be identified uniquely, but the vote should remain anonymous at the same time. Therefore, it is important to highlight the fundamental principles of electronic identities in Austria since the proposed e-voting schema is fully based on it. The following sections give an overview of the Austrian electronic identity management concept in general and the Austrian Citizen Card in particular.[4]

6.1.1 Unique Identity—the Source PIN ($sPIN$)

Austria established its Central Residents Register (CRR) in 2002. Every person residing in Austria is registered in the Central Residents Register and is assigned a unique Personal Identification Number (PIN), called a CRR-number. Similar registers have been created for legal entities, e.g. the Register of Company Names for companies, the Register of Associations for organizations, etc. Any other person or entity which does not fit in the registers mentioned can be registered with the Supplementary Register (SR). As a result, any person or entity in Austria can get a unique PIN. However, in order to explain the principle of the electronic identification system, the following section only takes private persons into consideration.

The base register numbers (CRR or SR number) of a private person are not used as unique identification numbers in the Austrian electronic identification system. These numbers are only allowed to be used in particular places, e.g. in the system of registration, and their use is strictly regulated by law. However, CRR numbers are allowed to be used for statistical purposes as well (in accordance with the legal regulations laid down in [87]). This makes the use of existing base register numbers undesirable due to privacy reasons. Instead, a specially derived number, called the Source Personal Identification Number (sPIN), is introduced as the base unique identifier for electronic identification.

The creation of the $sPIN$ is based on cryptographic one-way functions and symmetric encryption. As illustrated in figure 6.1, a person's CRR or SR number is taken as input for the $sPIN$-creation. First, the person's CRR or SR number is converted into a binary representation. Next, a secret seed value is added to the binary representation of the person's base number. Finally, the seeded value is encrypted by applying 3DES encryption using a secret key. The resulting encrypted value is converted to a base-64 encoding in order to have a printable representation. This encoded encrypted value is the person's $sPIN$. The detailed algorithm for $sPIN$-creation is specified in [86].

The Source PIN Register Authority is the only authority that is legally empowered to create Source PINs based on numbers taken from Austrian base registers. Thus, the secret seed value as well as the secret key used for 3DES encryption is securely held by the Source PIN Register Authority.

The usage of the $sPIN$ is strictly regulated by law. The only place where a person's $sPIN$ is allowed

[4] The author of this thesis has worked on several projects involving identity management, not only from the point of view of Austria but also from an international perspective. Thus, he contributed to the Austrian Citizen Card concept, e.g. further development of the Austrian Citizen Card concept, development of electronic mandates, acceptance of foreign e-IDs, etc. In addition, he worked for the **modinis**^{idm} study [86] of the European Commission. The **modinis**^{idm} study aimed to yield a survey of existing identity management solutions and to sketch up a possible European e-ID interoperability framework.

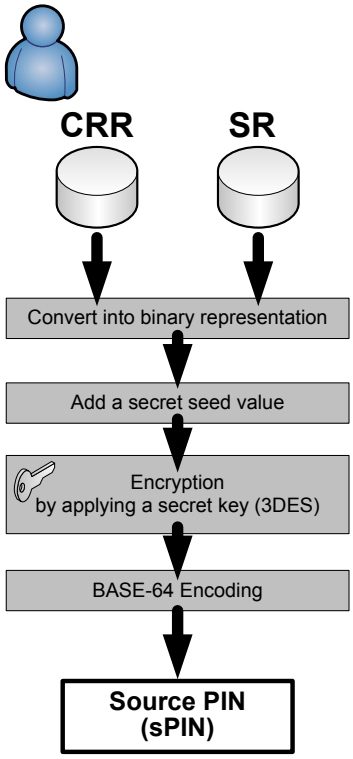

Figure 6.1: The principle of Source PIN generation.

to be stored is in the person's Citizen Card. No authority or governmental application is allowed to give out or store a $sPIN$ directly. Although the name "Source PIN Register Authority" might lead to the misinterpretation that this authority maintains a register holding all Source PINs, no central register exists for storing Source PINs. Thus, a citizen's $sPIN$ is under the sole control of the citizen which makes it a very citizen-centric solution with regards to privacy. However, the Source PIN Register Authority is allowed to recreate a citizen's $sPIN$ in the course of creating a Sector Specific PIN (the definition of Sector Specific PIN is given in the following section) for a dedicated, foreign sector without involving the citizen or her Citizen Card under certain legal circumstances. From a legal and technical point of view, this is a complex task since several organisations and authorities are involved in it and a clear legal mandate must exist.

The above described the situation for private persons. Electronic identification works slightly different for legal entities (e.g. corporations and companies, registered associations and etc.), because they are not entirely covered by the regulations in the Data Protection Act [25]. Source PINs for legal entities are taken directly from their base registers, e.g. the register for companies. No further cryptographic derivation mechanism is applied to these base register numbers. For example, the $sPIN$ of a registered company is its register number taken from the Register of Company Names.

6.1.2 Sectoral Identifier—the Sector Specific PIN ($ssPIN$)

In order to further protect privacy, the $sPIN$ created is not used directly by applications for the purpose of identification. Instead of using a single $sPIN$ to identify a person in all the different governmental applications, further derivations of the $sPIN$, called Sector Specific Personal Identification Number (ssPIN), are introduced.

In Austria, all governmental applications are divided by law into different application sectors. The relevant law [88] currently defines 35 different sectors of governmental applications, e.g. the “Taxes and Charges”, “National Defense”, or “Health” sectors. Furthermore, these sectors might be further segmented if applicable. Each governmental sector is assigned a specific alphanumeric code. For each of these sectors, the Austrian e-ID concept foresees using a separate unique identifier for identification purposes called the Sector Specific PIN ($ssPIN$).

The $ssPIN$ is created by combining the $sPIN$ with the sector’s alphanumerical code and applying a cryptographic one way function (a HASH function). Thus, based on a person’s $sPIN$ various $ssPIN$ can be created. Each $ssPIN$ is different and due to the application of a one way function it is impossible to calculate the underlying $sPIN$ or any other sector’s $ssPIN$ from a given $ssPIN$. In figure 6.2, the basic steps of the $ssPIN$ creation process are illustrated for two different sectors.

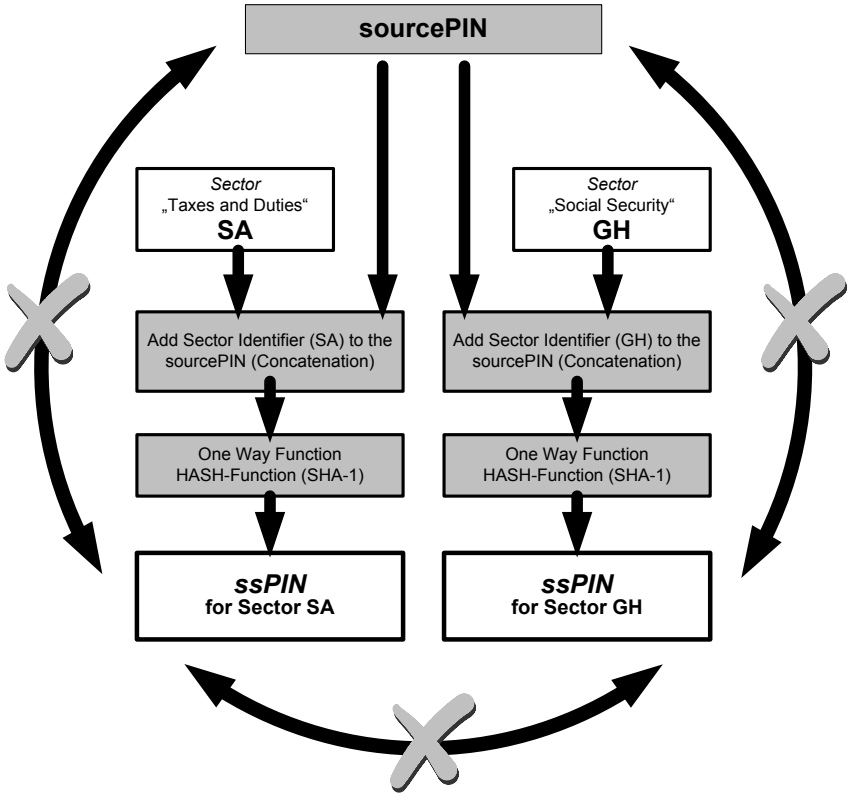

Figure 6.2: Workflow to create $ssPIN$ based on a given $sPIN$; it is not possible to calculate the underlying $sPIN$ nor any other sector’s $ssPIN$ from a given $ssPIN$

The use of sector-specific identifiers is not foreseen with respect to legal entities. Since the $sPIN$ of a

legal entity is its base identifier, which is publicly available, e.g. the number taken from the register of companies is printed and used on nearly every official document of a company, the introduction of sector identifiers would yield no improvement. Therefore, sectoral identifiers do not exist for legal entities. Instead legal entities are identified in applications using their Source PINs directly.

6.2 Concept of the Austrian Citizen Card

The Citizen Card concept is the technological framework for the Austrian e-ID concept which handles electronic identification and authentication of citizens. It also provides a number of additional functionalities which are needed within e-Government applications. For instance, the Citizen Card concept specifies a huge set of commands for creating XML digital signatures of various kinds following [89], and provides encryption and decryption functionality in accordance with the XML Encryption Standard [90][5]. However, the main objective of the Citizen Card concept is to identify and authenticate citizens.

For authentication purposes, the Citizen Card concept makes use of electronic signatures according to the European Directive on Electronic Signatures [29] and the Austrian Signature Law [26]. The basis for a Citizen Card following this concept is a secure signature creation device in accordance with the respective laws. For identification purposes, the Citizen Card concept makes use of the $sPIN$ as defined previously. In order to authenticate a citizen in relation to the $sPIN$, an Identity-Link is introduced.

The Identity-Link is an XML-based data structure which combines the $sPIN$ of the citizen with the citizen's electronic signature. In other words, the Identity-Link combines the citizen's $sPIN$ with her public keys that are used to verify her electronic signatures. The Identity-Link itself is signed by the issuing Source PIN Register Authority to confirm its authenticity. Therefore, using the Identity-Link it is possible to create the relation between a citizen's electronic signature and her claimed identity. To do so, an application which wants to identify and authenticate a citizen will need to compare the electronic signature created by the citizen using her Citizen Card with the public key wrapped in her Identity-Link. If the public key can be mapped to the electronic signature, the electronic signature can be considered as a proof of authenticity for the claimed identity. In other words, it can be strongly assumed that the person who possesses the signature creation device (i.e. the Citizen Card) and knows the secret code required to release signature creation is the person described in the Identity-Link. Thus, the $sPIN$ saved in the given Identity-Link represents the unique electronic identity of the citizen in question. In this way, an Identity-Link is comparable to a digital certificate for electronic signatures. In contrast to a digital certificate, the Identity-Link contains the citizen's $sPIN$ which remains the same for a citizen throughout her lifetime. This cannot be guaranteed for the serial number of the digital certificate. However, digital certificates are usually publicly obtainable through directories for signature verification purposes, thus a $sPIN$ held in a digital certificate would not be as protected adequately enough as required by law. Therefore, the Austrian Citizen Card concept introduces the Identity-Link.

On a technical level, the Citizen Card concept defines an abstract XML interface, called Security Layer, which provides abstract commands based on a request-response schema. Since the Security Layer is very abstract, there is no limitation for the technical implementation of the Citizen Card concept. This means that an implementation of the Citizen Card could be built using smart cards, but could also realized using any other technical device which fulfils the requirements specified in the concept.

[5]For encryption purposes, the Citizen Card specification recommends using a separate, additional key-pair. Thus, a Citizen Card typically holds two key-pairs: one for creating electronic signatures, and the second for encryption purposes.

In Austria, there is not just a single type of "Citizen Card". There are several different cards and signature creation devices that may be used as Citizen Cards. For example, the Austrian health insurance card, the e-card, could be activated to function as a Citizen Card by its owner[6]. Moreover, every bank card issued since February 2005 is capable of creating electronic signatures according to the Austrian signature act and can therefore also be used as a Citizen Card. However, the Citizen Card Concept is not only implemented using smart cards but also using alternative technologies as well. For instance, the "A1 Signature" is a cardless implementation of the Citizen Card concept provided by the Austrian mobile phone provider, which uses the citizen's mobile phone in order to authenticate the citizen (the mobile phone is used for user authentication; signatures are created on a secure server).

The Austrian Citizen Card is not merely a certain type of card but rather a concept defined by a set of technical specifications[7][8]. Although it is mainly intended to be used for e-Government applications, it serves several additional functionalities and could, and even should, be used for applications apart from e-Government as well.

Citizen Card Environment

The Citizen Card Concept is a set of requirements and specifications whereas the requirement for creating electronic signatures is one of the major criteria for any implementation of the Austrian Citizen Card concept. However, since the Citizen Card concept defines an abstract XML interface for accessing Citizen Card functionality, some form of additional middleware is needed to act as intermediary between the signature creation device and defined Security Layer interface. Furthermore, some functions of the Citizen Card Concept do not use the signature creation device and its cryptographic mechanisms. Thus, the Citizen Card Concept is much more than just a signature creation device combined with a certain type of driver software. It consists of several additional components arranged around and on top of the signature creation device. The sum of all elements and components implementing the Citizen Card concept is denoted as the Citizen Card Environment (CCE). Figure 6.3 roughly outlines a plan for a Citizen Card Environment[9]. As this sketch shows, a Citizen Card Environment consists of many additional parts and elements beside the signature creation device. For example, a Citizen Card Environment embraces XML modules for parsing and processing XML-commands received through the Security Layer interface, and includes cryptographic software modules as well as graphical user interfaces. Additionally, a secure viewer component is required for signature creation according to Austrian law. The secure viewer component guarantees that the signed document does not contain dynamic or hidden elements which could yield ambiguous representations. Thus, the signer of the document can be confident that the document will be displayed during the verification process exactly the same as during the signature creation process.

[6] Each person insured by Austrian social security holds an e-card, therefore already has a potential Citizen Card.

[7] The Citizen Card Concept is laid down through [91] and legally established by the Austrian E-Government Act [85]. A working group established by the Federal Chancellery is responsible for the maintenance and further development of the Citizen Card concept. The author of this thesis chairs this working group.

[8] Due to the fact that the Citizen Card is a concept, several technical implementations may be possible. For instance, the author of this thesis discussed a full Citizen Card implementation based on mobile phones in [92].

[9] This plan was created by the author of this thesis as input for a discussion regarding a recommended modularisation of smartcard-based Citizen Card Environments. This plan has been discussed in the Citizen Card working group of the Federal Chancellery.

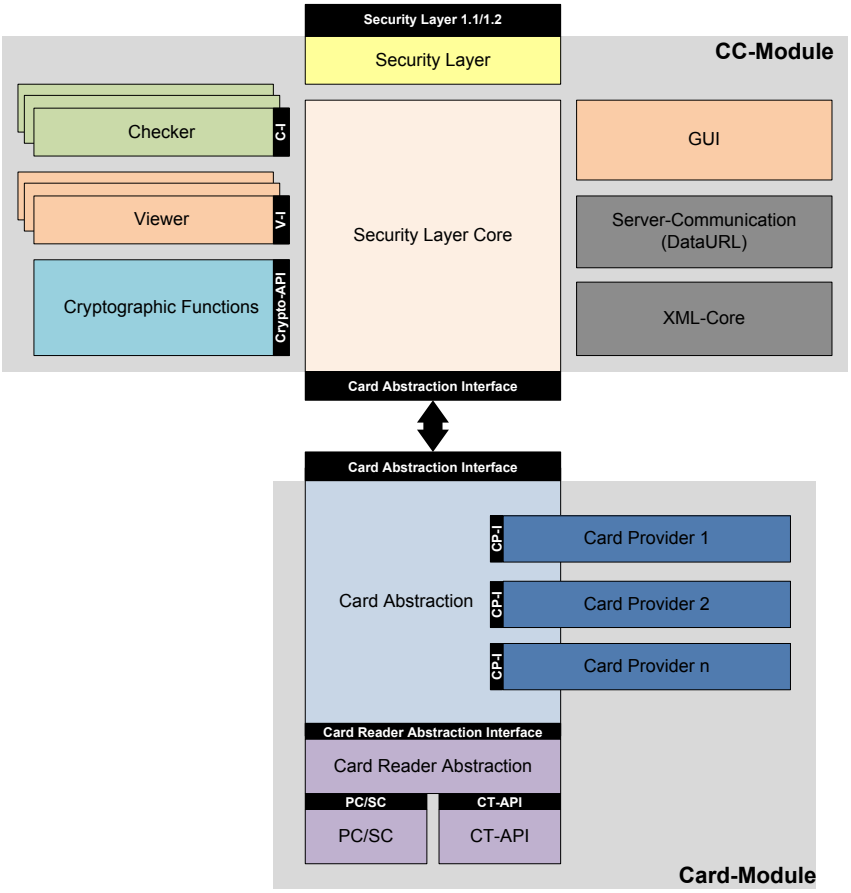

Figure 6.3: Example of a plan for new Citizen Card Environments [5]

6.3 Further Specialties of the Austrian E-Government

Various further elements and concepts increase the complexity of the Austrian electronic management system exponentially. The following sections highlight two examples, namely the integration of foreign electronic identities into the Austrian e-ID system and the concept of electronic mandates[10].

6.3.1 Recurring Identities and the Integration of Foreign e-IDs

The Austrian E-Government Act [85] defines two types of identities, as follows[11]:

- ***Unique identity**: designation of a specific person by means of one or more features enabling that data subject to be unmistakably distinguished from all other data subjects*

[10] The author has contributed largely to the development of both concepts. The concepts have been published through [93] [94] [91].

[11] The Austrian E-Government Act [85] will be amended by the end of 2007. In the course of this, the regulations about recurring identities and the integration of foreign e-IDs will be modified.

- ***Recurring identity****: designation of a specific person in a way which, while not ensuring unique identity, enables this person to be recognised by reference to a previous event, such as an earlier submission;*

[85]

As described before, the $sPIN$ represents a citizen's unique identity in the meaning of the E-Government Act. In contrast to this, a recurring identity does not have to provide unique identification throughout a citizen's lifetime. Thus, a recurring identity can be assigned to persons not registered with in of the Austrian base registers, e.g. citizens of other European member states. The basis for creating a recurring electronic identity is to use data that guarantees that the person associated with the data can be repetitively recognised. This idea is especially useful for foreign electronic identities, since the unique identification number used in a foreign e-ID fulfils this requirement and thus can be used as feature to identify a person repetitively. In other words, the unique PIN of a foreign e-ID, called the Substitute Source PIN, can be used to create a substitute for the $sPIN$ with respect to recurring identities. The detailed requirements for a foreign e-ID being used as a recurring identity are laid down in the administrative order regulating matters of the Source PIN Register Authority [95].

In addition to the requirements for a unique foreign identification number being used as a recurring identity, the foreign e-ID has to make use of electronic signatures according to the European Signature Directive [29] as required by the administrative order [95] and by the Austrian Citizen Card concept. However, even a recurring identity is represented by an Identity-Link that combines the Substitute Source PIN and the public key of the underlying electronic signature. This Identity-Link can then be used in Austrian e-governmental applications as a recurring identity similar to an ordinary Identity-Link of an Austrian citizen.

From a technical point of view, the foreign e-ID and the underlying signature creation device—i.e. smart card—has to be integrated into a Citizen Card Environment which then allows accessing of the foreign e-ID by use of the abstract Security Layer interface. Furthermore, a Citizen Card Environment must be capable of handling the foreign signature creation device. This is not a big issue, however, since many signature creation devices—e.g. smart cards—make use of standardised interfaces.

Integrating Finnish and Italian e-ID

As a case study, the e-IDs of Finland and Italy have been integrated into the Austrian identity management system following the principle previously described. Both Finnish and Italian e-IDs make use of electronic signatures that are in accordance with the European Signature Directive [29]. Thus, these e-ID systems satisfy the requirements of the Austrian Citizen Card concept and are qualified for being used as recurring identities.

In order to use these foreign e-IDs in connection with the Austrian electronic identity management system, a new Citizen Card Environment prototype has been developed. This prototype enables the incorporation of arbitrary signature creation devices through the standardised PKCS#11 interface. Since both Finnish and Italian e-IDs support the PKCS#11 interface, this prototype is able to integrate both of them seamlessly.

For identification purposes, a Substitute Source PIN can be created based on both foreign e-IDs. In the case of the Italian e-ID, a tax number is assigned to every Italian citizen as a unique personal identification number within Italian e-Government. Therefore, according to the regulations laid down in the adminis-

trative order [95], this tax number can be directly used as the basis for creating a Substitute Source PIN. In contrast to the Italian e-ID, the Finnish e-ID does not provide any similar unique identifier, so the serial number of the digital certificate of the Finnish e-ID is taken as the basis for creating an according Substitute Source PIN. The law even explicitly allows the use of serial numbers of digital certificates as the basis for creating a Substitute Source PIN. Moreover, since a recurring identity is not necessarily a unique identity, it is not required for the Substitute Source PIN to remain the same throughout a person's lifetime. Thus, the serial number of a certificate concatenated with the name and the country of the issuer of the certificate serves as a perfect basis for creating a recurring identity.

However, the process of creating Substitute Source PINs for the Finnish and Italian e-IDs is depicted in figure 6.4. Since the tax number as well as the certificate's serial number are usually not secret in a recurring identity, a Substitute Source PIN could be created by anybody. Thus, the process of creating Substitute Source PINs includes a keyed-Hash Message Authentication Code (HMAC) applying a secret key due to privacy reasons. The key used is kept secret by the issuing authority, the Source PIN Register Authority. As a result, it is not possible to calculate the base identification number from a given Substitute Source PIN, neither can a Substitute Source PIN be created without knowing the secret key.

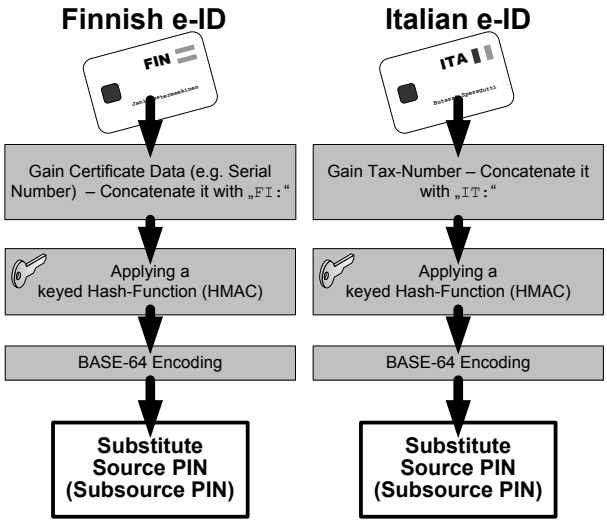

Figure 6.4: The derivation of the Substitute Source PIN (subsourcePIN) for the Finnish and Italian e-ID

The Substitute Source PIN is treated like an ordinary $sPIN$. It is also wrapped in an Identity-Link structure combining the public key of the electronic signature with the Substitute Source PIN. In contrast to an Identity-Link representing a unique identity, the Substitute Source PIN inside the Identity-Link is marked as a recurring identity. The whole Identity-Link is signed by the issuing authority. Thus, using the Identity-Link based on the foreign e-ID and using Citizen Card Environment prototype, the citizens of Finland and Italy could access all Austrian e-government services that require a recurring identity.

As part of the proof of concept, a web service was developed which offered the possibility to request an Identity-Link representing a recurring identity generated using a foreign citizen card. In the course of this issuing process, the foreign citizen is asked to apply for an Austrian identity based on a Substitute Source PIN. The application has to be signed by the foreign citizen using her qualified certificate. After verifying the signature, the service uses the certificate along with the signature to gain all necessary data in order

to generate a Substitute Source PIN. Finally, the Substitute Source PIN is wrapped in an Identity-Link that represents the resulting recurring identity which is then stored in the Austrian Citizen Card Environment, e.g. our prototype Citizen Card Environment mentioned above. As a result, the requester is able to use e-governmental applications with the Austrian e-ID that was created.

The introduction of recurring identities based on foreign e-IDs should serve as an example of e-ID interoperability. Interoperability of electronic identities is considered one of the most challenging topics in the near future for e-Government[12]. The European Commission has put e-ID interoperability on the top of their project agenda and with good reason. The upcoming European large scale pilot project involving electronic identities testifies to this. However, recurring identities are an early attempt to demonstrate interoperability from a member state's perspective in a unidirectional manner.

6.3.2 Representation and Authorisation—Electronic Mandates

Empowering a person to act for another person or to conduct a certain transaction are important legal elements in everyday business. Empowering is almost always implicitly accepted in various situation, e.g. if a parent acts for her minor child or if a businessman acts on behalf of his company. Both scenarios are examples of authorisation because a person becomes authorised to act under delegated power. In the former example, the law empowers parents to represent their child in business. If a parent wants to act for her child in a conventional business, it is almost always sufficient to claim to be the parent. In the "worst" case, the adult would have to prove her identity and if the surname of both the adult and the child are the same, then parenthood is usually deemed to be proved. In the latter example, when "claiming" that a businessman acts in the name of some company it is often sufficient just to present a business card. Often no further proof is required, depending of course on the intended action[13].

Both examples demonstrate that authorisation and representation are elements of daily life that are taken for granted implicitly. In everyday life, proof of authorisation is not usually required, but when working with electronic transactions, authorisation has to be expressed explicitly. This creates a need for having an electronic form of empowerment and representation. The vehicle for achieving this is the concept of electronic mandates (further information can be found in [99] [100] [101]; electronic mandates are specified in [102]).

Electronic mandates were introduced into the Austrian identification schema in 2006 for two main reasons. On the one hand, electronic mandates are the electronic equivalent of conventional mandates for empowering a person, in which a representative acts for another person, referred to as the mandator under certain circumstances. On the other hand, electronic mandates serve to close the gap between private persons and legal entities with respect to the Austrian electronic identity management system. Citizen Cards in Austria are issued to private persons only[14]. Legal entities cannot possess a Citizen Card and thus cannot actively participate in e-Government.

On a technical level, an electronic mandate is a specific XML structure containing at least [102]:

[12] The author of this thesis works in the field of e-ID interoperability very actively. Beside his engagement within the **modinis**^{idm} study, he contributed to [96] [97] [98].

[13] Depending on the action and the transaction value, proving one's authority to act is inevitable, especially in business to business or government to business relations.

[14] This is due to the requirement that a Citizen Card has to make use of qualified signatures according to the Austrian Signature Act [26]; the Signature Act further requires that qualified certificates (required for creating qualified signatures) can be issued to private persons only.

- identity of the mandator
- identity of the representative
- date and place of issuing
- content and concern of the mandate
- optional restrictions

The electronic mandate holds the electronic identity of the mandator (i.e. the person who empowers another person to act in her name). The identity of the mandator is denoted by her first and last name, date of birth and her Source PIN. The electronic mandate is the only place, with exception of a citizen's Identity-Link, that a person's Source PIN is allowed to be stored. The identity of the representative is similarly formulated by her full name, date of birth and Source PIN.

The main concern of this mandate is formulated in a textual description, more precisely, in arbitrarily combinable textual description blocks. It is expected that standard text blocks will come up for all types of standard mandates, e.g. mandates representing a procuration. In addition to the textual description of a mandate's concern, optional restrictions may be applied. Restrictions are formulated using specified XML-elements.

The concept for electronic mandates introduces an electronic mechanism for revoking a mandate. The introduction of this technical revocation mechanism is a great improvement in comparison to conventional mandates and it is especially necessary for electronic mandates. On the one hand, it is sufficient from a legal perspective to revoke a mandate by publicly announcing a revocation. Consider conventional paper-based mandates: if the representative is still in the possession of a paper that pretends to act as a valid mandate, the representative would still be able to act illegally in the name of the mandator. Thus, the only effective way to avoid this problem is to request that the representative destroy the paper mandate, which would prove hard to verify. With electronic mandates, this situation is much more difficult since the representative could create an arbitrary number of copies of the electronic mandate and the mandator could never be sure whether any illegal copies still exist. An electronic revocation mechanism is therefore very desirable for electronic mandates.

Although the electronic revocation mechanism is optional it is strongly recommended to add it to every electronic mandate. To make an electronic mandate electronically defeasible, the mandate needs to be registered with a certain revocation service. As a result, electronic mandates hold an Internet address that provides revocation information on request. When attempting to verify an electronic mandate, the named revocation service has to be asked about the current revocation status by using the serial number of the electronic mandate. A similar revocation mechanism for digital certificates is already widely used and well-established. Thus, the concept of mandate revocation was made similar to the revocation mechanism of digital certificates.

Electronic mandates are stored in the Citizen Card of the representative. This means that the representative holds not only her own $sPIN$ but also the $sPIN$ of the mandator. This is the only exception to the rule that a person's $sPIN$ is only allowed to be stored on her own Citizen Card. Every time the representative makes use of a mandate, she has to use her Citizen Card to prove her own identity by applying the Identity-Link and an electronic signature. She must also declare to the e-Government application that she is acting rightfully in the name of the mandator by showing the electronic mandate.

The electronic delivery service[15] was one of the very first e-Government applications which accepted electronic mandates. Mandates are especially important for the Austrian electronic delivery service since legal entities are only able to register for electronic delivery with the use of electronic mandates (a private person has to act in the name of a legal entity). However, mandates are an important element of the Austrian electronic identification system in general and thus enrich the Austrian e-Government framework.

[15]The Austrian electronic delivery service is the electronic equivalent of postal registered letters. Public authorities may send notifications and documents through this service to citizens. In exchange, the citizen has to sign an acknowledgement of receipt.

Chapter 7

The EVITA Concept

Austrian law allows postal elections under certain circumstances. Austrian legislation specifically mentions the electronic voting in two types of elections; the elections for the Austrian Chambers and the Austrian National Union of Students. These two democratic elections were the models used for the EVITA e-voting concept. In other words, the EVITA e-voting system should be able to conduct these two elections according to the needs of the Austrian law.

The requirements stated by law for both types of elections are very similar. However, the election of the Austrian National Union of Students has been chosen as the target scenario for the EVITA e-voting schema. One reason for choosing the election for the Austrian National Union of Students is that e-voting trials have been conducted already[1]. These e-voting trials followed a technical and organisational approach different than the EVITA voting model. Furthermore, these trials only focused on core aspects rather than being a complete and comprehensive e-voting solution. A legal and organisational description of the election for the Austrian National Union of Students is given in section 2.3.

This chapter introduces the core elements of the proposed EVITA-voting concept as it applies to the target election. It lays down the theoretical basis for the following discussion on the process models of the EVITA-concept provided in chapter 8.

7.1 EVITA-Voting Model

The EVITA voting model aims to follow the process model of conventional postal elections for three reasons[2]. First, both postal and electronic elections are a type of remote election. From a legal perspective, there is no big difference between these forms of remote elections. From a very abstract point of view, the only difference is the communication medium. Secondly, electronic elections should be conducted parallel to conventional elections. Furthermore, the conventional postal election could be used as be a fallback system in case the electronic voting system breaks down or any of its required technical com-

[1] Reports of these trials are given in [43] and [71]; section 4.2 introduces the e-voting schema used by the e-voting System of the University of Economics.

[2] In anticipation of the following sections, the EVITA e-voting concept introduces an Asserting Authority for blindly signing (asserting) cast votes. The Asserting Authority as well as the whole asserting process does not seem to be compliant with the process model of simple conventional postal elections. However, the basic process flow of postal elections is still kept, thus both process flows are still comparable.

ponents, e.g. the Internet, cause problems. The third rationale behind designing the e-voting process according to the process of conventional postal elections is that voters are already acquainted with the steps to be carried out in an election and therefore are more likely accept the e-voting system.

The postal election model has two phases. In phase one, voters have to register and in phase two the voting process is carried out. In order to map this election model to an adequate e-voting system, the basic process is kept. Therefore, the phases of the EVITA e-voting concept are:

1. phase one: the voter registers for electronic voting.
2. phase two: the voter casts her vote based on the registration.

Figure 7.1 contains a sequence diagram that shows both phases of the EVITA voting concept. Chapter 8 elaborates the process model in detail.

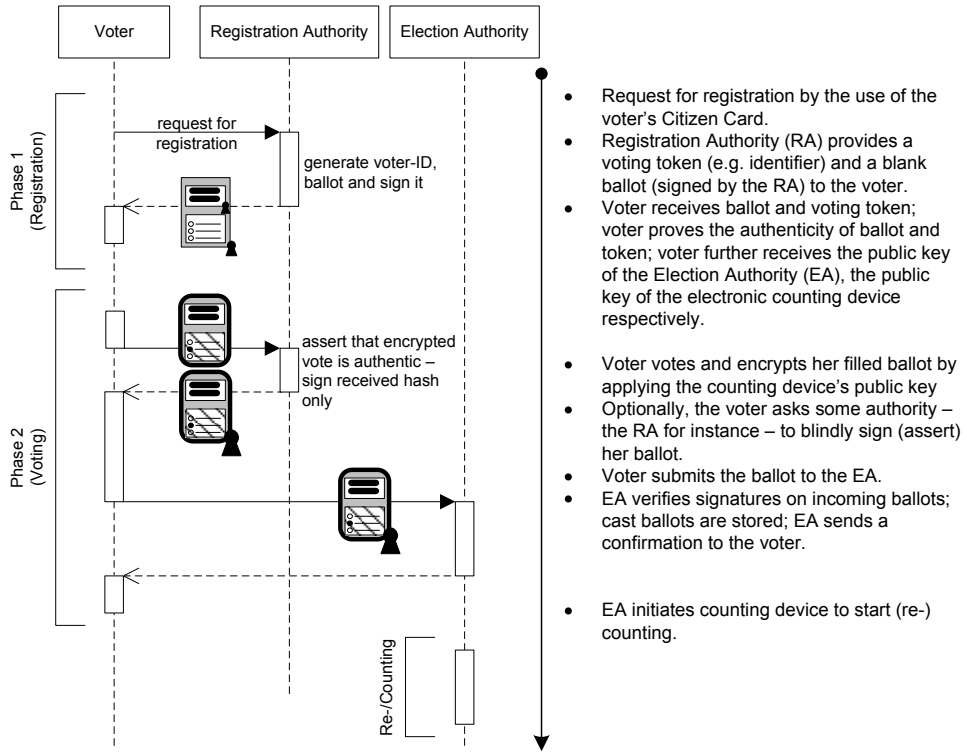

Figure 7.1: The two phase model of the EVITA voting concept at a glance [6]

7.2 Core Elements of the EVITA Schema

An e-voting schema must guarantee that a voter's decision (her vote) remains secret. To achieve this, two distinct approaches seem to be promising. One approach is to have a voting scheme that prevents the vote from being spied on by applying cryptographic methods. Another approach for protecting the secrecy of the ballots is by removing any form of identifying information from the cast vote thus breaking

any link between the voter and her cast vote. Both approaches have drawbacks and advantages. Furthermore, regarding the requirements given by the targeted use-cases neither approach by itself would be satisfactory. Therefore, the EVITA schema combines both approaches in an effort to build a comprehensive e-voting concept.

In the first approach, the use of encryption algorithms seems to be adequate. Various strong encryption algorithms exist, so question that remains is how and where to hold the decryption keys needed to decrypt votes. There are several schemes which do not need to decrypt votes in order to count them, but those approaches have limitations regarding write-in votes or they are too complex[3]. Contrary to the schemes that use homomorphic encryption algorithms, the EVITA schema makes use of asymmetric encryption and has well-designed key management.

However, the use of strong encryption algorithms in order to protect the secrecy of ballots is no guarantee that these algorithms will be able to resist attack in the future. Due to the ever-increasing power of new computer systems it could become quite easy to crack a given encrypted vote by a brute force attack (e.g. by trying all encryption keys possible). The following example describes possible consequences with respect to the decryption of votes. In 1938, Austrian citizens were asked to vote on the annexation of Austria by the German Reich. In the course of an election campaign in the late seventies (about forty years later), it would have been interesting to find out how people voted in the election of 1938. Assuming that the election of 1938 was conducted electronically using some sort of encryption algorithm, the computational power of computer systems forty years later should be sufficient to easily crack votes of the past.

The use of encryption only guarantees secrecy for a certain amount of time. Thus additional stringent organisational and technical measures are necessary. Therefore, the EVITA schema follows the second aforementioned approach and also introduces an additional mechanism to keep cast votes anonymous throughout the election and beyond. Due to a sophisticated identification and authentication model that is based on the Austrian identity management concept[4], it can be ensured that the identity of a voter cannot be determined based on her cast vote, especially after the election. This eliminates the the progressive weakness inherent to encryption algorithms.

To summarize, using strong encryption mechanisms in combination with a comprehensive identity management concept are the key elements of the EVITA e-voting schema. The first element ensures that the voter's decision remains a secret throughout and beyond the election event. The second element guarantees that a cast vote cannot be linked to the voter and thus remains anonymous. The following sections describe these two core elements of the EVITA schema in more detail.

7.2.1 Encryption using a Hardware Security Module

The EVITA schema uses encryption to keep a cast vote secret. From the moment the voter makes her decision there is no more need to reveal it except for the reason of counting. There is no need to uncover the voter's decision, her vote respectively, at any other time. This means that the vote has to be decrypted during the counting process only. Figure 7.2 depicts the basis concept of this end-to-end encryption.

The aim is to achieve an end-to-end encryption of the cast vote between the voter and the counting device. At this point two questions arise. How to provide the voter with the encryption key and how to

[3] For e-voting schemes based on homomorphic encryption see section 3.3.1.

[4] For further details about the Austrian electronic identity management system see section 6.1.

ensure that only the counting device is able to decrypt the vote. An obvious answer to the first question is to use an asymmetric encryption algorithm and a public key infrastructure. The latter question is more difficult to address as both technical and organisational measurements have to be put in place.

One technical solution for protecting the confidentiality of the private decryption key is to build the counting device on the basis of a hardware security module. Due to this, the private key used for decrypting of cast votes is solely stored in the hardware security module in a very secure way. However, additional organisational and technical measures are required in order to address the process of key generation and distribution. The private key—or any copy of it—must not exist outside the hardware security module without any technical or non-technical security measure.

In order to export, backup and (re-)import the private key of the hardware security module—which is necessary in real election scenarios—an adequate and sophisticated key management must be put in place. It would be a desirable to require the hardware security module to provide a key export and import mechanism following a defined shared key schema (e.g. see survey on shared key schemes provided in [103]; as well as [104], [105]). If a shared key schema is provided, a dedicated organisational framework has to be defined that states how to distribute the key shares and to whom. The organisational framework as well as the legal framework of an election must state clearly how many shares are required at a minimum to import or reset the decryption key of the hardware security module. Furthermore, it must describe which organisations—or more generally which entities of the election process—are eligible to hold a key share. From an organisational and legal perspective, a shared key schema would be perfect for replicating the legal responsibilities of the participating political parties regarding the election.

The key aspects of the encryption schema are:

- **Key Distribution and Public Key Infrastructure**
  ...distribution of the encryption key by using a public key infrastructure
- **End-to-End Encryption**
  ...end-to-end encryption of the vote by the voter
- **Decryption in the Counting Device**
- **Backup and Distribution of the Decryption Key**
  ...proper schema for backup/distribution of the encryption key

The following sections elaborate on each of these key aspects.

7.2.1.1 Key Distribution and Public Key Infrastructure

The encryption algorithm used takes the asymmetric encryption approach. In order to provide the voter with the publicly available encryption key, a public key infrastructure should be used. It is not only a question of how to distribute the key material, but also a matter of establishing trust. The voter must be sure that the encryption key provided is really the key of the counting device. Otherwise an outside party could provide a bogus encryption key to a voter and thus could decrypt her decision. This voter would lose her vote since a wrongly encrypted vote could not be accepted and counted by the counting device.

However, due to the public key infrastructure used, the public encryption key is wrapped into a public key certificate which is finally electronically signed by some issuing authority. By verifying the electronic

signature on the public key certificate, the voter find out which organisation or entity issued the certificate and check whether the public key has been modified or altered. Furthermore, by verifying the identity of the issuer of the public key certificate, the voter is able to decide whether or not to trust the certificate issuer and its certificate.

Verification of the certificate issuer leads to the process of trust establishment which is more of an organisational process than a technical one. In other words, the voter has to decide whether she trusts the issuing authority or not. Therefore, it is desirable that the public key certificates are not issued by the Election Authority (EA) itself or by any other (governmental) authority which is involved into the election process. Public key infrastructure providers are organizations that exist outside of e-Government, and there are plenty of issuing organisations, called certificate service providers, on the marketplace. The task is to choose the appropriate certificate service provider which is trusted by the most of the voters.

To summarize the requirements for key distribution and the public key schema:

Requirements

R1 The public encryption key has to be publicly distributed. Public key certificates and a public key infrastructure are required.

R2 The issuer of the public key certificate that holds the encryption key must be trusted by voters.

R3 The Election Authority should publicly announce the correct certificate through various channels so that the voter can easily retrieve and verify the encryption certificate.

7.2.1.2 End-to-End Encryption

Demanding end-to-end encryption is of paramount importance in order to protect the voter's election secrecy. The citizen's vote must be encrypted for the counting device immediately after she made her decision. There is no reason to store or hold the plain and unencrypted vote. Therefore, the voter's local voting environment, which usually includes some form of voting client software, shall not store the voter's decision in any plain form. Neither a local copy of the plain vote nor any other electronic trace of the vote should remain on the voter's environment.

There is no need to decrypt the vote in any other phase of the election process except the counting phase. Therefore in the scope of this election process, end-to-end encryption means the encryption of the vote by the voter in a way that the encrypted vote can be decrypted only inside the secure counting device during the counting phase.

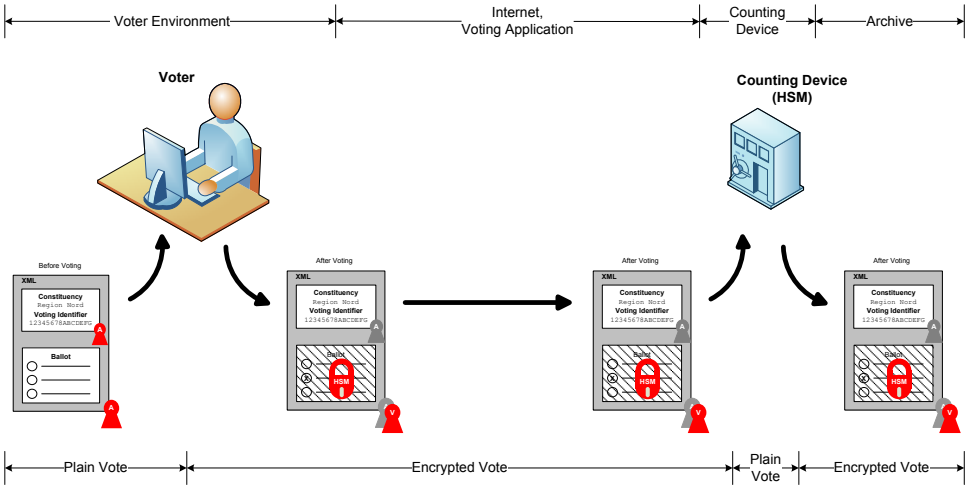

Figure 7.2: The principle of end-to-end encryption of the vote between the voter and the counting device.

To summarize the requirements for end-to-end encryption:

Requirements

R4 The vote must not be decrypted in any other phase of the election process except the counting phase.

R5 The vote must be encrypted immediately and stay encrypted until it reaches the counting device (counting phase).

7.2.1.3 Decryption in the Counting Device

The requirement that the encrypted vote should only be decrypted by the counting device comes from the requirements regarding end-to-end encryption. The encrypted vote must only be decrypted by the counting device. The EVITA approach is to decrypt the vote only at the very single moment of counting; a cast vote remains encrypted at any time before and after counting. This contrasts with other e-voting approaches where votes are decrypted before counting. However, when re-counts are considered, keeping votes encrypted is more advantageous.

The counting device holds the decryption key for decrypting the votes within the counting process. It must meet the requirements of a hardware security module in order ensure that the key cannot be exported or stolen. Furthermore, the counting device must ensure that votes are decrypted only for the purpose of counting. There must not be any chance to learn decrypted votes by accessing the counting device by any means. It is not sufficient to use a hardware security module only for the purpose of securely holding the keys. Additional critical components of the counting device—critical with respect to revealing encrypted votes unintentionally—are the counters used to compute the result. The counting device must not offer any possibility of finding out intermediate results or to observe the current status of the counting

process. However, logs for recording information might be put in place throughout the counting process by the counting device in order to collect additional information that confirm the correctness of the count, e.g. for an election audit. This information also must not be disclosed to anybody during counting as it can be used to reveal cast votes.

Therefore, the counting device has to be built in the style of a hardware security module. This includes not only the component holding the key for decrypting votes but also all other components involved in the counting process. The counting device should protect against technical as well as physical attacks.

To summarise the requirements for the counting device:

Requirements

R6 The decryption of cast votes must take place in the counting phase and in the counting device only.

R7 The decryption process is provided by a hardware security module that securely holds the decryption key.

R8 The counting device must protect against technical and physical attacks.

R9 The counting device must not disclose any information useful for revealing votes.

7.2.1.4 Backup and Distribution of the Decryption Key

It is necessary to export and import the decryption key in order to initiate and start the counting device or to set-up a backup counting device. The export of the decryption key is one of the most critical aspects since an exported and reconstructed decryption key can be used to decrypt all cast votes.

Although holding the decryption key externally is very critical, exporting the key is necessary in real large-scale elections in order to set up a backup counting device. There are several schemes that exist that can export and import key material securely from and to a hardware security module. The chosen mechanism has to ensure that the key cannot be used in any situation but for the counting event. This requirement cannot be met by technical measures only. There is a need for additional organisational requirements.

State of the art hardware security modules export key material using secure smart cards or similar components which can be considered as hardware security modules as well. This makes it a requirement that the components used to hold the key material externally are hardware security modules as well. Additionally, there is a need for further organisational measures and requirements because storing the key material in hardware security modules does not prevent abuse by the person or authority that holds the key. A possible solution to counter this is the introduction of shared key scheme.

A shared key scheme requires splitting up the key material (the encryption key) in n different shares. In order to reconstruct the whole key at least m shares are required where $m \leq n$. The shared key mechanism is also useful for modelling the organisational structure and legal responsibilities of the Election Authority. Usually, the Election Authority is recruited from different organisations with different interests in order to provide mutual supervision. By providing each member of the Election Authority with one share of the key, it can be ensured that neither one member alone nor a group of members are able to

reconstruct the decryption key. The shared key schema applied must prevent one holder of a key share from being able block the counting process. Therefore, it is advisable to choose $m < n$ or to introduce further organisational measures in order to prevent this threat. This discussion on the shared key schema demonstrates perfectly that a symbiosis between technical and organisational measurements is vital for a voting schema.

To summarize the requirements for the backup and distribution of the decryption key:

Requirements

R10 The counting device (hardware security module) must be able to securely export and import the private decryption key.

R11 The decryption key must not be exported from the hardware security module. Instead, an adequate key export schema must be used.

R12 The key export schema used should be a shared key schema (the hardware security module of the counting device should allow to export only shares of the key but not the whole key).

R13 Each key share must be stored on a secure device, such as a smart card, meeting the requirements of an hardware security module.

R14 The key shares are held by members of the Election Authority.

R15 To (re-)import the key into the hardware security module of the counting device, at least m shares out of n are required, where $m \leq n$.

7.2.2 Domain Separation and Identification Model

Electronic voting is a very special e-Government application with regards to identification issues. On the one hand, the process requires unique identification of the voter in the course of the registration procedure in order to record who has cast her vote. On the other hand, the cast vote must not be linkable to the voter. Although these requirements seem to be contradictory, the EVITA voting schema meets both requirements by introducing a sophisticated identification concept and domain separation schema (domain separation with respect to identity domains).

The concept of domain separation is based on the need-to-know principle since neither of the involved organisations need to know the voter's unique identifier. Usually it is sufficient to identify the voter within a dedicated context. This principle is also the underlying idea of the whole identity management of Austrian e-Government and the Citizen Card concept (see chapter 6.1 for a description of the electronic identity management system). The Austrian identity management concept introduces a unique identifier for each citizen, called Source Personal Identification Number ($sPIN$), as well as identifiers for sectors, called Sector Specific Personal Identification Numbers ($ssPIN$), in order to uniquely identify a citizen within a given sector of applications. Due to the use of sector-specific identifiers, it is not possible to identify a citizen in a different application sector, e.g. sector A, using her sector-specific identifier for another sector, e.g. sector B, and vice versa. Since it is the aim to develop a EVITA voting schema that is fully compliant

with Austrian e-Government elements and specifications, the EVITA voting schema adopts and extends the concept of sector-specific identifiers.

For this specific e-voting schema, the use of the existing Austrian identity management system is not sufficient. As stated in section 6.1, the Source PIN Register Authority is allowed to gain a citizen's $ssPIN$ for a dedicated, foreign sector without involving the citizen or her Citizen Card under certain legal circumstances. This means that it is technically possible to gain access to the $sPIN$ or any $ssPIN$ of a citizen without the knowledge of the citizen. However, from a legal and technical point of view, this is a very complex task since several organisations and authorities are involved in it and a clear legal mandate must exist. Nevertheless, it is possible and this is a problem since a "bad government" and/or a "bad public administration" might have an interest monitoring a citizen's behavior in past elections (maybe not now but in the future). This worst case scenario makes it it obvious that legal and organisational security mechanisms may fail. Therefore, it must be technically impossible to link a cast vote to a voter and vice versa, even if the vote and the voter's decision is encrypted following the requirements of section 7.2.1 as encryption may lose its effectiveness over the years.

As a consequence, simple sector-specific identifiers as used in other governmental applications are not adequate for marking votes or for identifying voters during the whole election. In order to find a satisfactory solution to this problem it is necessary to clarify the requirements regarding identification and to locate where and in which context identification is needed.

The EVITA voting schema follows a two phase approach, which differs between registration phase and election phase. Therefore, the identification schema needs to be discussed and developed in two levels. On the first level, the identification schema must handle registration issues. On the second level, the identification schema must offer the possibility to determine whether or not a voter has cast her vote already.

To clarify the requirements for the identification schema, here is a list of scenarios and phases where identification is necessary:

1. During the registration phase: The voter requests to vote electronically using her Citizen Card.
2. During the election phase: In the event the voter is unable to vote electronically—due to technical problems within the voter's technical environment etc.—the voter should have the possibility to visit a polling station in order to vote conventionally. At the polling station, the election officials must (electronically) identify the voter in order to determine whether she has already cast her vote via e-voting or not. It is important to consider that the voter might not be identifiable using her Citizen Card (e.g. in the event of a lost Citizen Card or alike) and thus there must exist some alternative method of finding out the voter's electronic identity and/or identifier.
3. During the election phase: In the course of casting a vote electronically, the voting system has to determine whether the voter has already cast a vote or not, and thus the election system has to identify the voter. The system has to mark the voter in some way in order to prevent double votes.

These three scenarios describe different requirements and identify problem areas. Although the second and the third scenarios appear to contradict the election secrecy at first glance, the proposed domain separation model is able to solve the problem.

The following sections propose and define an identification schema that is split into two different domains; the Registration Domain and the Election Domain. The whole identification schema is built on the estab-

lished identity management concept of Austrian e-Government and makes use of two different identifiers which are loosely bound to each other using cryptographic technologies.

7.2.2.1 Two Identification Domains: Registration Domain and Election Domain

From an organisational point of view, there are two different domains. The registration system has to identify the voter in existing registers and databases, such as the register of voters, the Central Resident Register, etc. The representation of a voter's identity must match existing records of registers and authorities, therefore, the first form of identity is taken directly from the conventional identity management system of the Austrian e-Government, i.e. a conventional sector-specific personal identification number ($ssPIN$). Since these registers are used for conventional elections as well, they usually contain additional information about the voter, such as her given name, name, date of birth, etc.

The cast vote must contain some identification information in order to determine the person who cast it. Votes must contain at least some representation of the voter's identity in order to determine whether a voter has already cast her vote and thus prevent double votes. The latter question is important when conducting a conventional election in parallel and allowing e-voters to cast their votes by conventional means as well (in the event of technical problems, etc.).

Two different domains and two different representations of a voter's identity appear necessary:

1. The first domain is denoted as Registration Domain and it deals with identifiers taken from the conventional Austrian e-Government (such as $ssPIN$).
2. The second domain is denoted as Election Domain and it deals with identifiers distinct from those of the Registration Domain.

Figure 7.3 depicts both domains and their respective authorities. This figure has three authorities whereas the Registration Authority (RA) and the Asserting Authority (AA) are located within the Registration Domain and the Election Authority is located within the Election Domain. It also shows what kind of personal information about a voter, i.e. signing certificate, name, $sPIN$, etc., may be accessed by the different authorities.

A bidirectional link must not be allowed to exist between the identity representations of both domains. Nevertheless, it must be possible to prove whether or not a given voter has already cast a vote by checking the voter's identity representation in the Registration Domain. This requirement may appear to be questionable at first, but when taking a closer look at the use case behind it, the reasons for it become clear.

There is only one use case in which the question "Has a given voter X cast her vote already?" is allowed. This question might only arise in the event that an e-voter is not able to cast her vote electronically for some reason and thus shows up at a conventional polling station to cast her vote. In this special case, it is legitimate to search for the existence of the voter's vote. It must be noted that this is a strict uni-directional query from a given identity to the appropriate cast vote. The query in the other direction must never be possible. In terms of identity representations, it means that a corresponding identity representation in the Election Domain should be derivable from a given identity representation in the Registration Domain but not vice versa.

The requirement is to define two identity domains and two respective identity representations in which a corresponding identity representation in the Election Domain can be derived from a given identity

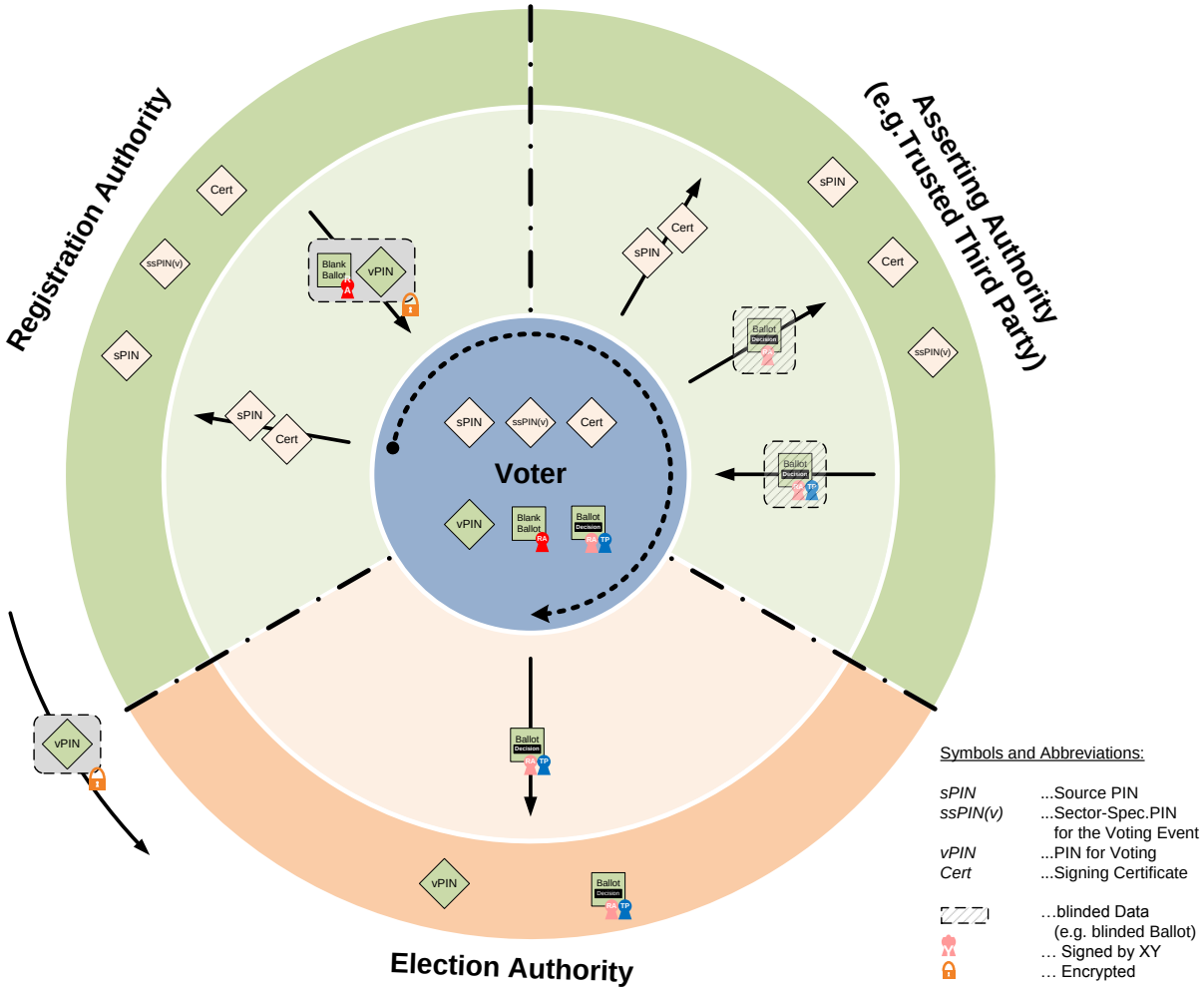

Figure 7.3: Two identification domains: Election Domain and Registration Domain.

representation in the Registration Domain. This requirement leads to having a link between identity representations from the Registration Domain and the corresponding personal identifiers of the Election Domain. Creating this link using simple derivation mechanisms—since they are used for deriving a $ssPIN$ from a given $sPIN$—is not satisfactory since the identity representations of the Registration Domain are conventional e-governmental identifiers and are based more or less on conventional identification information (such as name, date of birth, etc.). Without additional measures it would be too easy to find out a citizen's identity representation in the Registration Domain, and with this information find the corresponding identity representation in the Election Domain.

Considering the use case drafted above once again leads to the conclusion that this use case is not standard procedure and would only happen occasionally. Moreover, there is no need to search for a voter's cast vote after polling stations have been closed[5]. This means that the uni-directional link between identity representations of the Registration Domain and the Election Domain is required over a very short period only.

[5]This statement specifically relates to Austrian electoral law. For the sake of completeness, legislation in some other countries requires that a cast vote be able to be used to reveal the voter's identity, e.g. in United Kingdom in response to a court order.

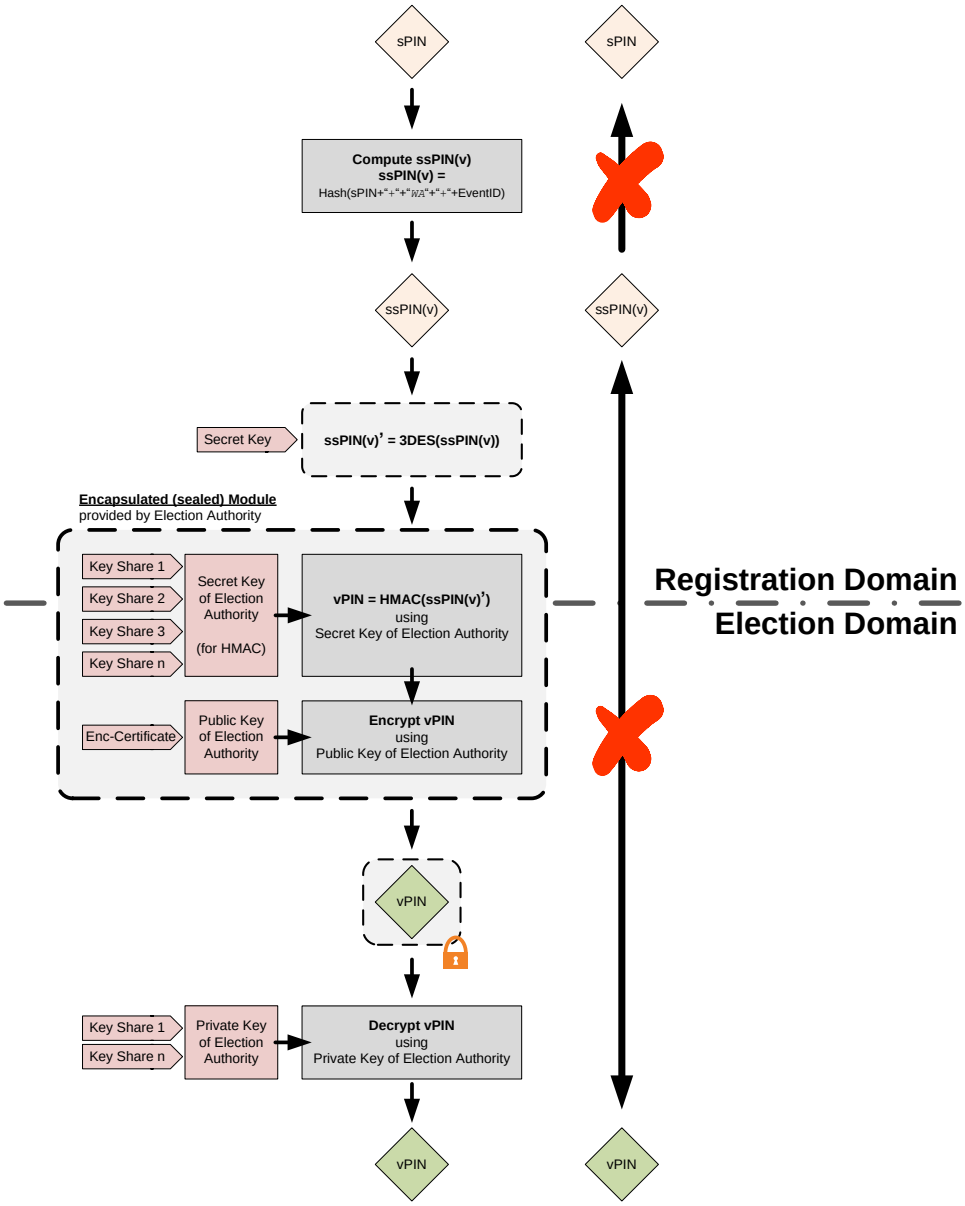

Figure 7.4: Cryptographic link between Registration Domain and Election Domain.

The EVITA voting schema suggests creating the link between the personal identifiers in the Registration Domain and the corresponding identifiers in the Election Domain as depicted in figure 7.4. This sketch outlines both domains and the different forms of identifiers. The Registration Domain deals with conventional electronic identifiers; i.e. the Source PIN ($sPIN$) and a sector-specific identifier which is specific to the election event ($ssPIN(v)$). In the course of crossing domains, the EVITA schema requires that a special personal identification number be derived that is only to be used within the Election Domain—referred to as a Voting Personal Identification Number (vPIN)—from a given $ssPIN(v)$. By applying a mathematical one-way function (HASH function), the link between the $ssPIN(v)$ and the derived $vPIN$ is uni-directional, pointing from the Registration Domain to the Election Domain. Furthermore, in order

to have no permanent direct link between both identifiers, the derivation procedure applies secret keys.

Since the link between both domains is only necessary during the election event, the secret keys that are used to create a $vPIN$ from a given $ssPIN(v)$ are needed during the term of the election event only and have to be destroyed immediately after the election event. This can be ensured on a technical level by using hardware security modules for generating and holding the keys. If the hardware security modules do not provide functionality for exporting the keys, there would not exist any copy of these secret keys outside the hardware security module, thus there would be no way to create a $vPIN$ from a given $ssPIN(v)$ without using the hardware security module. This means that the link between $ssPIN(v)$ and $vPIN$ can be permanently broken by securely erasing the secret keys or by destroying the corresponding hardware security modules.

The transformation of a given $ssPIN(v)$ to a $vPIN$ represents the "border" between both domains from an abstract point of view. From the technical point of view, the transformation process can take place in either of the two domains. In order to prevent one domain from learning the identifiers in the other domain, the technical implementation of this transformation process must ensure that the foreign identifier created for the corresponding domain is encrypted immediately. The schema depicted in 7.4 shows the $vPIN$ created for the Election Domain being encrypted immediately. This makes sure that the Registration Domain cannot learn any identifier from the Election Domain even though the transformation process may be situated within the Registration Domain itself.

In order to prevent any kind of abuse, it is important to log whenever the system is used to transform a $ssPIN(v)$ to a $vPIN$. The use of hardware security modules means that there is only one single point to control, so it is easy to apply both technical and organisational mechanisms to prevent abuse. For example, by requiring audit logs and stringent access restrictions, the link between the domains is controllable. Nevertheless, the introduction of two different identification domains as well as a link between both domains is a crucial aspect of the EVITA schema. The following sections describe both identity domains and their personal identifiers in more detail.

Requirements

R16 Two identification domains—Registration Domain and Election Domain—with two different personal identifiers—$ssPIN(v)$ and $vPIN$—must be introduced. In order to identify a voter's cast vote, only the $vPIN$ is allowed to be used.

R17 A uni-directional mapping must exist that points from an identity in the Registration Domain ($ssPIN(v)$) to the corresponding identity in the Election Domain ($vPIN$).

R18 The mechanism to transform a given $ssPIN(v)$ to a corresponding $vPIN$ must only be possible during the election event.

R19 The mechanism to transform a $ssPIN(v)$ to a corresponding $vPIN$ has to be audited and controlled. Adequate organisational and technical measures are required.

R20 Besides the $vPIN$ and $ssPIN(v)$, no other representations of a voter's identity should be used.

7.2.2.2 Registration Domain – Creation and Use of $ssPIN(v)$

The voter registers for electronic voting using a process provided in the Registration Domain. Since the application for electronic voting requires discrete identity data as well, such as the voter's name, date of birth and in particular her address, a conventional electronic identification schema is used. The main activities of the registration process are (section 8.3 describes the registration process in detail):

1. to identify the voter
2. to determine the voter's permanent address according to the Central Residents Register (due to determination of the election district)
3. to contact the election register in order to mark the voter as an electronic voter (e-voter).

The registration service usually identifies the voter using her Citizen Card. This means that the registration process has access to the $sPIN$, and can also find out the application-specific sectoral identifier $ssPIN(v)$. The $ssPIN(v)$ is the conventional sectoral identifier specific to an election. The registration application contacts registers—such as the Central Resident Register—using the $ssPIN(v)$. As the $ssPIN(v)$ conforms to the conventional identification schema, every register is able to resolve the identifier and provide the requested information. Furthermore, thanks to the Austrian identification schema, it is also possible to transform the given $ssPIN(v)$ into another sector-specific identifier $ssPIN(XY)$ if necessary, for example, in order to contact or make a request to another governmental application or service located within a foreign application sector.

All actions taken in the registration phase correspond to conventional governmental processes. Therefore, the personal identifier used within the Registration Domain is a conventional sector-specific personal identifier. The sectoral identifier is derived from the voter's unique $sPIN$ following the schema defined in the Austrian identification scheme. Expression 7.1 shows the whole derivation process in detail.

$$ssPIN(v) \quad = \quad \text{HASH}\,(sPIN \oplus \text{'ed'}) \tag{7.1}$$

$sPIN$ ... the voter's Source Personal Identification Number taken from her Citizen Card
'ed' ... short-name of the sector, e.g. **e**lection and **d**emocracy (ed)

7.2.2.3 Election Domain – Creation and Use of $vPIN$

In contrast to the Registration Domain, the Election Domain does not require any discrete identity information about the voter. It is not even necessary to identify the voter in person within the Election Domain since the processes of the Election Domain do not deal with identification but rather with authorisation. The election process is not interested in the unique identity of the voter. The only thing the voter has to prove is that she is eligible to vote.

There needs to be a way to track which voter has already cast a vote. This is necessary when running a conventional election process in parallel and considering the conventional election process as a fallback scenario for the electronic election. This implies that the officials at the polling station must be able to prove whether or not the voter has already cast a vote. It must be kept in mind that the voter at the polling station might only be carrying a conventional identity card, e.g. a passport, which leads to the

requirement of having a link from a voter's conventional identity information through a sectoral identifier ($ssPIN(v)$) to her corresponding identifier of the Election Domain ($vPIN$).

This leads to two assertions. The first is that the polling station and all processes there are logically located in the Registration Domain since they deal with conventional identity information. Furthermore, these processes must not use any other personal identifier other than the $ssPIN(v)$. The second assertion is that a temporary uni-directional link must exist between $ssPIN(v)$ and $vPIN$ (see the conclusions given in section 7.2.2.1 introducing the both identification domains).

The creation of a $ssPIN(v)$ from a set of discrete identity information which is sufficient enough to identify the person uniquely is only possible with the help of the Source PIN Register Authority. Thus it is possible to determine a voter's $sPIN$ and to further create the $ssPIN(v)$ based on the information given on her conventional identity card. As a consequence, the algorithm for creating the $vPIN$ has to take the $ssPIN(v)$ as input. Moreover, this creation algorithm must always yield the same $vPIN$ for a given $ssPIN(v)$. Since the link between $ssPIN(v)$ and $vPIN$ is only needed temporarily, there must be a way to remove the link relation permanently, for example, immediately after the election event. The algorithm given in equation 7.2 achieves both requirements.

$$vPIN = \text{HMAC}\left(ssPIN(v)'\right)_{SK_{EA}} \tag{7.2}$$

$$= \text{HMAC}\left(\text{3DES}\left(ssPIN\left(v\right)\right)_{SK_{RA}}\right)_{SK_{EA}} \tag{7.3}$$

$$= \text{HMAC}\left(\text{3DES}\left(\text{HASH}\left(sPIN \oplus \text{'ed'}\right)\right)_{SK_{RA}}\right)_{SK_{EA}} \tag{7.4}$$

$sPIN$	... the voter's source personal identification number taken from her Citizen Card
$ssPIN(v)$	... the voter's sector-specific personal identification number for the election event
'ed'	... short-name of the sector, e.g. **e**lection and **d**emocracy (ed)
SK_{EA}	... a secret key of the Election Authority (EA)
SK_{RA}	... a secret key of the Registration Authority (RA)

The algorithm for creating $vPIN$s is a logical continuation of the $ssPIN(v)$ algorithm. Here again the algorithm makes use of a one-way function (HASH function) in order to ensure uni-directionality. Contrary to the creation of the $ssPIN(v)$, the algorithm for creating $vPIN$s requires a secret security measure for both the Registration Domain and the Election Domain. This measure may be implemented in several ways, for instance by adding secret phrases or by applying cryptographic algorithms such as encryption algorithms or keyed HASH functions.

The proposed algorithm for creating a $vPIN$ takes the previously created $ssPIN(v)$ as input. First, the algorithm adds the secret of the Registration Domain to the $ssPIN(v)$ by applying a symmetric encryption algorithm (e.g. 3DES). Here the encryption algorithm makes use of a secret key which is under the sole control of the Registration Authority. The resulting encrypted $ssPIN(v)$ is further derived by applying a keyed HASH function as a one-way function. This keyed HASH function, called a HMAC, not only creates the HASH value for the given input but also encrypts it by applying a secret key provided by the Election Authority.

As a result, the link between a $vPIN$ and the underlying $ssPIN(v)$ cannot be created without knowing both secret keys. Thus both secret keys are important elements of the $vPIN$-creation algorithm, which leads to a temporary link between the personal identifiers of both domains. The application of the Registration Authority's secret key is necessary since a bogus Source PIN Register Authority, which

is able to create a $sPIN$ and the corresponding $ssPIN(v)$ for any person, would otherwise be able to create $vPIN$s if the Election Authority cooperates with it. Vice versa, the application of the Election Authority's secret key is required in order to prevent the Registration Authority, in cooperation with the Source PIN Register Authority, from being able to calculate $vPIN$s. Therefore, both keys are required for creating a $vPIN$, and destroying one of these two keys breaks the link between $ssPIN(v)$s and $vPIN$s permanently.

However, just involving secret keys in the derivation process as a technical measure is not sufficient. Additional organisational measures are required. The management of the secret keys is of crucial importance since possession of both secret keys enables the owner to create $vPIN$s. Therefore, each secret key has to be provided and handled within the respective domain by the according authority and has to be handled appropriately. The use of a hardware security module is not only strongly recommended, but rather should be treated as a requirement for creating and holding the keys securely. In this respect, the requirements regarding the management of these secret keys are similar to the requirements of the hardware security module as stated in section 7.2.1.4 discussing strategies for backup and distribution of the decryption key.

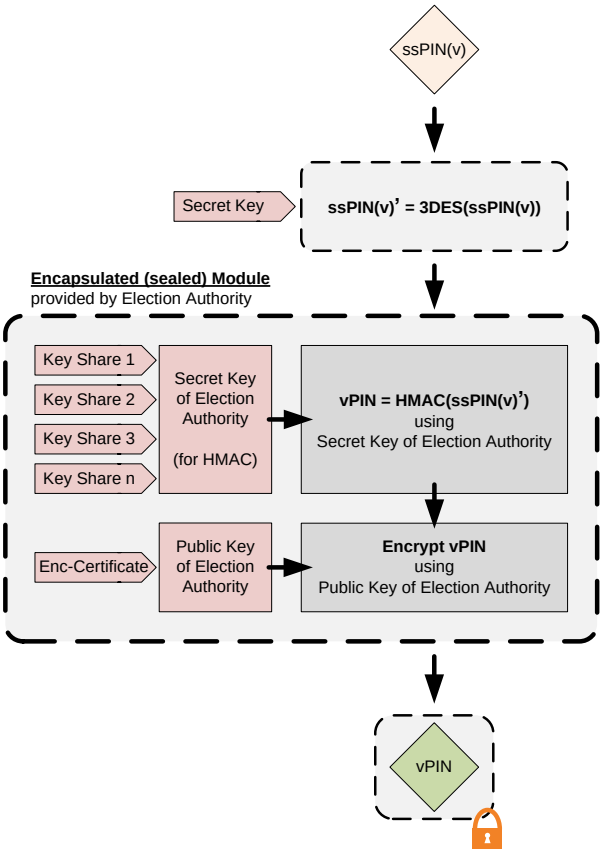

Figure 7.5: Proposed process of transforming a given $ssPIN(v)$ into the according $vPIN$.

Figure 7.5 shows the proposed approach for handling both secret keys. This proposal suggests using a shared key schema for the handling of the Election Authority's secret key. The key shares should be held by the members and representatives of the election commission and thus the handling of them should

be very similar to the handling of the encryption key as stated in section 7.2.1.4. In order to permanently break the link between the identifiers of both domains, it is sufficient to destroy at least one of both secret keys. However, there should be an organisational requirement that secret keys of both domains have to be erased or destroyed. From a practical perspective this can be achieved either by destroying or resetting the hardware security modules holding the secret keys or by destroying all the existing key shares.

Figure 7.5 highlights a second but also very important issue in the $vPIN$ creation process. Since a $vPIN$ is created by using a specific $ssPIN(v)$ as input, the creation process should be located within the Registration Domain. The process has to ensure that the $vPIN$ that is created cannot be accessed by any entity in the Registration Domain. Therefore, the schema requires encryption of the $vPIN$ for the Election Authority (Election Domain) immediately after it has been created. A stringent key management is vital here as well. Thus the public key of the Election Domain used for encryption must be provided by the Election Domain and must not be interchangeable.

Any technical implementation of the $vPIN$-creation process must follow the requirements stated above. In addition to all technical measures there is a strong need for organisational measures. Thus it is recommended that the Election Authority provide the technical implementation for dealing with its secret keys for the $vPIN$ creation process by means of a sealed module that contains a hardware security module holding all keys of the Election Authority (figure 7.5 highlights this component as "Encapsulated (sealed) Module"). Section 8.3.5 gives a detailed description of the $vPIN$-creation process from a technical point of view.

7.2.3 Additional Elements of the EVITA concept

7.2.3.1 Ballot, Ballot Envelope, Ballot Card and Vote

The core data structure of the EVITA voting concept is the ballot, which consists of several elements. The ballot is a container which stores all required data elements for a voter during the election event. Thus, the content of a ballot is added to during different phases and grows incrementally. Figure 7.6 depicts all phases and elements of a ballot at a glance.

This section focuses on the semantic structure and content of the ballot. With respect to the syntactical structure of the ballot, the EVITA voting system strongly recommends the use of an XML structure since XML is not only one of the major basis technologies used in Austrian e-Government but also because a standardised XML language for election purposes already exists, i.e. EML.

OASIS has a technical committee that is responsible for developing EML being a standardised language for *"[..] the structured interchange of data among hardware, software, and service providers who engage in any aspect of providing election or voter services to public or private organizations"*[6].

It is highly recommended to incorporate international standards and definitions whenever possible. It is especially important to use standardised interfaces—and EML is considered a standardised interface—because it makes it easier for external election observers to verify the data flow between the modules of an e-voting system. Furthermore, using a standardised interface offers the opportunity to draw on existing products and systems if available. Section 9 makes several proposals for a technical implementation of

[6]Taken from the Statement of Purpose of the OASIS Election and Voter Services Technical Committee; as seen at http://www.oasis-open.org/committees/election/charter.php on 13th May, 2007.

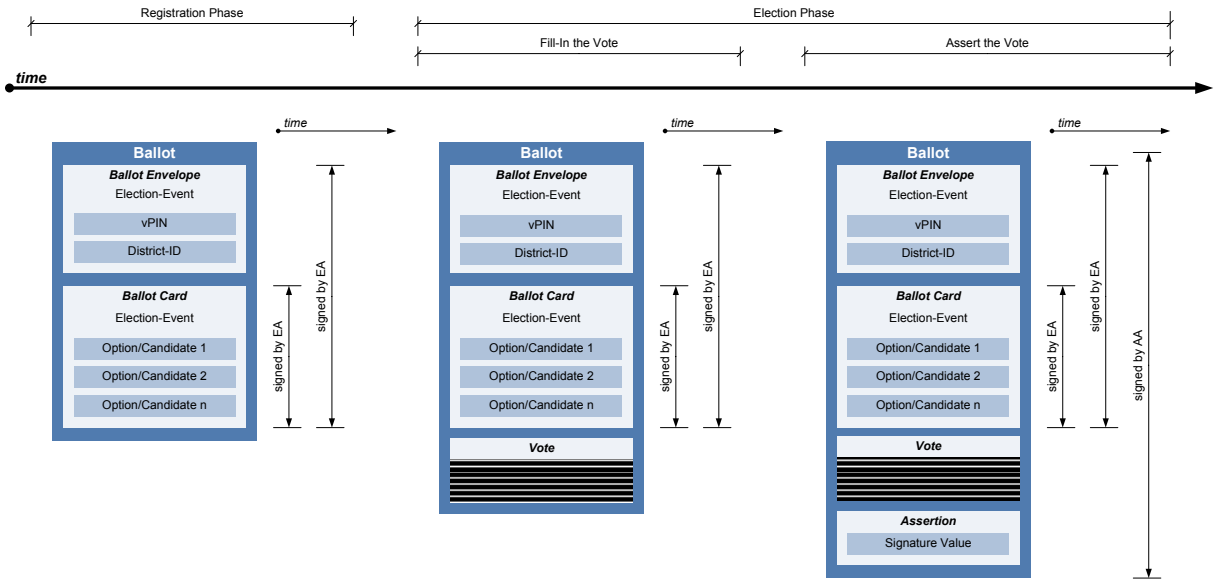

Figure 7.6: Left: initial ballot. Middle: ballot after the encrypted vote has been added. Right: complete ballot containing the encrypted vote as well as the assertion.

the EVITA voting concept and thus will suggest an XML syntax for ballots based on EML.

Ballot after the Registration Phase

As a result of the registration process, the voter receives her initial ballot, which consists of two parts:

1. Ballot Envelope
2. Ballot Card

The ballot envelope holds all meta-data about the election event and the voter. The ballot envelope holds at least

1. $vPIN$
   .. the voter's personal voting identifier for the Election Domain.
2. District-ID
   .. the unique identifier of the election district the voter belongs to.

The second element of the initial ballot is the voter's ballot card. It holds the voting options for the present election event. The ballot card is created according to the voter's election district since voting options may vary from one election district to the next. The voter's vote will be created based on the option list provided within this ballot card.

This first version of the voter's ballot carries two signatures. As depicted in 7.6, the left-most ballot (the whole ballot card) is signed by the EA. As the detailed description of the registration process will point

out, the ballot card might be signed in advance so that all ballot cards for a certain election district carry the same electronic signature.

The second signature confirms that the ballot card and ballot envelope belong together. This second signature along with the meta-data provided within the ballot envelope and the ballot card proves the authenticity of the ballot card.

Ballot after the "Fill-In Vote" Process

After the voter has made her decision and has prepared her encrypted vote, the encrypted vote has to be added to the ballot. Since the encrypted vote is an XML fragment as well, it can be easily added to the ballot provided by the registration process.

After the "Fill-In Vote" process, the ballot consists of the following parts:

1. Ballot Envelope
2. Ballot Card
3. Encrypted Vote

The ballot envelope and the ballot card remain in the ballot since they were issued from the Registration Authority. Even both signatures remain on the ballot. Only the encrypted vote is added to the existing ballot in the form of an extra XML element. This status of the ballot is depicted in figure 7.6 (middle ballot).

Ballot after the "Assert-Vote" Process

This is the very last status of a ballot. After the voter has added her encrypted vote, she might ask a trusted third party to confirm her ballot. In response, the trusted third party, i.e. the Asserting Authority, adds an assertion to the voter's ballot (see also process description given in section 8.4.2) and section 7.2.3.2. Thus, after the "Assert-Vote" process, the voter's ballot consists of the following parts:

1. Ballot Envelope
2. Ballot Card
3. Encrypted Vote
4. Assertion

The ballot envelope, ballot card, encrypted vote, and the electronic signatures all remain in the ballot. Only the assertion is added to the ballot in the form of an additional XML element.

The Asserting Authority signs the whole ballot and its elements including the two electronic signatures in order to be able to detect any later modification, thus a third electronic signature is added to the ballot. The assertion added to the vote contains the additional signature created by the trusted third party (Asserting Authority).

The right-most ballot in figure 7.6 depicts the final form of a ballot. The ballot is then ready to be cast.

7.2.3.2 Indirect Voter Authentication

The EVITA voting schema does not necessarily require the voter to sign her ballot before casting. Instead, this voting schema introduces an additional Asserting Authority which blindly signs the ballot to prevent any manipulation of the ballot after being cast. Thanks to the proposed registration and asserting processes of the EVITA voting schema, even the voter herself can be indirectly repetitively authenticated by her cast ballot.

Indirect voter authentication is based on the combination of the registration and asserting process. During the registration process, the voter is identified and authenticated by providing her Identity-Link and an electronic signature. Based on this, the registration service creates her voting credentials which are immediately encrypted by applying the voter's public key that is provided in the voter's Identity-Link. In other words, the voting credentials are encrypted solely for the voter by applying her public key that is asserted as belonging to the voter by the Source PIN Register Authority. Thus it is ensured that the voting credentials that are returned—containing her blank ballot card and ballot envelope—are only able to be decrypted by the voter's Citizen Card. This implies that the person who is able to decrypt the voting credentials is the same person who registered and to whom the voting credentials have been issued.

The same argumentation is applicable to the asserting process. During the asserting process, the voter is identified and authenticated once again by providing her Identity-Link and an electronic signature. In addition, the voter provides her encrypted blinded ballot and asks the Asserting Authority to blindly sign it. As a result, the asserting service blindly signs the ballot and returns the resulting signature value encrypted with the voter's public key. Thus, the voter's blindly signed encrypted ballot is encrypted again for the voter who has been identified by the provided Identity-Link. In other words, it is ensured that the person who is able to decrypt the encrypted signature value is the voter who has been identified and authenticated by the provided Identity-Link. Finally, after the voter has decrypted the signature value, she has to unblind it according to the blind signature schema applied. The decrypted and unblinded signature value resulting from the asserting process is further denoted as "assertion".

In order to ensure that the voter who requests for her vote to be asserted is the same person who is registered for e-voting and to whom the presented ballot has been issued, the Registration Authority provides the encryption key used to encrypt the voter's voting credentials during registration process to the Asserting Authority. Since both the Registration Authority and the Asserting Authority are located in the Registration Domain, both are allowed to handle the voter's $ssPIN(v)$. Moreover, since the Registration Authority creates a list of e-voters based on the $ssPIN(v)$, the Registration Authority should put the voter's encryption key on this list as well. Thus, with the help of this list, the Asserting Authority is able to decide whether or not the voter requesting for asserting is an eligible e-voter. The Asserting Authority is then able to encrypt the resulting assertion with the voter's public key that she has presented during the preceding registration process. This ensures that no other person other than the one who has been registered for e-voting during the registration process is able to decrypt and use the returned assertion.

Finally, before the voter casts her ballot, she has to decrypt the assertion received from the asserting service and add it to her ballot. Thus, the Election Authority might draw the following conclusions based on a cast ballot:

1. The cast ballot has been decrypted by the person who has registered for e-voting and to whom the underlying blank ballot has been issued during the registration process. This can be concluded because the blank ballot received during the registration process has been encrypted for the regis-

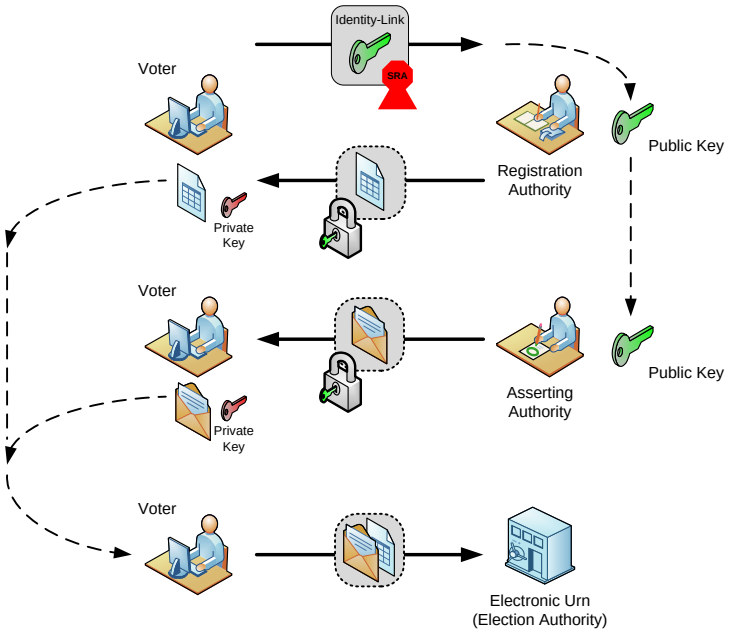

Figure 7.7: Simplified illustration of indirect voter authentication.

tered voter only.

2. The cast ballot has been asserted through the same voter who registered for e-voting and to whom the underlaying blank ballot has been issued during the registration process. This can be concluded because the assertion returned to the voter is encrypted for this voter only by drawing on the voter's public key stored by the Registration Authority during the registration process. Thus, the voter who has requested for e-voting and to whom the encrypted voting credentials have been issued during registration has compiled the cast ballot, and the cast ballot contains the decrypted assertion.

3. If the signature contained in the assertion of the encrypted cast ballot can be verified successfully, the cast ballot has been asserted by the identified voter.

Due to the conclusions 1), 2) and 3) and assuming that the voter has not lost her Citizen Card—and knows the secret codes needed to use it—or has not lent it to anyone else, the cast ballot can be assumed to be the ballot from the voter who has been registered for e-voting and to whom the blank ballot card has been issued. This means that the $vPIN$ provided in the cast ballot represents the voter who cast the ballot. Figure 7.7 depicts the principle of indirect voter authentication as used within the proposed e-voting schema.

Moreover, it is assumed that the voter does not aim at decrypting her ballot and giving it to any third party or to give her Citizen Card to any third party; the voter is assumed to have a strong interest in voting and in protecting her vote as well as her right to vote.

Chapter 8

EVITA Process Model

This chapter defines the processes of the EVITA e-voting concept in detail. The concept is based on the core principles described in the preceding chapter. The core principles are important but at the same time only serve as the basis for an e-voting system. However, the core principles specify the fundamental requirements for the processes. The processes have to complete the security concept by fulfilling these requirements.

The processes presented in this chapter were developed using a business process modelling methodology specifically targeted at the needs of the public sector and for designing Austrian e-Government processes. The methodology and the tools applied were developed in the course of the project ADOamt[1]. The ADOamt methodology includes the most important requirements for implementation of an e-Government solution from a business process management and integrated service modelling perspective. In addition to standard elements of business process modelling, this methodology includes e-Government elements at the process level. Furthermore, several IT security aspects can be modelled as well. The IT security and e-Government aspects of this methodology have been developed by the author of this thesis (see [106], [107] and [108]).

8.1 Actors, Roles and Authorities

A number of dedicated roles and authorities are present throughout an election event. In the registration and voting phases, three required parties can be identified:

- The Voter
- The Registration Authority
- The Election Authority

Additionally, for security considerations, a trusted third party, referred to as the Asserting Authority, might be useful. An Asserting Authority is not explicitly required by the election process itself, and is not yet foreseen by law. However, the EVITA voting concept introduces the Asserting Authority as a trusted third

[1] The meta modelling tool “ADOamt” following this methodology was developed by BOC; http://www.boc.com.

party from an academic point of view. Additionally, section 8.6 describes variations of the EVITA election schema in which the Asserting Authority is replaced by alternative actors and mechanisms.

This section gives a general description of the required actors.

8.1.1 The Voter

The voter is the person who wants to cast a vote using the electronic e-voting system. In addition to the legal requirements, which should not be further emphasized in the course of this thesis, the following technical and organisational requirements must be met by the voter:

- Technical Requirements:
  1. Citizen Card (Signature Creation Device, Citizen Card Environment)
  2. A storage area to hold the blank ballot (consisting of the ballot card and ballot envelope) after the registration phase. The storage area should be under the (sole) control of the voter (although the blank ballot should remain encrypted until the voting phase, a loss of the ballot would be very inconvenient or in the worst case would exclude the voter from e-voting).
  3. The voter must have a computer system with access to the Internet. The computer needs to be under her sole control and considered to be secure and free of any kind of malicious software[2].
  4. If required by the technical implementation of the EVITA voting system, the voter must run voting client software.

The logical unit of all hardware and software components used by the voter in order to vote electronically is denoted as the *voting environment*. In other words, the voting environment contains all required technical components the voter uses. All these components are under the sole control of the voter. From a bottom up view, the voting environment includes:

1. computer or similar device
2. a Citizen Card Environment (Citizen Card software, as described in section 6.2)
3. a Citizen Card (as described in section 6.2)
4. an e-voting client (software) to participate in electronic elections, if required
5. voting credentials and/or additional voting credentials, if required

Elements 1) to 3) are standard requirements for using Austrian e-Government applications. Elements 4) and 5) are additional e-voting elements, such as special client-software, voting credentials, etc., that may be required by an e-voting system. The EVITA e-voting concept requires an e-voting client which is special client software used to handle and manage different actions in connection with the voter's Citizen Card.

[2]Malicious software (malware) is an imminent problem which cannot be entirely defeated using of security and antivirus software. Instead, a trusted computing approach seems to be promising. However, it is the responsibility of the voter to keep her computer device free of malware which can be achieved to a high extent with a level of caution and the use of antivirus software.

- Organisational/Legal Requirements:
  1. The person has to be registered with the electoral register (electoral roll) and must be eligible by law to vote.

In general, every person that fulfills the legal requirements for voting is denoted as a voter. Furthermore, all voters who are registered for e-voting are denoted as e-voters.

8.1.2 The Registration Authority

The Registration Authority (RA) is responsible for the whole registration phase. Its duties are:

- to identify a person
- to prove and confirm the right of a person to vote
- to register a person to vote by e-voting
- to delete a person from the list of conventional voters
- to provide the citizen with a blank ballot (consisting of ballot card and ballot envelope) and further data necessary to vote electronically (the voting credentials)

All persons that fulfill the legal requirements to vote are registered for conventional elections. Voting using the electronic channel is an option for which the person has to apply explicitly. This means that at first the Registration Authority has a complete list of all persons approved to vote. As a result of the registration phase, the Registration Authority holds a list of voters registered for electronic voting (the list of e-voters). To prevent double voting, all voters registered for e-voting become marked in the list of conventional voters so that they can not vote conventionally without additional measure.

Since the EVITA e-voting concept takes place alongside conventional elections, the registration phase affects the conventional election process as well. Thus, the list of e-voters produced by the Registration Authority not only affects the e-voting system but also the conventional election (to be distributed to all polling stations).

8.1.3 The Election Authority

The Election Authority (EA) is generally responsible for the overall election. Its specific duties are:

- the administration of the list of voters
- the administration of the list of candidates
- to publish official election information such us:
  - list of voters
  - list of candidates
  - list of polling stations

- to count cast votes
- the announcement of the election results
- the organisation of the election in general

The head of the Election Authority is usually the leading officer for the present election.

8.1.4 Asserting Authority (Trusted Third Party)

The core process of the EVITA e-voting schema recommends having an additional “authority”. In terms of this thesis, an abstract trusted third party, the aforementioned Asserting Authority, is included. As an independently driven organisation, the Asserting Authority is used to ensure anonymity and to establish a certain trust relationship.

A more detailed description of this authority will be provided in the process description, in section 8.4.2, where it is required.

8.2 The Process Landscape

Although the EVITA process model adheres to the conventional election process given by law, the EVITA processes are distinctive in many respects. This section aims to elaborate on the EVITA process model in detail and goes into the detailed processes of the EVITA voting schema.

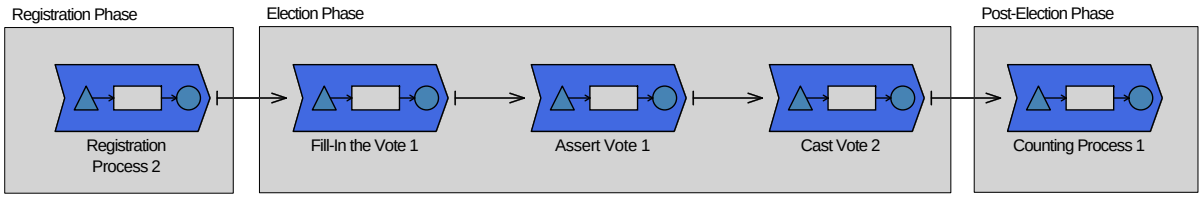

Figure 8.1: The EVITA process landscape.

The EVITA schema is a two-phase e-voting schema (two phases from the point of view of the voter according to the definition given in section 3.1). In addition to the registration phase and the election phase, the EVITA schema introduces a post-election phase in which counting or re-counting takes place. Thus, the overall EVITA process landscape consists of three phases as depicted in figure 8.1:

- Registration phase, consisting of one process:
  - Registration Process
- Election phase, consisting of three processes:
  - Fill-in the vote
  - Assert the vote

  - Cast the vote

- Post-election phase, consisting of one process:

  - Counting process

The schematic shown in 8.1 shows the logical order of the phases and processes but does not reflect the time relation between them. There is a time shift between the registration phase, the election phase and the post-election phase. Furthermore, there might be a need for a re-count which has to be considered as an additional process of the post-election phase, which occurs at an unspecified time after the first counting process. However, the EVITA concept treats counting and re-counting as equal, so there is no need for a dedicated re-counting process.

8.3 Registration Phase

In the EVITA-voting concept, the registration phase is carried out in a single process. During this phase, the voter has to be uniquely identified and has to apply for electronic voting explicitly. Figure 8.2 depicts the process in a process diagram that follows the methodology described in the introductory section of this chapter.

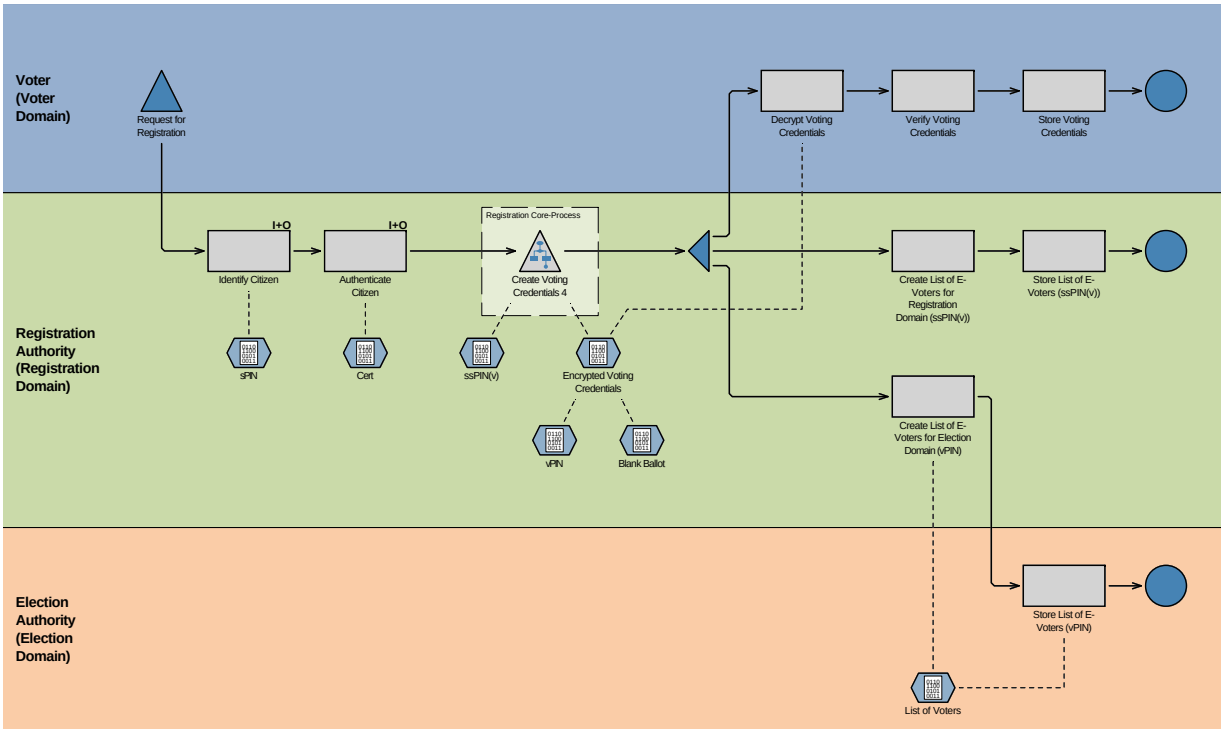

Figure 8.2: Registration Process (a high resolution figure can be found in appendix B.1).

8.3.1 Actors and Participating Authorities and their Domains

Within the registration procedure three actors are required:

- Voter (voter domain)
- Registration Authority (Registration Domain)
- Election authority (Election Domain)

The Voter

The voter is a citizen that fulfills all legal requirements to vote and is eligible to participate in a particular election event. Since choosing to vote electronically is a decision made explicitly by the voter, she has to initiate the registration procedure. The voter receives all voting credentials required for e-voting, such as a ballot envelope, ballot card, etc., during the registration process.

The Registration Authority

The Registration Authority is the authority that runs the registration service. This authority is responsible for identifying the voter, issuing voting credentials for the voter, and creating the list of e-voters. The Registration Authority provides a registration service for voters to apply for electronic voting.

The Registration Authority is logically situated in the Registration Domain (as described in section 7.2.2.2).

The Election Authority

During the registration phase, the Election Authority has a passive role only. It receives the final list of e-voters from the Registration Authority at the end of the registration process.

However, the Election Authority has to provide the core component of the registration service to the Registration Authority prior to the registration process. The core component is used to create blank ballots and to generate the voters' identifiers for the Election Domain (the $vPIN$). This component provides a series of activities and thus is described as a separate sub-process in section 8.3.5 in detail.

8.3.2 Context and Prerequisites

Since e-voting should take place parallel to a conventional election, a certain time interval needs to be kept between the completion of the registration phase and the start the election phase. This is to allow time for distributing the final list of voters to every polling station prior to election day. So it is not necessary to equip every polling station with online access to the electronic voter register to prove whether a person has cast a vote electronically already (to prevent double voting).

On the other hand, if permanent online access at every polling station is desirable, election officials could access the electronic voter register during the election and the time interval between the registration phase and the election phase would not be necessary. It would also make it possible to conduct the

registration and election phases in parallel, although, combining the registration phase with the election phase is only an option for small elections, e.g. election of the board members for a registered association.

Since the targeted scenario of the EVITA voting concept is a political election on a larger scale, the conventional election process needs to be kept. In such a scenario it is not feasible to provide every polling station with online access to the electronic voter register. Therefore, the registration phase is assumed to occur prior to the election phase.

Prerequisites for the Voter

In addition to the general requirements given in section 8.1.1, the voter has to meet the following prerequisites:

1. The voter must be eligible by law to vote.

Prerequisites for the Registration Authority

In addition to the general requirements given in section 8.1.2, the Registration Authority has to meet the following prerequisites:

1. The Registration Authority must be equipped with a list of citizens that are legally allowed to participate in the election event.
2. The Registration Authority must have generated the secret key used for $vPIN$-generation.
3. The Registration Authority must be equipped with the secret key of the Election Authority used to generate the voter identifiers for the Election Domain ($vPIN$).
4. The Registration Authority must be equipped with the public key of the Election Authority used to encrypt the $vPIN$s for the Election Authority.
5. The Registration Authority must provide a registration service to citizens.

Prerequisites for the Election Authority

In addition to the general requirements given in section 8.1.3, the Election Authority has to meet the following prerequisites:

1. The Election Authority must have generated the secret key used for $vPIN$-generation. The Election Authority has to provide the secret key to the Registration Authority (preferable within a sealed security module).
2. The Election Authority must have generated the key-pair used for encrypting generated $vPIN$s. The Election Authority has to provide the public key to the Registration Authority (preferably in a sealed security module).
3. The Election Authority must have generated the key-pair used for encrypting the cast votes. The Election Authority has to provide the public key to the voters. The private key is securely held in the counting device (hardware security module).

8.3.3 Stepwise Process Description

The voter starts the registration process by applying for electronic voting. A priori each voter is assumed to vote conventionally.

P1-A1: Request for Registration

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	None.
Output/Results:	None.

The voter contacts the registration service provided by the Registration Authority. The voter initiates the registration process and asks the service to register her as an e-voter.

P1-A2: Identify Citizen

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The voter's Identity-Link.
Output/Results:	The registration service receives the Identity-Link of the citizen.
	The registration service gets the claimed identity of the requesting citizen.

Following the identity management system specified in the Austrian Citizen Card concept, the registration service identifies the citizen by reading the Identity-Link stored in the Citizen Card. The registration service asks for the Citizen Card of the citizen to retrieve her Identity-Link by sending an Infobox-Read-Request to the Security-Layer interface of the citizen's Citizen Card. In response, the Citizen Card sends the Identity-Link directly to the requesting registration service (as long as the registration service fulfills the technical security requirements specified in the Austrian Citizen Card concept, e.g. the registration service must use an adequately secure communication channel and must provide either a TLS server certificate containing a governmental object identifier (gv-OID) or the registration service must be located within the Austrian gv.at-domain).

After the registration service has received the citizen's Identity-Link, it tries to verify the electronic signature on the Identity-Link. If the service can successfully verify the electronic signature, the registration service holds the claimed identity of the requesting citizen, i.e. the citizen's $sPIN$.

P1-A3: Authenticate Citizen

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	Application form.
	Identity-Link.
Output/Results:	Registration Authority holds the filled-in registration signed by the citizen.
	Citizen is considered being strongly authenticated.

In order to ensure that the person applying for electronic voting is really the person she claims to be, a strong authentication mechanism is needed. The identification and authentication mechanisms provided by the Citizen Card are based on electronic signatures. Electronic signatures—as created by the Austrian Citizen Card—are an adequate authentication mechanism since they use two-factor authentication by requiring possession (possession of the underlying signature creation device) and knowledge (knowledge of the secret PIN-code used to activate the signature creation process).

In the course of providing an electronic signature, the signer is asked to sign the application form to apply for electronic voting. This means that the form which has to be signed in order to apply for electronic voting is used as the "challenge" to be signed for authentication. The authentication process of the Citizen Card is described in section 6.2 in detail. Due to using the signed application form to authenticate the citizen, there is no need to ask the citizen to provide a further signature.

The registration service presents the application form to the citizen. The citizen has to fill in and explicitly express her wish to vote electronically. After the voter has completed the form, the registration service asks her to sign it using her Citizen Card. To do so, the registration service sends a signature creation request through the security layer interface to the voter's Citizen Card. In response, the Citizen Card client presents a dialog to the voter displaying the document to be signed. The Citizen Card client asks the voter to enter her secret PIN-code to create the electronic signature. It then returns the signed document to the requesting registration service.

Now the registration service has all the information it needs in order to fully authenticate the voter. According to the authentication schema of the Citizen Card, the registration service has to verify whether the public key information contained in the voter's Identity-Link (provided in activity P1-A2) matches the electronic signature provided in the activity. If it matches, the citizen is authenticated in accordance with the authentication schema laid down by the Austrian Citizen Card concept.

P1-A4: Create Voting Credentials

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	Verified Identity-Link.
Output/Results:	Voting credentials (ballot envelope, ballot card) encrypted for the voter. $vPIN$ of the voter encrypted for the Election Authority.

The results of the whole registration process is that the voter receives her voting credentials, the Registration Authority holds a list of e-voters (i.e. citizens who have decided to vote electronically), and the Election Authority receives a list of encrypted voting identifiers ($vPIN$) representing the e-voters within the domain of the Election Authority.

The term "voting credentials" denotes all elements required by a voter in order to vote electronically. At this stage they are:

- the ballot envelope
- the ballot card

The activity of creating voting credentials is one of the most critical elements of the registration process because at this stage the Election Domain and Registration Domain must work together. Therefore, this activity consists of several steps which interact which each other in a rather complex way. Due to the complexity and importance of this activity, section 8.3.5 describes this activity as a separate sub-process.

P1-A5: Decrypt Voting Credentials

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The encrypted voting credentials of the voter.
Output/Results:	The voter holds her ballot and all other data and tokens needed to vote electronically.

The voter receives an encrypted container that holds her personal voting credentials, which consist of the ballot envelope and the ballot card. This container is encrypted using the citizen's public key of her Citizen Card (according to the Austrian Citizen Card concept, the second key-pair is used to encrypt/decrypt data).

Although it is strongly recommended to keep the voting credentials encrypted until the election phase, the voter is asked to decrypt her credentials temporarily during the registration phase in order to verify the correctness of her credentials.

P1-A6: Verify Voting Credentials

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The voter's decrypted voting credentials.
Output/Results:	Voter is aware that her voting credentials have been issued by the proper Election Authority.

The voter verifies the electronic signature of the Election Authority on her voting credentials. The signature verification can be done either by the Citizen Card Environment or by any other signature verification service trusted by the voter. For privacy reasons and security concerns, the preferred method of signature verification is using the voter's Citizen Card Environment.

P1-A7: Store Voting Credentials

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The voter's verified voting credentials.
Output/Results:	The voter stores her voting credentials securely for the latter election phase.

After having proved the authenticity of the voting credentials, the voter has to store her personal voting credentials for the election phase. The voter is advised to store her voting credentials in encrypted form only. Therefore, any temporarily decrypted voting credentials should be securely and completely erased. The encrypted container as returned by Registration Authority is the only copy that should be kept.

P1-A8: Create List of E-Voters for Registration Domain

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	Registration phase is over and all e-voters have been registered for e-voting.
Output/Results:	The Registration Authority holds a list of $ssPIN(v)$.

As an outcome of the registration phase, the Registration Authority holds a list of all e-voters. Since this list is used within the Registration Domain, it uses the voters' $ssPIN(v)$ as identifiers. This list represents the final electoral roll and could be distributed to polling stations.

P1-A9: Store List of E-Voters for Registration Domain

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	A list of encrypted $ssPIN(v)$s.
Output/Results:	The Election Authority holds a list of all e-voters identified by the voter's identifier of the Election Domain ($ssPIN(v)$).

The Registration Authority stores the list of e-voters.

P1-A10: Create List of E-Voters for Election Domain

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	Registration phase is over and all e-voters have been registered for e-voting.
Output/Results:	The Election Authority receives a list of encrypted $vPIN$s.

As an outcome of the registration phase, the Election Authority receives a list of all e-voters. Since the Election Authority must not gain access to the conventional sectoral voting identifier used within the Registration Domain ($ssPIN(v)$), the EVITA voting schema introduces the $vPIN$ as the voting identifier to be used within the Election Domain. Vice versa, the Registration Authority must not have access to the $vPIN$ used to identify voters within the Election Domain. Thus, the $vPIN$ has to be encrypted immediately after creation and has to be sent to the Election Authority in an encrypted form (for more information, see description in section 8.3.5).

The registration service however has to provide the Election Authority with a list of encrypted $vPIN$s representing all registered e-voters.

P1-A11: Store List of E-Voters for Election Domain

Responsibility:	Election authority (Election Domain)
Input/Prerequisites:	A list of encrypted $vPIN$s.
Output/Results:	The Election Authority holds a list of all e-voters identified by the voter's identifier of the Election Domain ($vPIN$).

The Registration Authority creates a voting identifier for the Election Domain ($vPIN$) for each registered e-voter. Since the creation of the $vPIN$ takes place in the Registration Domain, the $vPIN$ is immediately encrypted upon created. Finally, the Election Authority receives a list of e-voters identified by their $vPIN$ and stores it securely.

8.3.4 Objectives and Results

The registration process sets up the basis for the election phase. Thus, the voter receives all the information and credentials needed to vote electronically and the Election Authority puts out a list of voters which have been registered for electronic voting.

The Voter

During the registration phase, the voter explicitly registers for electronic voting. As a result, the Registration Authority excludes her from voting by conventional means and marks her as "e-voter" on the electoral

roll. In exchange, the voter receives all data and credentials necessary to vote electronically. These are:

- ballot envelope
- ballot card

The Registration Authority

At the end of the registration process, the Registration Authority holds the current electoral roll in which all e-voters are marked. This list is the basis for the conventional election conducted in parallel. With this list, the election officials at the polling stations can decide whether a voter is eligible to vote by conventional means. The electoral roll is created based on $ssPIN(v)$s, since $ssPIN(v)$s are the proper identifier for voters (citizens) within the Registration Domain.

The Election Authority

For the Election Authority, the list of e-voters is the most important result of the registration process. It receives this list after the registration process is completed. The list of e-voters for the Election Authority is based on $vPIN$s. Since this list is created during the registration process, and thus within the Registration Domain, a voter's $vPIN$ becomes encrypted for the Election Authority immediately after creation. The list of e-voters for the Election Authority therefore consists of encrypted $vPIN$s.

8.3.5 Sub-Process: Create Voting Credentials

As mentioned in the description of the registration process in section 8.3, the step "Creating Voting Credentials" (P1-A4) is considered to be the core component of the whole registration procedure. This core component is responsible for:

- the separation between Registration Domain and Election Domain
- the creation of $ssPIN(v)$
- the creation of $vPIN$

This activity is critical regarding election secrecy since both the registration and election domains come into contact with each other. This sub-process creates voters' identifiers for the Election Domain ($vPIN$) from a given $ssPIN(v)$. In order to keep both domains separated and since this process is running in the Registration Domain, the $vPIN$ created must be encrypted immediately so that the Registration Domain is not able to access the voter's corresponding identifier in the Election Domain. Therefore, this activity uses a public key of the Election Authority in order to encrypt $vPIN$s immediately. This sub-process is also responsible for creating blank ballots for voters. Since a voter's blank ballot contains her $vPIN$ as well, the blank ballots created must be immediately encrypted for the voter using the voter's public encryption key.

As described in section 7.2.2, the $vPIN$ is created by applying a keyed HASH-function to the encrypted $ssPIN(v)$. Thus, this sub-process requires not only the Registration Authority's secret key but also the

Election Authority's secret key. The use of the latter secret key is crucial at this stage as the $vPIN$ creation process takes place in the Election Domain.

As the following description of this sub-process will point out, the technical implementation of this sub-process must adhere to stringent security requirements. It is required that the technical implementation of this sub-process become sealed after it has been set up. The core component in particular, which holds and deals with the Election Authority's secret keys should be provided by the Election Authority in form of a encapsulated, sealed security module. This core module should provide interfaces for the external environment (i.e. to the registration service) only. Any attempt to manipulate this core module must be easily detectable. A compact module can be verified more easily and is more controllable from an organisational perspective as well.

The main component of the core module provided by the Election Authority should be a hardware security module that securely holds the secret key of the Election Authority used to create $vPIN$s. This hardware security module should provide a shared key schema in order to import the secret key (as depicted in figure 7.5; see algorithm of $vPIN$ creation defined in section 7.2.2.3). Moreover, this core module must hold the public encryption key of the Election Authority—the key is used to encrypt the $vPIN$s after they have been created—in a very secure way as well, preferably inside the hardware security module itself.

It should not be possible to exchange, spy-out, or modify the Election Authority's secret key for $vPIN$-creation. Nor should it be possible to exchange, spy-out, modify the public key for encrypting $vPIN$s after the core module has been set up by the Election Authority. After the whole election is completed, all keys—or preferably the whole core module—should be securely and completely erased. If the core module is designed as a compact stand-alone component, the destruction of the whole core module is advisable. However, at least the secure deletion of the keys held by hardware security modules is achievable, since this is a state-of-the-art feature of reputable hardware security modules.

The whole sub-process of creating voting credentials is depicted in figure 8.3. This sub-process involves all three actors—the voter, Registration Authority and Election Authority—as well as their domains.

P2-A1: Verify Identity-Link

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The voter's Identity-Link.
Output/Results:	None.

Although the voter has already been identified in activity P1-A2 according to the Citizen Card concept and the voter's Identity-Link is assumed to be verified, the Identity-Link should be verified here once again for two reasons. Firstly, identification and authentication of a voter following the Citizen Card concept is usually done using a standard identification module (e.g. MOA-ID). If this identification module is faulty or, generally speaking, if the Identity-Link has been altered by an attacker, registration would be impossible or the voting credentials created would be useless for the voter. The latter is the worse of the two. Secondly, based on the information given in the Identity-Link, the registration service creates the $ssPIN(v)$ and the $vPIN$. All voting credentials are finally encrypted by applying the voter's public key that is stored in the Identity-Link. Thus, if an attacker is able to manipulate the public key by tampering the Identity-Link, the voting credentials as well as the $vPIN$ contained will be encrypted for a different person (the attacker) or will not be able to be decrypted by the voter.

The whole sub-process of creating voting credentials should be implemented as an encapsulated device

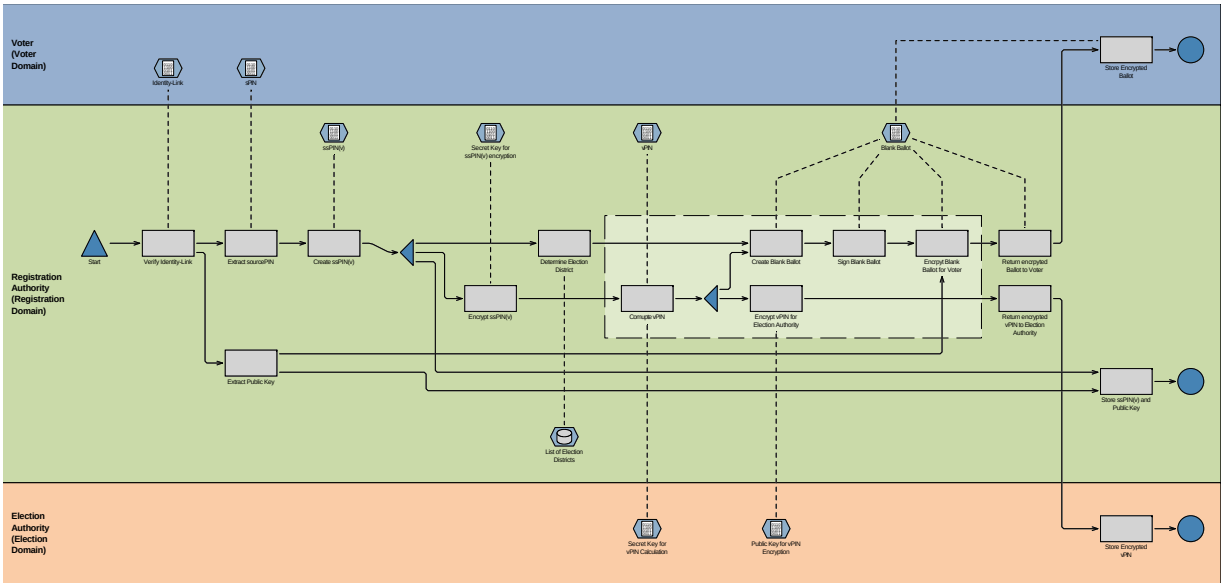

Figure 8.3: Sub-Process: Creation of voting credentials (a high resolution figure can be found in appendix B.2).

with well defined interfaces and input elements. The Identity-Link is one of these input elements. From an organisational perspective, it is advisable to check these input elements in the device once more.

For the reasons mentioned, this activity carries out an additional verification of the electronic signature on the Identity-Link. This activity also verifies whether the certificate used to sign the Identity-Link is an official certificate from the issuing authority, namely the Source PIN Register Authority, and whether this certificate is valid and has not been revoked.

P2-A2: Extract Source PIN ($sPIN$)

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The verified Identity-Link of the voter.
Output/Results:	$sPIN$.

This activity extracts the Source PIN ($sPIN$) from the given Identity-Link.

P2-A3: Create $ssPIN(v)$

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The $sPIN$ of the voter.
Output/Results:	The according $ssPIN(v)$ of the voter.

In order to uniquely identify the voter throughout the election process, the Registration Authority has to compute a sector-specific personal identification number ($ssPIN$) for the current election event—the $ssPIN(v)$. The algorithm used to compute a $ssPIN(v)$ is given in section 7.2.2.2.

This activity extracts the $sPIN$ from the Identity-Link and applies to it the defined derivation algorithm. The resulting $ssPIN(v)$ is the citizen's unique sectoral identifier for the current election event. The

$ssPIN(v)$ will be used to identify the citizen for any administrative actions required in connection with this election. Thus, the $ssPIN(v)$ is stored along with other administrative information about the voter and is also used to manage the list of e-voters within the Registration Domain.

All citizens who have registered to vote electronically are managed in a database. In order to be able to prove whether or not a person has decided to vote electronically, the identifier used for managing the list of e-voters must be a conventional sectoral e-governmental identifier as this can be determined without the person's Citizen Card if necessary. This is necessary in the event that a citizen loses her Citizen Card, etc. Therefore the $ssPIN(v)$ is used as the personal identifier of the citizen within the Registration Domain.

P2-A4: Determine Election District

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The $ssPIN(v)$ of the voter.
Output/Results:	The voter's election district.
	A list of voters and their respective election districts.

Based on the voter's identifier for the Registration Domain—the $ssPIN(v)$—the Registration Authority holds a list assigning every voter to a certain election district. The registration service determines a voter's election district based on this list. The election district is necessary as input for creating the blank ballot card in the next activities.

P2-A5: Extract Public Key

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The voter's verified Identity-Link.
Output/Results:	The voter's public key for encrypting her blank ballot

The Identity-Link contains the citizen's public keys. The Austrian Citizen Card usually contains two key pairs: one for creating electronic signatures and a second one for encryption purposes. The Identity-Link thus holds two public keys. For encrypting the voter's blank ballot, the second public key in the Identity-Link is taken.

P2-A6: Encrypt $ssPIN(v)$

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The voter's $ssPIN(v)$.
Output/Results:	The voter's encrypted $ssPIN(v)$($ssPIN(v)$').

The $ssPIN(v)$ is encrypted by applying a secret key provided by the Registration Authority as required by the $vPIN$-creation algorithm proposed in section 7.2.2.3. The encrypted $ssPIN(v)$ (denoted as $ssPIN(v)'$) is used as input for the $vPIN$ creation procedure that takes place in activity P2-A7.

P2-A7: Compute $vPIN$

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The voter's encrypted $ssPIN(v)$.
	The secret key of the Election Authority used for creating the $vPIN$.
Output/Results:	The resulting $vPIN$ of the voter.

The $vPIN$ is created by applying a keyed HASH-function to the voter's encrypted $ssPIN(v)$ (more details about the creation of the $vPIN$ is given in section 7.2.2.3). This activity creates the $vPIN$ and thus is in the possession of the secret key of the Election Authority.

Any technical implementation of this activity has to ensure that no other entity or activity can access or use the Election Authority's secret key. Therefore, the implementation of this activity should be encapsulated in a sealed module provided by the Election Authority. It should be based on a hardware security module that securely holds the Election Authority's secret key (as suggested in section 7.2.2.3).

P2-A8: Encrypt $vPIN$ for Election Authority

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The voter's $vPIN$.
Output/Results:	The encrypted $vPIN$ (encrypted for the Election Authority).

Although the $vPIN$ is created in the Registration Domain, no service or entity of the Registration Domain is allowed to access a voter's $vPIN$. To prevent this, the registration service must encrypt the $vPIN$ for the Election Authority immediately using the Election Authority's public key.

This activity is responsible for encrypting the $vPIN$. The public key of the Election Authority should be securely stored and it must be ensured that this key cannot be altered or modified. It is recommended to store this key in a hardware security module. The technical implementation of this activity should be to encapsulate it in a sealed module provided by the Election Authority. It is advisable to encapsulate the technical implementations of activity P2-A7 and this activity in the same sealed module.

P2-A9: Create Blank Ballot

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The voter's $vPIN$.
	The voter's election district.
Output/Results:	The blank ballot (containing the ballot envelope and the ballot card) for the given voter.

This activity creates the blank ballot for the current voter. The blank ballot at this stage consists of two parts:

- the ballot card
  ...holding the voter's options according to her election district
- the ballot envelope
  ...holding the voter's $vPIN$ and her election district (e.g. represented through some election district identifier)

A detailed definition of a blank ballot and its parts is given in section 7.2.3.1.

The ballot card holds the voting options. Since the list of options (candidates) may vary from one election district to the next, the ballot card is created according to the voter's election district. The ballot card is the core element of the blank ballot. The voter makes her decision according to the options provided in the ballot card. The final cast vote is made up of the options that were selected by the voter. It is of paramount importance that the authenticity of the ballot card is verifiable by the voter as well as by the Election Authority during the counting procedure. This can be achieved by applying a separate electronic signature to the ballot card.

It is important that the signature on the ballot card cannot be used to identify the voter. For instance, creating and signing the ballot card on-the-fly during this activity may lead to a signature value which could be used to identify the voter if the signature on the ballot card includes a timestamp (e.g. the signing-time). To prevent this, the way to implement this activity should either be to create or sign all possible ballot cards in advance, or it should be to sign ballot cards on-the-fly without adding any timestamp value. In general, the first possibility would be preferable since the resulting signature may contain the (claimed) signing time. In the latter case, although the signatures would lack of a signing time, it would be possible to figure out the signing-time by making organisational assumptions. This would even be feasible since the signing time is only important for verifying the status of the signing certificate. In terms of certificate verification it must be ensured that the signing certificate has not been revoked until the very last ballot card has been issued. This could be achieved by making organisational assumptions as well. However, the issue of having a signing time within the signature of blank ballot cards should not be overrated as long-term verifiability is not a dedicated requirement.

The ballot envelope holds any additional information necessary in order to identify the voter and to authenticate her through the cast vote. In the case of the EVITA voting schema, this information includes:

1. the voter's $vPIN$
2. the voter's election district

This activity takes all these elements as input, creates the ballot card according to the voter's election district, and creates the ballot envelope which will hold the voter's $vPIN$and election district. Finally, this activity combines the ballot card and ballot envelope to form the voter's blank ballot. Since the ballot envelope holds the voter's $vPIN$, the technical implementation of this process has to ensure that other activities or other entities are not able to access the blank ballot and/or able to link this ballot using the $vPIN$ to the voter's identity (e.g. name, $ssPIN(v)$, etc.).

P2-A10: Sign Blank Ballot

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The voter's blank ballot.
Output/Results:	The signed blank ballot.

The whole blank ballot created in the preceding activity P2-A9 must be electronically signed. The ballot card itself is signed already, however, the whole ballot containing the ballot envelope has to be signed as well in order to assert the combination of ballot card and ballot envelope.

This activity signs the voter's blank ballot, which consists of the ballot card and the ballot envelope on-the-fly. Although this activity is located within the Registration Domain, the signing certificate used may

belong to the Election Authority. Finally, the voter should be able to prove the authenticity of her blank ballot by verifying this signature.

P2-A11: Encrypt Blank Ballot for Voter

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The signed blank ballot. Voter's public key
Output/Results:	The signed blank ballot that has been encrypted for the voter.

The blank ballot contains the $vPIN$ of the voter, so it must not be stored or transmitted in unencrypted form by either any entity or service within the Registration Domain or the voter herself.

This activity takes the public key of the voter's Citizen Card from the voter's Identity-Link (see activity P2-A5) and uses it to encrypt the blank ballot. This ensures that the encrypted blank ballot can only be decrypted by the voter using her Citizen Card.

P2-A12: Return encrypted Blank Ballot to Voter

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The voter's encrypted blank ballot.
Output/Results:	The voter holds her encrypted blank ballot.

This activity returns the encrypted blank ballot to the voter.

P2-A13: Store encrypted Blank Ballot

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The voter's encrypted blank ballot.
Output/Results:	The voter securely stores the received ballot.

The voter has to securely store the returned encrypted blank ballot that contains all her voting credentials and her ballot card.

P2-A14: Store $ssPIN(v)$ and Public Key

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The voter's $ssPIN(v)$. The voter's public key.
Output/Results:	The Registration Authority prepares a list of e-voters by using the voters' $ssPIN(v)$s.

The Registration Authority has to create a list of e-voters using the personal identifiers of the Registration Domain, i.e. the $ssPIN(v)$. Since the $ssPIN(v)$ is a conventional sector-specific personal identifier, every public administration can use it to identify a citizen. Thus, the Registration Authority prepares a list of $ssPIN(v)$ that contains all voters who have decided to vote electronically. This list is the input for creating electoral rolls for conventional polling stations. These electoral lists are used by the election officials in the polling stations in order to distinguish e-voters from conventional voters.

Within this activity, $ssPIN(v)$s are added to a roll or are stored in a database in order to be able to create the list of e-voters at the end of the registration phase.

This activity also stores the voter's public key from the voter's Identity-Link and uses it to encrypt her voting credentials along with her $ssPIN(v)$. The public key is stored to be used later during the assert vote sub-process to encrypt the assertion (see description in P4-A13 and P4-A14 provided in section 8.4.2).

P2-A15: Return encrypted $vPIN$ to Election Authority

Responsibility:	Registration Authority (Registration Domain)
Input/Prerequisites:	The voter's encrypted $vPIN$ (encrypted for the Election Authority).
Output/Results:	The Election Authority receives a list of encrypted $vPIN$s.

This activity returns encrypted $vPIN$s to the Election Authority.

P2-A16: Store encrypted $vPIN$

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	List of encrypted $vPIN$s.
Output/Results:	The Election Authority holds a list of encrypted $vPIN$s.

The Election Authority has to securely store the returned encrypted $vPIN$ of every e-voter. The Election Authority needs a list of all e-voters in order to determine whether or not a cast vote belongs to an eligible e-voter without learning her identity. With the introduction of the $vPIN$, the voter remains anonymous in the Election Domain.

During the election phase, conventional polling stations may need to query the Election Authority to check whether or not a given e-voter has already cast her vote electronically. In this case, the polling station uses the $vPIN$ in order to identify the e-voter in question. A detailed description of the $vPIN$ and its use is given in section 7.2.2.

8.4 Election Phase

The EVITA-voting concept divides the election phase into three different sub-processes:

1. Fill-In Vote
2. Assert Vote
3. Cast Vote

Depending on the organisational and technical implementation of the EVITA voting concept, the assert vote process and the cast vote process may be seamlessly joined together (see discussion on variations of the EVITA concept provided in section 8.6). The following sections describe each of these sub-processes in detail.

8.4.1 Sub-Process: Fill-In Vote

This sub-process deals with the voter making her decision and preparing her vote for being cast. This requires the voter to make her personal decision and to fill in her blank ballot. The voter is the only actor involved in this sub-process. The process diagram given in figure 8.4 illustrates this process.

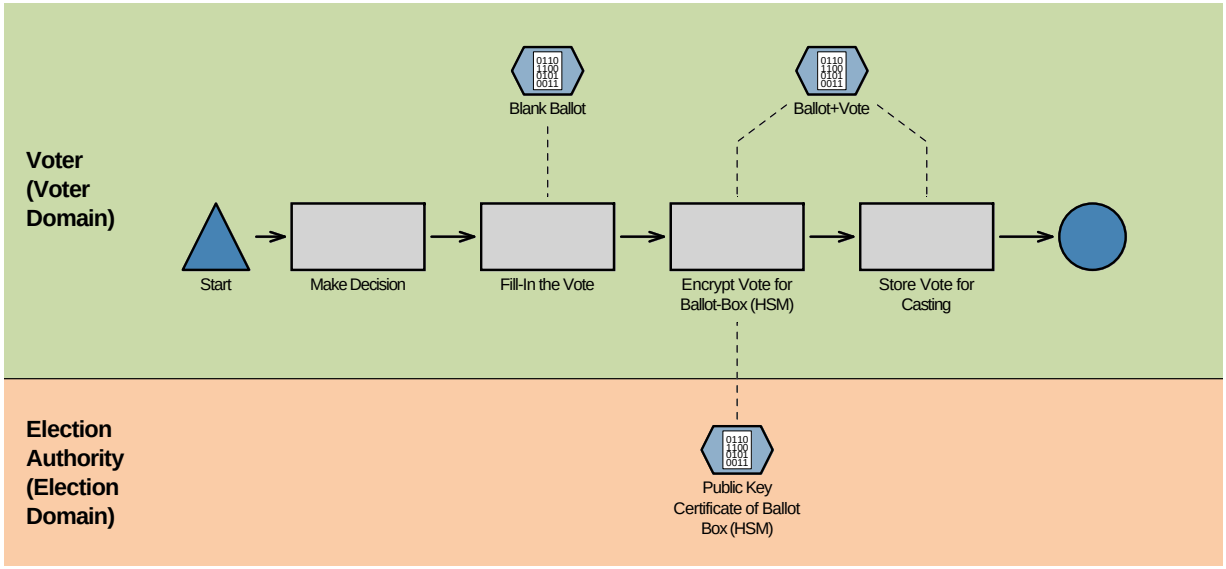

Figure 8.4: Sub-process: Fill-In Vote (a high resolution figure can be found in appendix B.3).

8.4.1.1 Actors and Participating Authorities and their Domains

Within this process, only one actor is required:

- Voter (Voter Domain)

The Voter

The voter has already been registered for e-voting and she holds her blank ballot containing all voting credentials required for voting electronically (i.e. her ballot card and ballot envelope). The voter has already verified her voting credentials after having them received from the registration service.

During this process, the voter has to prepare her vote for being cast.

8.4.1.2 Context and Prerequisites

This process comes after the registration process. The prerequisite for the present process is that the registration process has been carried out.

Prerequisites for the Voter

In addition to the general requirements given in section 8.1.1, the following prerequisites have to be fulfilled:

1. The voter must have been registered for e-voting.
2. The voter must hold her decrypted blank ballot containing the ballot envelope and the ballot card. Decryption may be done using her Citizen Card in advance (similar as described in activity P1-A5; see section 8.3).
3. The voter has already verified that her blank ballot and the elements contained are authentic.

8.4.1.3 Stepwise Process Description

During this process the voter is asked to make her decision and prepare the ballot for being cast. The voter initiates this sub-process.

P3-A1: Make Decision

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	None.
Output/Results:	None.

This activity is carried out personally by the voter. The voter has to make her decision by choosing from the list of possible options for the present election. From a technical point of view, the voter's decision may be based on the options provided in the blank ballot. However, the possibility to intentionally cast an invalid vote might also be a possible decision.

P3-A2: Fill-In the Vote

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The decrypted blank ballot.
Output/Results:	The created vote.

The voter has made her decision and now she has to fill-in the vote accordingly. The voter must decrypt her encrypted ballot by using her Citizen Card, if it has not been done already.

A technical realisation might be to create the vote using a voting client. For example, the voting client takes the decrypted ballot card as input and asks the voter to choose amongst the provided options. Then the voting client creates the vote according to the voter's decision. The method used to create a blank ballot depends heavily on the technology used to implement the EVITA voting concept.

P3-A3: Encrypt Vote for Ballot Box (Hardware Security Module)

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The created vote.
Output/Results:	The encrypted vote.

The filled-in vote must be encrypted for the electronic ballot box. As stated in section 7.2.1, the vote has to be immediately encrypted after it is created. The only time it will be decrypted is for the counting device during the counting procedure (see description of the counting process given in section 8.5).

The public key for encrypting the vote has to be distributed to the voter in the form of a public key certificate which has been preferably issued by a certificate service provider trusted by most of the citizens. Here the question arises as to how to distribute this certificate to the voters. This is a crucial issue since an attacker could attempt to distribute false or modified certificates and thus mislead voters into encrypting their votes with a wrong public key. As a result, the attacker might be able to reveal the voter's decision. Furthermore, the vote will not be able to be decrypted by the counting device and thus the vote will have been stolen from the voter.

Several possibilities seem to be adequate for distributing the public key certificate. The certificate should be sent to the voter along with her voting credentials during the registration phase. Additionally, an official announcement about the public key certificate is advisable. Within this announcement, the issuer and the serial number of the certificate as well as the certificate's fingerprint should be announced so that every voter receives this information out of band (out of band as the primary way of certificate distribution, i.e. the registration process). Thus, every voter can easily prove the correctness of the public key certificate she has been told to use. The voter is also able to retrieve the certificate from the certificate provider directly if she has any doubt.

The voter only has to encrypt the vote itself. All other elements provided within the blank ballot, such as the ballot envelope or the ballot card, remain unencrypted although they will be entered into the electronic ballot box as well. This activity only deals with the encryption of the part carrying the voter's decision. This part is denoted as "vote" (see section 7.2.3.1 defining the structures of vote, ballot and ballot envelope).

P3-A4: Store Vote for Casting

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The filled-in ballot containing the voters encrypted vote.
Output/Results:	The voter securely holds her prepared ballot containing her encrypted vote.

The voter securely stores her ballot containing her encrypted vote. Depending on the amount of time between this sub-process and the succeeding sub-processes of the election phase, it could be advisable to store the prepared ballot in encrypted form, preferably using the citizen's Citizen Card.

8.4.1.4 Objectives and Results

This process is the first one in the election phase. It only involves the voter.

The Voter

During this process the voter is asked to make her decision and to prepare her vote. This process results in two different results: the voter's personal decision and the filled-in vote. After this process is completed, the voter holds an encrypted vote and thus is prepared for the next process step, "Assert Vote".

8.4.2 Sub-Process: Assert Vote

This is the second of three sub-processes in the election phase. It covers all actions and activities necessary to assert the vote by a trusted Asserting Authority. A very important requirement is that the registration phase was completed and all authorities are equipped with their electoral rolls—created either on the basis of the $vPIN$ or on the basis of the $ssPIN(v)$—and that the voter holds all credentials needed as well as the encrypted vote ready to be cast.

The voter is asked to add an electronic signature to her vote during this process, in order to be able to recognize any form of tampering. However, the voter is not required to sign her vote personally by using her Citizen Card. In order to prevent branding her cast vote with her personal certificate, this process introduces a trusted third party, an Asserting Authority. The Asserting Authority is also responsible for upholding the principle of indirect voter-authentication (a description of indirect voter-authentication is given in section 7.2.3.2).

It is important to mention that the introduced Asserting Authority is neither an existing authority nor it is substantiated by Austrian law. However, the EVITA voting concept considers the Asserting Authority to be a very important contribution in order to separate the Registration Domain from the Election Domain. Thus, the preferred way of setting-up the EVITA voting system is to put a trusted third party in place as the Asserting Authority. However, if an Asserting Authority is not achievable on an organisational or legal level, the service of the Asserting Authority—the asserting service—may also be carried out by the Registration Authority or the Election Authority in form of a strictly separated service that precedes the service for casting votes. In this case, stringent organisational and technical measures have to be put in place in order to ensure the separation of services and both domains.

The process diagram given in figure 8.5 illustrates this process. This process description describes the recommended form of the EVITA concept. Thus, it assumes that an independent Asserting Authority is in place.

At the end of this process, the voter holds her asserted vote that is ready to cast.

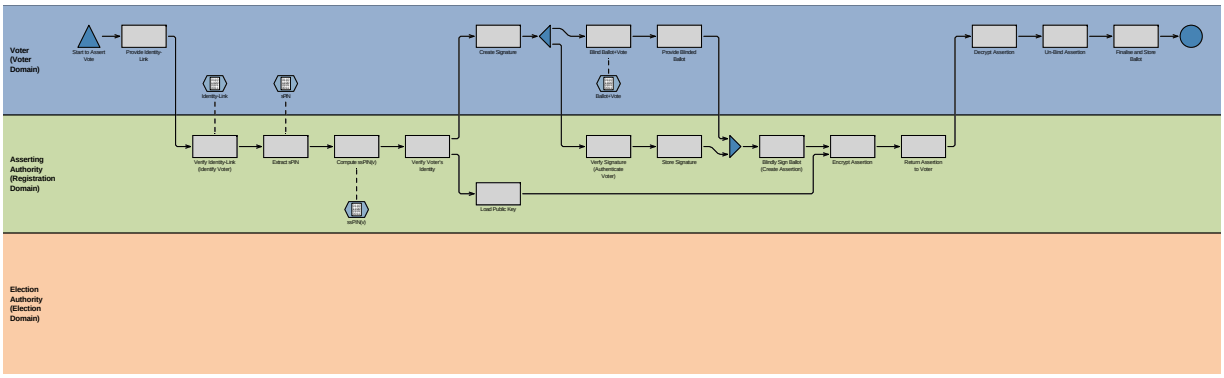

Figure 8.5: Assert Vote Process (a high resolution figure can be found in appendix B.4).

8.4.2.1 Actors, Participating Authorities and their Domains

Two actors are required in this sub-process:

- Voter (Voter Domain)
- Asserting Authority (Registration Domain)

The Voter

The voter has completed the preceding sub-process "Fill-In Vote" and thus holds an encrypted vote which is ready to be cast. The voter is now required to add an electronic signature to the whole ballot consisting of the voter's ballot envelope, ballot card and her encrypted vote.

The Asserting Authority

The Asserting Authority is responsible for providing an asserting service which is used to authenticate the voter and to sign the voter's ballot containing her vote. There is no legal basis for this extra authority, however, the role and duties of this Asserting Authority are very important elements of the EVITA voting concept since the asserting service is used to blindly sign the ballot after the voter has been authenticated. Thus, the signature of the Asserting Authority on the voter's ballot replaces the voter's personal signature since the voter's personal signature would otherwise brand the ballot with her signing certificate.

Furthermore, the asserting service is important with regards to indirect voter-authentication. Since the asserting service accesses the electoral roll prepared by the registration service, the asserting service encrypts the resulting assertion, i.e. the blindly signed ballot, by applying the voter's public key stored during the registration process. The asserting service ensures that the voter who has registered for e-voting through the registration service is the only who is able to decrypt the assertion.

The Asserting Authority is located in the Registration Domain since it makes use of the voter's $ssPIN(v)$ and needs access to the voter's signing certificate. Due to the lack of a legal basis for an Asserting Authority, the role of the Asserting Authority could be fulfilled by the Registration Authority as well following stringent technical and organisational requirements. Nevertheless, it is recommended to set up the EVITA system with a dedicated Asserting Authority.

8.4.2.2 Context and Prerequisites

This process follows the registration phase. The e-voter has to have a filled-in vote which is already encrypted.

Prerequisites for the Voter

In addition to the general requirements given in section 8.1.1, the following prerequisites must also be fulfilled:

1. The voter must have made her decision.

2. The voter must have a filled-in vote.
3. The voter's vote must be encrypted using the ballot box's public key certificate.

Prerequisites for the Asserting Authority

The Asserting Authority is responsible for signing the ballot provided by the voter. It thereby asserts indirectly that the vote presented by the voter belongs to the voter's claimed identity. The Asserting Authority is situated in the Registration Domain so it makes use of the $ssPIN(v)$ in order to identify the voter. Furthermore, the Asserting Authority may access the voter's signing certificate.

In addition to the general requirements given in section 8.1.4, the following prerequisites have to be fulfilled:

1. The Asserting Authority has to be equipped with a signing certificate that is used to sign the voter's ballot (containing her encrypted vote).

8.4.2.3 Stepwise Process Description

Assuming that the service for voter authentication is provided by an independent Asserting Authority—which is the preferred and recommended method—this sub-process may take place a certain time before the cast vote process. The voter initiates this sub-process.

P4-A1: Start to Assert a Vote

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	None.
Output/Results:	None.

The voter has to initiate the assert vote process by accessing the asserting service provided by the Asserting Authority.

P4-A2: Provide Identity-Link

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	Voter must have a Citizen Card.
Output/Results:	Asserting Authority receives the voter's Identity-Link.

The voter is asked to provide her Identity-Link. The Identity-Link is used to identify the voter according to the Austrian Citizen Card concept. The Identity-Link contains the voter's $sPIN$ which is used to create the voter's $ssPIN(v)$.

P4-A3: Verify Identity-Link

Responsibility:	Asserting Authority (Registration Domain)
Input/Prerequisites:	Identity-Link provided by the Voter.
Output/Results:	The verified Identity-Link.

The Asserting Authority verifies the authenticity of the Identity-Link provided by the voter. The Identity-Link is signed by the issuing authority—the Source PIN Register Authority—thus the Asserting Authority verifies the signature on the Identity-Link with respect to its cryptographic correctness and verifies the validity of the signing certificate.

P4-A4: Extract Source PIN

Responsibility:	Asserting Authority (Registration Domain)
Input/Prerequisites:	The voter's verified Identity-Link.
Output/Results:	The voter's $sPIN$.

The Asserting Authority extracts the $sPIN$ from the verified Identity-Link. The $sPIN$ is required to create the voter's $ssPIN(v)$.

P4-A5: Compute ssPIN(v)

Responsibility:	Asserting Authority (Registration Domain)
Input/Prerequisites:	The voter's $sPIN$.
Output/Results:	The voter's $ssPIN(v)$.

Based on the $sPIN$ extracted from the voter's Identity-Link, the Asserting Authority creates the according $ssPIN(v)$ identifying the voter within the Registration Domain. Section 7.2.2.2 describes the $ssPIN(v)$ generation process in detail.

P4-A6: Verify Voter's Identity

Responsibility:	Asserting Authority (Registration Domain)
Input/Prerequisites:	The voter's $ssPIN(v)$. Electoral roll provided by the Registration Authority.
Output/Results:	The signed $ssPIN(v)$ of the voter.

The asserting service identifies the voter by her $ssPIN(v)$. Furthermore, the asserting service searches for the voter on the electoral roll provided by the Registration Authority. Only if the voter can be found—thus the voter requesting the asserting service is registered as an e-voter—should the asserting service proceed with asserting.

Depending on the underlying organisational election model, it might be desired to mark the voter on the electoral roll so that she cannot make a second request for assertion. However, if the election model allows a voter to cast her ballot several times (e.g. in order to correct and replace a previously cast ballot), marking voters is not desirable.

P4-A7: Create Signature

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	Text to be signed.
Output/Results:	The signed text.

The Asserting Authority asks the voter to sign some text in order to authenticate the voter. This could entail the asserting service asking the voter to assert that she has been unattended and was not influ-

enced by any third party while filling-in the vote. However, this is more of a legal matter than a technical requirement.

The signature created by the voter is mainly required for authenticating the voter. The voter creates the required electronic signature using her Citizen Card.

P4-A8: Verify Signature (Authenticate Voter)

Responsibility:	Asserting Authority (Registration Domain)
Input/Prerequisites:	The signature provided by the voter. The voter's verified Identity-Link.
Output/Results:	The Verification result.

The asserting service verifies the electronic signature returned by the voter. This activity is similar to activity P1-A3 of the registration process as described in section 8.3. After successfully verifying the signature provided by the voter, the Asserting Authority is able to authenticate the voter.

In order to authenticate the voter, the asserting service verifies whether the public keys contained within the voter's Identity-Link (the Identity-Link was provided by the voter during the preceding activity) matches the electronic signature created by the voter. If one of the public keys of the Identity-Link matches the provided signature, the voter is authenticated and assumed to be the person identified in the Identity-Link (this identification procedure is again the default way of identifying/authenticating a citizen following the Austrian Citizen Card concept).

P4-A9: Store Signature

Responsibility:	Asserting Authority (Registration Domain)
Input/Prerequisites:	The voter's signature which has been positively verified.
Output/Results:	Store signature and signed text.

If the text signed by the voter is used as assertion that she has been unattended and was not influenced while filling-in her vote, the signed text has to be stored since it might be relevant at a later time (e.g. after the vote has been cast).

P4-A10: Blind Ballot

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The voter's ballot consisting of her ballot envelope, ballot card and encrypted vote.
Output/Results:	The voter's blinded ballot.

The Asserting Authority has to assert the authenticity of the voter's ballot, whereas the ballot contains the voter's ballot envelope, her ballot card as well as her encrypted vote. Since not even the Asserting Authority is allowed to access any information on the voter's ballot, the Asserting Authority is requested to add a blind signature on the voter's ballot.

Blind signatures were introduced by David Chaum [36] [39] and there are various voting schemes which are solely based on the principle of blind signatures. Section 3.3.3 discusses these schemes.

In general, a blind signature provides an entity with the ability to sign a document without having seen it. In terms of the EVITA voting concept, it means that the voter has to obfuscate her ballot (the voter has to

"blind" her ballot). She further provides the blinded ballot to the Asserting Authority which then signs the ballot without knowing its content. After the Asserting Authority returns the blindly generated signature value, the voter de-obfuscates it (the voter "unblinds" the signature value). As a result, the voter holds a ballot which has been electronically signed by the Asserting Authority whereas the Asserting Authority has not seen the ballot or the resulting unblinded signature value.

The blindly created assertion serves two purposes. Firstly, the Asserting Authority adds a signature to an electronic document without learning its content. In other words, the voter provides some electronic document to the Asserting Authority which it signs without looking at the content of the document. It is the voter's responsibility to provide a correctly blinded document representing her ballot. There is also no way for the Asserting Authority to prove whether the blinded document is really a ballot or not. Secondly, the Asserting Authority must not learn the resulting signature value as this could be used to reveal the voter's cast vote. Both purposes are perfectly served by Chaum's concept of blind signatures.

In general, this activity represents the action of the voter obfuscating her vote to prepare it for being signed by the Asserting Authority. In the following sections, the term "blinded ballot" denotes the obfuscated ballot according to David Chaum's schema.

P4-A11: Provide Blinded Ballot

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The voter's blinded ballot.
Output/Results:	The Asserting Authority receives the voter's blinded ballot.

The voter is asked to provide her blinded ballot—i.e. the blinded ballot according to David Chaum's principle—to the Asserting Authority.

P4-A12: Blindly Sign Ballot (Create Assertion)

Responsibility:	Asserting Authority (Registration Domain)
Input/Prerequisites:	A data structure representing the blinded ballot.
Output/Results:	A signed data structure representing the blindly signed ballot.

The Asserting Authority finally signs the voter's blinded ballot. This result—the detached blind signature—is referred to as blinded assertion.

P4-A13: Load Public Key

Responsibility:	Asserting Authority (Registration Domain)
Input/Prerequisites:	Data from Registration Authority (electronic electoral roll).
Output/Results:	The voter's public key provided during registration process.

During the registration process, the voter provided her Identity-Link from which her public key has been extracted in order to encrypt her voting credentials. Furthermore, the registration service stores the voter's public key provided during registration along with her $ssPIN(v)$. The asserting service uses the stored public key to encrypt the created blinded assertion for the voter. Thus it is ensured that the blinded assertion can only be decrypted by the voter who is registered.

P4-A14: Encrypt Assertion

Responsibility:	Asserting Authority (Registration Domain)
Input/Prerequisites:	The created blinded assertion.
Output/Results:	The blinded assertion encrypted for the voter.

The asserting service encrypts the prepared blinded assertion by applying the voter's public key retrieved through the preceding activity P4-A13.

P4-A15: Return Assertion to Voter

Responsibility:	Asserting Authority (Registration Domain)
Input/Prerequisites:	The encrypted blinded assertion.
Output/Results:	The voter holds the encrypted blinded assertion.

The Asserting Authority returns the created signed data structure, i.e. the blinded assertion, to the voter.

P4-A16: Decrypt Assertion

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The encrypted blinded assertion.
Output/Results:	The voter holds the decrypted blinded assertion.

The voter receives an encrypted container holding her blinded assertion. This container is encrypted using the citizen's public key of her Citizen Card (according to the Austrian Citizen Card concept, the second key-pair is used to encrypt/decrypt data). The voter is asked to decrypt the container in order to get the decrypted blinded assertion using her Citizen Card.

P4-A17: Unblind Assertion

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The signed data structure asserting her identity/authenticity and the authenticity of her vote.
Output/Results:	Un-blinded signed ballot containing the assertion provided by the Asserting Authority.

Since the Asserting Authority returns the blinded assertion as a blind signature of the voter's encrypted ballot, the voter must to unblind the received signature value. Depending on the technology used for blinding the ballot, the unblind mechanism may vary. If David Chaum's blind signature algorithm has been applied, unblinding has to be done following the analogous algorithm. As a result, the voter holds the unblinded signature value thus the unblinded assertion—further denoted as "assertion".

The voter should be requested to verify the received assertion (the contained signature value). It is important to assure the voter that the assertion returned by the Asserting Authority really represents a signature of her ballot. This issue can be addressed by verifying the electronic signature provided through the assertion. The signature verification process has to focus on two aspects. First, it must be verified that the signing certificate used to create the assertion really belongs to the Asserting Authority (the official signing certificate of the Asserting Authority should be publicly announced). Secondly, the voter has to confirm that the signed content really represents her ballot.

This activity results in a ballot containing

1. ballot envelope
2. ballot card
3. encrypted vote
4. assertion

The prepared ballot is now ready to be cast (section 7.2.3.1 defines the structure and the content of the ballot).

P4-A18: Store Vote

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The voter's ballot ready to be cast.
Output/Results:	None.

The voter has to securely store the prepared ballot. The ballot is ready to be cast.

8.4.2.4 Objectives and Results

The Voter

At the end of this process, the voter will have her ballot which has been blindly signed by the Asserting Authority; the signature value is added to the voter's ballot in form of an assertion (see section7.2.3.1 defining the structures of vote, ballot and ballot envelope). Due to the added assertion, any form of tampering is detectable. The voter's ballot is now ready to be cast.

The Asserting Authority

In exchange, the Asserting Authority may store the authentication statement signed by the voter during authentication procedure (P4-A7), for instance, as kind of self-declaration that she was unattended and uninfluenced during voting. Furthermore, the Asserting Authority may maintain a list of those e-voters who have requested asserting. However, both results are more of an optional outcome than a fundamental requirement for the EVITA voting concept.

8.4.3 Sub-Process: Cast Vote

This is the last process of the election phase. It covers all activities necessary to cast a vote, or to be more precise, to cast a ballot containing the voter's encrypted vote. A very important requirement is that the registration phase is completed and all authorities are equipped with their according electoral rolls (created either on the basis of the $vPIN$ or on the basis of the $ssPIN(v)$) and the voter holds all credentials needed as well as the ballot ready to be cast. At the end of this process, the Election Authority will hold all cast votes and stores them for the following counting phase. The process diagram given in figure 8.6 illustrates this process.

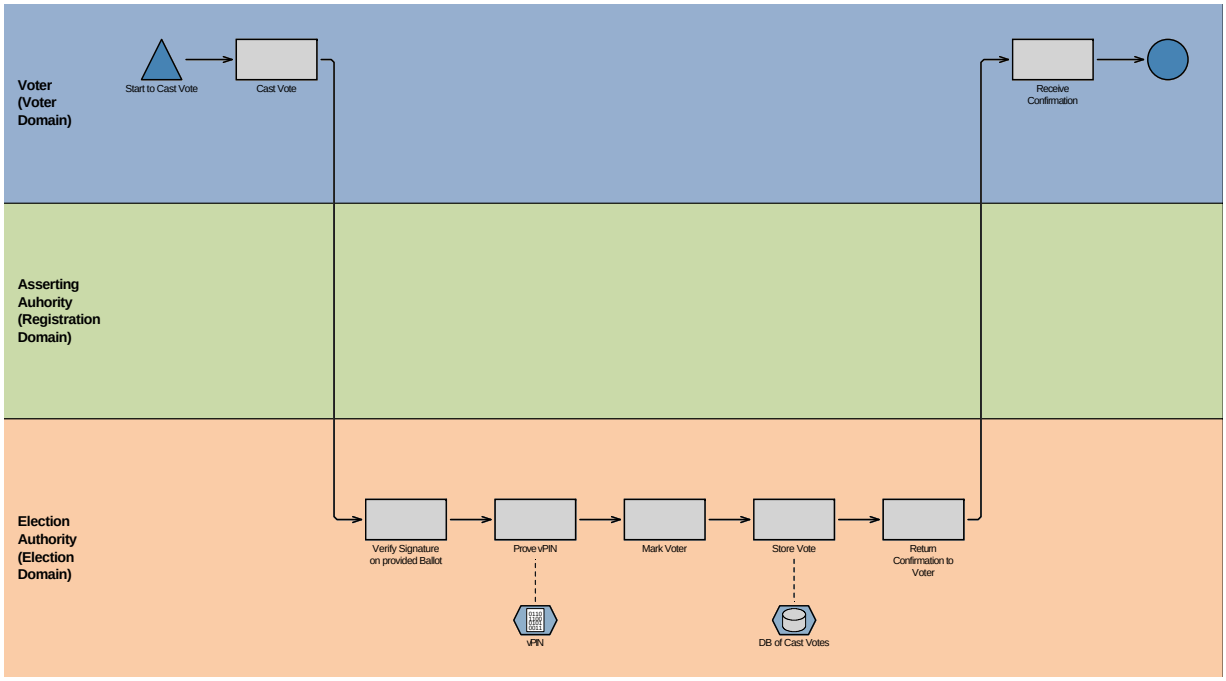

Figure 8.6: Sub-Process: Cast Vote (a high resolution figure can be found in appendix B.5).

8.4.3.1 Actors, Participating Authorities and their Domains

Two actors are required within this election process:

- Voter (Voter Domain)
- Election Authority (Election Domain)

The Voter

The voter is a citizen who is eligible to vote by law and has been already registered as an e-voter and thus is enabled to vote electronically. Furthermore, the voter holds her ballot encrypted, asserted and ready to be cast. During this process, the voter is asked to cast her prepared ballot.

The Election Authority

The Election Authority is responsible for collecting all cast ballots. It provides an election service which takes a voter's cast ballot, verifies it and stores it for the later counting phase.

8.4.3.2 Context and Prerequisites

This process follows the registration phase. All e-voters have been registered and thus hold their voting credentials. The Election Authority holds a list of $vPINs$ of all registered e-voters in order to detect unregistered e-voters.

The e-voter holds a prepared ballot that is ready to be cast.

Prerequisites for the Voter

In addition to the general requirements given in section 8.1.1, the following requirements must be fulfilled:

1. The voter must have a prepared and asserted ballot containing her ballot card, ballot envelope, encrypted vote and the assertion (issued by the Asserting Authority).

According to the description given section 7.2.3.1, the ballot to be cast consists of the following elements:

1. ballot envelope
2. ballot card
3. encrypted Vote
4. assertion

Prerequisites for the Election Authority

The Election Authority must provide a service—called a cast-vote service—that allows voters to enter their ballot. The Election Authority holds a list of registered e-voters represented by their $vPIN$s since the Election Domain is only allowed to identify voters by their $vPIN$.

8.4.3.3 Stepwise Process Description

The voter initiates this sub-process. The sub-process “Cast Vote” may take place at a certain time after the preceding sub-processes.

P5-A1: Cast Vote

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The voter holds a prepared ballot containing her encrypted vote.
Output/Results:	Election Authority receives the voter’s ballot.

The voter received an asserted ballot from the Asserting Authority during the preceding sub-process. Thus, the ballot contains the voter’s ballot envelope, her ballot card, her encrypted vote as well as the assertion provided by the Asserting Authority. During this activity, the voter is asked to submit her ballot to the cast-vote service.

P5-A2: Verify Signature on Ballot

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	The voter’s ballot.
Output/Results:	The verified ballot.

The Election Authority has to verify all the signatures on the voter’s ballot. As defined in section 7.2.3.1, the ballot provided by the voter during the cast-vote process contains three signatures:

1. the signature of the Election Authority on the ballot card
2. the signature of the Election Authority on both the ballot card and ballot envelope
3. the signature of the Asserting Authority on the whole ballot that holds the ballot card, ballot envelope and the encrypted vote. This signature is provided through the assertion attached.

The cast-vote service has to verify all three signatures. The Election Authority only accepts the voter's ballot—and thus her vote—if all three signatures are valid.

P5-A3: Prove vPIN

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	The verified ballot.
Output/Results:	The Election Authority confirms that the present voter—identified through her $vPIN$—has been registered as an e-voter.

The Election Authority proves whether or not the present voter is a registered e-voter. To do this, the Election Authority searches for the voter's $vPIN$ stored in her ballot in the list of registered e-voters.

P5-A4: Mark Voter

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	The $vPIN$ of a verified e-voter.
Output/Results:	The Election Authority marks the voter as having cast her vote.

If the voter could be successfully identified by her $vPIN$ and if the ballot provided by the voter could be successfully verified, the ballot is accepted and the voter becomes marked as having submitted a vote. As a consequence, the voter will not be allowed to submit a second vote electronically or to vote in a conventional polling station[3].

The Election Authority maintains a list or database of $vPIN$s representing all voters registered for e-voting. Every voter who submits her ballot becomes marked and thus locked against further attempts at casting a vote.

For the sake of completeness, it could be desirable to accept a second cast vote as well, depending on the legal framework of an election. Such a system would allow the voter to "correct" her first cast vote by casting another one. The EVITA voting concept has no limitations with respect to this aspect, but this process description does not specifically address this issue.

P5-A5: Store Vote

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	The verified and accepted ballot.
Output/Results:	Election Authority securely stores the cast ballot.

The Election Authority stores all ballots submitted by voters for the succeeding counting process. For storing the votes, the Election Authority has to make appropriate provisions in order to ensure that votes

[3]The e-voter is allowed to vote in a conventional polling station under certain circumstances only. Such circumstances could be a lost or defect Citizen Card, a break-down of the Internet, failure of the citizen's computer, etc. In such an event, the election officials have to prove if the voter in question has already cast a vote electronically.

cannot be manipulated, modified, added or deleted. Therefore, the Election Authority has to define and follow adequate technical and organisational security measures.

P5-A6: Return a Confirmation to the Voter

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	The voter's ballot has been accepted and stored.
Output/Results:	The voter receives a conformation.

After the vote has been accepted by the Election Authority and the voter has been marked, the Election Authority should return some form of confirmation to the voter. The confirmation should confirm that her ballot has been accepted.

As proposed in the work of Josh Benaloh [109] and many others [42] as well as required in the SERVE report [66], an e-voting system must not provide any kind of receipt. The discussion given in section 5 leads to this conclusion as well, thus, the EVITA concept is a receipt-free voting system. This means that the voting system does not provide any form of receipt to the voter so that the voter cannot use it to prove to a third party how she cast her vote. Thus the EVITA voting concept protects against the problem of selling votes.

Nevertheless, a voting system has to provide a clear confirmation to the user about whether her vote has been accepted or denied. However, the confirmation must not be signed or contain any information that makes the confirmation itself authentic. Instead of a signature or similar mechanism, the EVITA concept proposes to display a confirmation message through an authenticated secure communication channel (i.e. TLS-communication using server-certificates). Thus, the voter can prove the authenticity of the confirmation message right at the moment of reading it, but is not able to prove it to any third party. In order to prove the authenticity of the confirmation message, the voter has to authenticate the sender of the message by proving the TLS-certificate used to authenticate the secure communication channel at the sender's side (i.e. server side).

P5-A7: Receive Confirmation

Responsibility:	Voter (Voter Domain)
Input/Prerequisites:	The confirmation sent by Election Authority.
Output/Results:	The Voter is sure that her ballot has been accepted or denied.

The voter receives a confirmation about the acceptance of her ballot. The Election Authority provides an unsigned confirmation message through a strongly authenticated secure communication channel. Therefore, the voter is requested to authenticate the sender of the confirmation message by checking the TLS-certificate used to authenticate the secure communication channel at the sender's side (i.e. the TLS-certificate of the Election Authority's service). If the voter is sure that the confirmation message has been sent via an authenticated communication channel and that the sender is the Election Authority, the voter can assume that the confirmation message is authentic. The voter may believe the confirmation message, but she is not able to provide evidence to any third party.

8.4.3.4 Objectives and Results

The Voter

The voter casts her ballot containing her encrypted vote. In exchange, the voter receives a confirmation from the Election Authority stating whether her ballot has been accepted or denied.

The Election Authority

The Election Authority holds all ballots that have been cast during the cast-vote process. All ballots stored by the Election Authority have been successfully verified and accepted. Furthermore, the Election Authority holds a list of $vPIN$s representing all e-voters that have cast their ballot. This list is also used during the election phase in order to determine whether an e-voter has already cast her vote or not.

8.5 Post-Election Phase

The post-election phase covers all activities that occur after all voters have cast their vote. Although the post-election phase includes a number of processes and activities, such as archiving of votes, count and re-count of votes, etc., the EVITA voting concept only discusses the counting process since the aim of this work is to focus on the most important core elements and processes of an election event. The process diagram given in figure 8.7 illustrates the counting process.

The Election Authority is in charge of counting all cast ballots at the end of the election event. All ballots cast by a defined deadline are accepted and will be counted. Counting is strictly regulated by law. In political elections, the democratic constitution of a country usually directly influences the way of counting.

As stated in section 7.2.1, all cast votes are encrypted and will only be decrypted by the counting device. The counting device's core module is a hardware security module securely holding the secret key for the decryption of votes. So the counting process is crucial regarding the election secrecy.

Counting is usually conducted for each election district separately since each district represents a partial result. Therefore, the Election Authority sorts the cast ballots according to the election district they belong to and thus creates several subsets of cast ballots.

Each of these subsets of ballots must meet the following requirements:

- Each subset of cast ballots must represent a certain election district.
- Each subset of cast ballots must not contain more than one ballot per voter; the voter is identified by her $vPIN$ given within the ballot. This means that there must not be more than one ballot in the subset containing the same $vPIN$.
- Each subset of cast ballots is considered to be complete and must not be altered after having been counted once.

Additional organisational requirements might be necessary; for example that election districts with a very low number of voters become merged with other election districts in order to ensure election secrecy. However, this description does not address these organisational requirements further as they do not influence the technical concept.

After the initial count of votes, it might be necessary to do a re-count (this is dependent upon the legal basis of the election event). Nevertheless, an e-voting system has to ensure that a re-count cannot be abused for revealing votes. For example, counting a given set of votes once and recounting the same set minus a specific vote would reveal that particular vote as the difference between the results.

The EVITA voting concept proposes specific requirements for the counting device and for the counting process in general. The counting device has to permanently store a fingerprint that represents the set of votes for each election district. The counting device would not re-count any set of ballots from a particular election district if the fingerprint of the recounted set of ballots does not match the fingerprint stored. How to achieve this technically will be described in the following process description.

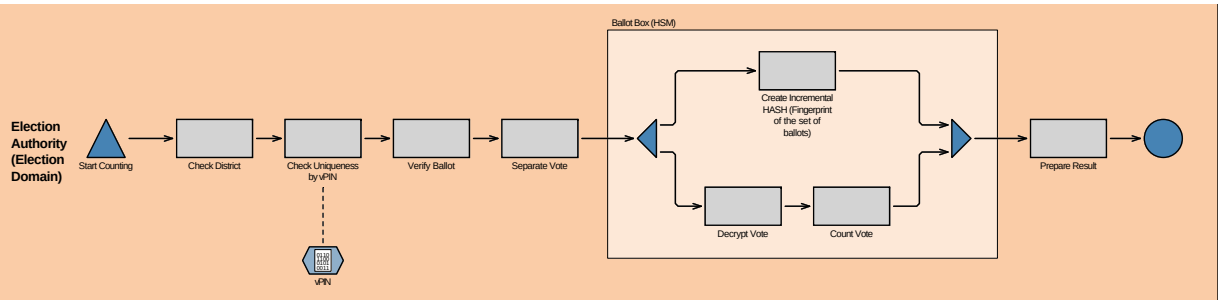

Figure 8.7: Counting Process (a high resolution figure can be found in appendix B.6).

8.5.1 Actors and Participating Authorities and their Domains

Within the registration procedure one actor is required:

- Election Authority (Election Domain)

The Election Authority

The Election Authority is responsible for the whole counting process. Thus the Election Authority runs the counting device.

8.5.2 Context and Prerequisites

The counting process is the last process of an election event. The Election Authority starts counting at a specific time after all ballots have been cast and the election phase is over.

Prerequisites for the Election Authority

As a prerequisite, the Election Authority holds all positively verified ballots that were cast within the election phase. Furthermore, the Election Authority must prepare a separate subset of ballots for each election district since each election district has to be counted separately.

In addition to the general requirements given in section 8.1.3, the following requirements must be fulfilled:

1. The Election Authority must hold all accepted ballots. These ballots have been already verified during the election phase.
2. The Election Authority must run the counting device according to the defined organisational and legal requirements. The counting device securely holds the secret key for decrypting cast votes.
3. The counting device has been initiated by the Election Authority. Depending on the technical implementation, it might be necessary to follow a stringent procedure in order to set up the counting device (e.g. due to a shared key schema, the key holders are required, etc.).

8.5.3 Stepwise Process Description

The Election Authority initiates the counting process.

P6-A1: Check District

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	The ballot cast by the voter.
Output/Results:	It is ensured that the present ballot belongs to the election district currently being counted.

The counting device should be set up to count the ballots of each election district separately. As mentioned before, this is the preferred way of counting votes.

The counting device has to check whether or not a ballot belongs to the currently counted election district. If the election district identifier given in the ballot matches the election district whose votes are currently being counted, the counting device will accept the ballot.

P6-A2: Check Uniqueness by vPIN

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	The ballot.
Output/Results:	It is ensured that no other ballot with the same $vPIN$ exists.

The counting device has to prove the uniqueness of a cast ballot by proving and comparing the $vPIN$ given in each ballot. Each $vPIN$ must not occur more than once; otherwise double cast ballots are likely.

The Election Authority conducts counting for each election district separately. The ballots of each district should be sorted according to the $vPIN$, not only for the sake of this activity but also for the creation of the fingerprint of the present (sub-)set of ballots (creation of the fingerprint see activity P6-A5).

P6-A3: Verify Ballot

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	The ballot.
Output/Results:	The verified ballot.

Although the ballots submitted by the voter were verified already in the election process, the ballots should be verified here again in order to detect whether any ballots were tampered with.

As already described in the description of activity P5-A2 (see section 8.4.3), the counting device has to verify all signatures on the ballot, in particular (according to the definition given in section 7.2.3.1):

1. the signature of the Election Authority on the ballot card
2. the signature of the Election Authority on both the ballot card and the ballot envelope
3. the signature of the Asserting Authority on the whole ballot (given within the assertion)

The counting device will accept the ballot for counting only if all three signatures can be successfully verified.

P6-A4: Separate Vote

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	The verified ballot.
Output/Results:	The separated ballot card and ballot envelope. The separated encrypted vote.

A cast ballot contains the voter's ballot card, ballot envelope and assertion as well as her encrypted vote. This activity separates the voter's encrypted vote from the rest of the cast ballot. In other words, the encrypted vote representing the voter's decision becomes separated from any kind of information that might be used to identify the voter. Afterwards, the voter's vote and all additional parts of her ballot are treated separately.

P6-A5: Create Incremental HASH (Fingerprint of the set of ballots)

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	The voter's ballot card, ballot envelope and assertion.
Output/Results:	A fingerprint (HASH-value) uniquely representing the counted (sub-)set of ballots.

The EVITA voting concept solves the problem of revealing votes through re-counting by permanently storing a fingerprint representing the first set of ballots counted for a given election district.

The EVITA-voting concept requires that the fingerprint of a (sub-)set of ballots reflects:

- a specific (sub-)set of ballots, i.e. the (sub-)set of ballots of a given election district,
- and the proper order of ballots

The first issue is obvious as the fingerprint should represent a certain set of ballots. The latter issue is an refinement since it requires that in the event of a re-count not only the exact same set of ballots has to be fed into the counting device but the order of ballots has to be the same as it was during the very first count as well. Due to this additional requirement, the EVITA voting concept prevents a vote from being revealed by changing the order of ballots and gaining access to intermediate results. However, the counting device must not provide any kind of intermediate results, hence gaining access to counter reading would be an effect of a successful attack.

As stated before, the ballots to be counted should be sorted according to the $vPIN$. Thus, in the event of a re-count the same order of ballots can be easily achieved.

There are several cryptographic methods for creating a unique fingerprint. The EVITA voting concept makes use of incremental HASH-functions to yield a fingerprint fulfilling both requirements defined before.

After the counting device has considered a ballot, the election device has to erase it immediately and completely. No information about the ballot may remain, neither in the form of temporary data nor in log files.

P6-A6: Decrypt Vote

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	The voter's encrypted vote.
Output/Results:	The decrypted vote.

This activity decrypts votes which have been separated from the rest of the ballot. Following the EVITA core principle laid down in section 7.2.1, the private key of the counting device is securely held in a hardware security module.

Although decrypted votes lack of any kind of identifying information, they must be securely treated. This and the succeeding activity P6-A7 are the only actions which deal with plain votes outside the voter domain. As stated in section 7.2, the whole counting device should be considered as a hardware security module. Therefore, it should never be possible to gain access to decrypted votes or for an attacker to access this and the succeeding activity.

P6-A7: Count Vote

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	The decrypted vote.
Output/Results:	The counting result.

Plain votes decrypted by the preceding activity are directly fed into counters. Depending on a voter's decision, the respective counter will be increased. As a result, this activity creates the (partial) result of the election.

Also this activity is crucial with respect to the election secrecy. The technical implementation of this activity has to ensure that neither any partial result nor any other information pointing to a voter's decision is leaked the outside the counting device. Therefore, the whole counting device has to be designed in the form of a secure module.

After the counting device has counted a vote, the device has to completely erase the plain vote immediately. There must not remain any trace of the vote left, either in the form of temporary data or log files.

P6-A8: Prepare Result

Responsibility:	Election Authority (Election Domain)
Input/Prerequisites:	Counting is over; the “stop-counting-signal” has been given.
	The final counter readings are available.
	The resulting fingerprint of the counted set of votes is available.
Output/Results:	The official result of counting a given (sub-)set of ballots.

This activity closes the counting process and creates the official (partial) result of counting. In order to get a result, the Election Authority has to tell the counting device to stop counting; this kind of command or signal will be further denoted as “stop-counting-signal”. The Election Authority may give the stop-counting-signal either by sending a dedicated command to the counting device or by feeding a special kind of vote, called a stop-counting-vote, into the counting device. Which form of stop-counting-signal is used depends on the way the counting process is implemented.

After receiving the stop-counting-signal, the counting device stops counting immediately and starts creating a report containing the detailed result of counting. The counting device determines whether the present election district has already been counted or not. For this check, the counting device must have a secure permanent memory with which it can store information about each election district together with the fingerprint of the district’s set of ballots determined during its very first count. If the set of ballots of a given election district has not yet been counted before, the counting device would not find any existing fingerprint for this election district. So the counting device counts the present set of ballots of the given election district for the very first time and thus stores the created fingerprint along with other information about this election district (e.g. number of ballots, date and time of first count, date and time of re-counts, etc.). If the counting device can find an entry inside its memory for the given election district, the counting device would only proceed to create a result if the previously stored fingerprint is equal to the fingerprint calculated during the re-count.

In the event of an initial count or in the event of a proper re-count—a proper re-count means that the resulting fingerprint is equal to the one previously stored—the counting device creates a detailed report containing at least (further information might be possible or requested by law):

1. identifier of the present election district
2. number of total votes
3. resulting fingerprint representing the set of counted votes
4. the counter readings in detail (including invalid votes)

It depends on the implementation whether the counting device should electronically sign the report in order to ensure its authenticity.

In the event of a re-count and if the recalculated fingerprint of the set of counted votes is not equal to the previously stored fingerprint, the counting device must completely erase all results immediately and alert the Election Authority. A detailed error report has to be created.

8.5.4 Objectives and Results

The Election Authority

At the end of the counting phase, the Election Authority receives a detailed result of the count/re-count. Depending on the legal or organisational requirements, the result could be electronically signed by the counting device in order to ensure its authenticity. If this is required, the counting device has to be equipped with a signing key and an according certificate.

Although the concrete form of the result should be defined in the course of the implementation of the counting device based on legal requirements, it is recommended to draw on existing standards and specifications. In order to maintain maximum interoperability, the result format should follow the definitions laid down by EML [1].

8.6 Variations of the EVITA-Concept

The proposed e-voting concept as presented in this process description shows the preferred way of setting up the EVITA e-voting concept. However, several variations of the concept are conceivable. Variations in the process might influence the following major aspects:

- **Conventional Elections in Parallel**
  ..how to handle conventional elections which might take place in parallel
- **Usage of** $vPIN$
  ..how to prevent double-votes and how to control a possible obligation to vote
- **Asserting Votes**
  ..how to assert votes

The proposed deployment of the EVITA voting concept assumes that electronic voting takes place parallel to conventional elections. Not only due to legal requirements[4] but also from a technical perspective. Since the e-voting schema introduced is a pure Internet-based voting schema and since the Internet itself is an instable factor by nature, the EVITA voting concept proposes using conventional polling stations as a fall-back. This means that if a voter's Internet access breaks down or even if a break down of the Internet infrastructure on a larger scale occurs, the EVITA voting concept provides the possibility for affected voters to go to a conventional polling station in order to case their vote.

If running a conventional election in parallel is not desirable, a variation of the e-voting process is possible. The question of conducting conventional elections in parallel has an impact on the issue of how to prevent double votes, because the danger of having double votes grows if an e-voter has the possibility to vote conventionally as well. For example, if e-voting takes place prior to conventional voting (advance e-voting), it would be easier to avoid double votes than when running conventional voting in parallel.

If advance e-voting is used, the conventional polling stations could be easily equipped with electoral rolls listing only those voters who have not yet cast a vote electronically. On the other hand, if conventional voting does not take place at all[5], this problem of double voting does not exist. However, the outlined

[4] In Austria today, it is not assumed that e-voting will take place prior or after conventional elections.

[5] This is not conceivable for political democratic elections; but with respect to other elections a pure electronic election could be an option, e.g. consider elections of representatives of a registered association.

EVITA voting concept assumes that a conventional election will be conducted in parallel and all described elements of the schema are aligned to this scenario. Nevertheless, since having no conventional election in parallel simplifies the process, the proposed concept can be adopted easily.

The question of having conventional elections in parallel also affects the way the voters' identifiers for the Election Domain ($vPIN$) are created. The process of creating a $vPIN$ has been designed to serve two requirements. On the one hand, the $vPIN$ should be unique for every voter in order to "identify" a voter's ballot and to prevent double cast votes. On the other hand, the $vPIN$ should be somehow linkable to the voter's electronic identity in a uni-directional way in order to be able to answer the question: "Has the given voter cast a vote or not?". This question may arise in two situations. Firstly, in the event of running conventional elections in parallel and allowing e-voters to vote conventionally in the event of technical difficulties, the election officials at the polling station might contact an e-voting register and check whether the present e-voter has already cast her vote electronically or not. Secondly, this question might arise in the case of an election where each citizen has the obligation to vote.

Both situations can be addressed through adequate legal regulations as well. The first situation might be simply disallowed by law. If the law says that after a voter has requested e-voting she is no longer allowed to vote conventionally—even in the event of a technical failure—the officials of a polling station no longer need to determine whether an e-voter has already cast her vote or not. The latter situation could also be addressed by law. Either by abandoning the obligation to vote in general[6] or by defining that if a voter requests for asserting her vote she is considered to have fulfilled her obligation to vote (since the Asserting Authority is allowed to handle the voter's $ssPIN(v)$, unique identification of voters is achieved)[7]. However, if these issues are addressed by the legal and organisational framework, the proposed $vPIN$ could also be replaced by a pseudo-random identifier that must be unique for each voter but does not have to be restorable based on the voter's identity. From the point of view of the election secrecy, this would be the better solution, but again, the proposed concept aims to demonstrate the most sophisticated scenario which includes having this kind of $vPIN$. If the defined organisational and technical requirements are followed, this would not lead to the election secrecy being threatened.

Furthermore, the Asserting Authority introduced for anonymously signing votes is an organisational suggestion so that voters do not have to sign their votes personally. Since the Austrian legal framework does not explicitly define this kind of additional independent authority as having to be provided by a third party, the Registration Authority itself could carry out the duties of the Asserting Authority instead. Alternatively, the Election Authority could act as the Asserting Authority whereby stringent organisational and technical measures would have to be taken up in order to keep the Election Domain and the Registration Domain apart.

Instead of having the Asserting Authority blindly signing a cast ballot, the voter could be requested to sign her encrypted ballot herself. This would of course lead to the cast ballot being branded with the voter's public key certificate and thus with a representation of her identity. However, the strength of the proposed e-voting concept is its core element, namely the hardware security module of the electronic urn. From this perspective, even having personally signed ballots would not be an additional threat to election secrecy at the time of the election event. But following the argumentation given in 7.2, it is recommended to avoid any identifying information on a cast ballot, so the proposed e-voting concept strongly suggests introducing a specific asserting service that prevents having cast ballots which are personally signed by

[6] In Austria today, citizen's are not obligated to vote.

[7] How to execute the obligation to vote with respect to remote e-voting more of a general question. Even in postal elections, the execution of such an obligation is hard to achieve considering that the letter containing a voter's vote might get lost on the way.

the voter.

In contrast to these simplified variations, the proposed e-voting schema could be strengthened as well. The reference process model of the EVITA concept asks the voter to cast her ballot simply by sending it to a cast-vote service provided by the Election Authority. Although no other identifying information is on the ballot, the voter's Internet address (at least her IP-address) is visible to the Election Authority. In a worst case scenario, the Election Authority—or, more generally speaking, an attacker—could try to infer the voter's identity from her IP-address. Although this might be unlikely, it is possible. In order to prevent this kind of "attack", the voter could optionally cast her vote through an mixing network which makes her request anonymous[8]. However, this is more a theoretical risk than a potential attack on the voter's election secrecy.

The variations mentioned in this section should serve as inspirations for further adoptions of the EVITA e-voting concept which might be subject for future work. Many variations of the outlined concept and described processes are conceivable and useful. The proposed e-voting concept should be considered as a framework consisting of many useful solutions and mechanisms, which finally can be designed individually, in a variety of ways, in order to suit the specific needs of a given election.

[8]The idea of mixing network follows the concept of David Chaum [36]—see also section 3.3.2 introducing e-voting schemes based on mixing nets; with respect to the Internet, a survey on mixing networks is given in [110].

Chapter 9

Implementation and Prototype

In the course of this thesis, a prototype was developed in order to verify the core elements of the EVITA concept. The prototype addresses all phases discussed in the previous chapter and adheres to the recommended implementation of the EVITA e-voting concept.

This chapter briefly outlines the elements and processes of the concept that have been implemented. It summarizes the lessons learned from the prototype and their effect on the proposed concept.

9.1 Prototype and its Scope

The prototype aims to verify the core principles of domain separation and strong encryption of votes since both principles together ensure secrecy in the election. Furthermore, it should demonstrate the interactions between the EVITA concept and existing e-Government components, such as the Citizen Card. The prototype addresses the following phases of the EVITA concept:

1. Registration Phase
    - Registration of Voters
    - Generation of Voting Credentials
2. Election Phase
    - Vote Process
    - Assert Vote Process
    - Cast Vote Process
3. Post-Election Phase
    - Counting Process

Although this prototype provides an implementation of all required phases and processes, it concentrates on the registration phase, in particular on creating voting credentials (ballot card, ballot envelope and voting identifier), and the election phase.

The prototype makes use of state of the art software modules where applicable. Functionality that was required but not yet available from software libraries was implemented for the project up to the required degree. The integration of an hardware security module is not necessary to verify the core principles of the proposed voting schema. Instead of a real hardware security module, the prototype simulates the functionality of a hardware security module in the software. The functionality of most of the organisational infrastructural elements, such as the Election Authority and Registration Authority, are simulated by a set of web-applications and databases running in the background.

9.2 Technical Outline

The prototype is fully based on Java[1] and Java components. Open Source Software was preferred whenever external Java components were used. The only external software components that were used which are not available under an Open Source License were the IAIK Security Libraries, most notably the IAIK Provider for the Java Cryptography Extension (IAIK-JCE). IAIK libraries were chosen since they are an in-house implementation of the department IAIK and were available for free for the author. However, due to the generic concept of cryptography providers, this commercial software component could be replaced by any adequate Open Source implementation.

The prototype consists of a server component and a client component. The server component runs the web application that provides the registration process and the server application used to collect cast votes. All server components and web applications are based on Java and Java Servlet technologies. The client component is used by voters to prepare their votes and is also built on Java technologies, e.g. Java SWT. The client component should be able to be run on several operating systems, thus an implementation needs to be independent from operating systems and local environments.

To summarize, here are the key data of the prototype:

- General Data:
  - Java Software Development Kit (SDK) Version 1.5.0
  - IAIK Provider for the Java Cryptography Extension (IAIK-JCE) Version 3.142
  - IAIK Elliptic Curve Cryptography (ECC) Library Version 2.15
  - IAIK XML Security Toolkit (XSECT) Version 1.10
- Client Component:
  - Java SWT Version 3.236
- Server Component:
  - Java Servlet Technologies Version 2.4 (using a Apache Tomcat 5.0 Servlet container)
  - Java Server Pages (JSP) Version 2.0 (using a Apache Tomcat 5.0 Servlet container)
  - Hibernate Version 3.0 (using a MySQL Server Version 4.1)

The following sections briefly describe the processes implemented by the prototype.

[1] Java Programming Language, developed by Sun Microsystems.

9.3 Registration Phase

During the registration process, the voter registers to e-vote. As a result, the voter becomes registered as an e-voter and receives her electronic voting credentials. From the user's perspective, the registration process is a web-form that prompts the voter to fill in her personal data and to sign the form in order to make her application official. The web form conforms to the style guide for Austrian e-Government forms[2].

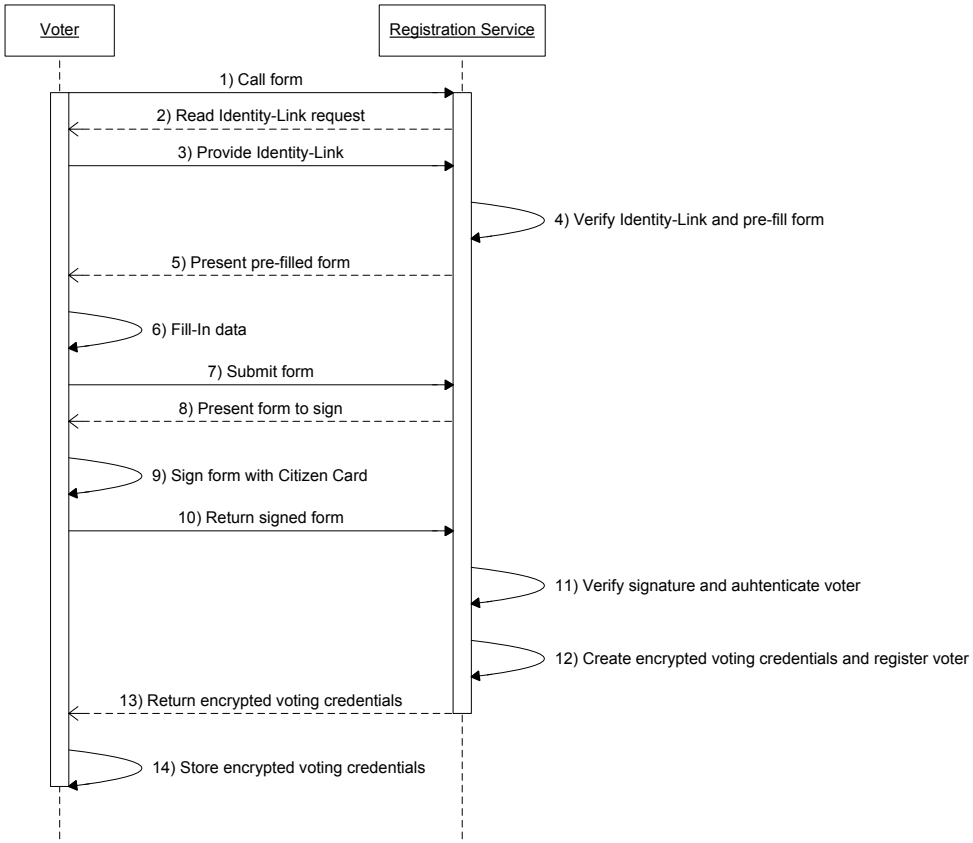

Figure 9.1: The sequence of the implemented registration procedure.

Figure 9.1 shows the registration process as a sequence diagram. This diagram along with the following description depicts the implemented process on a technical level. It sketches out how the processes theoretically defined in chapter 8 can be implemented using existing e-Government technologies.

1) Call form

The voter initiates this procedure by accessing the web application. The voter requests the registration form from the web application.

[2]The style and the layout of e-Government forms is regulated by strict conventions that define the layout and required elements of web-forms. [111]

2) Read Identity-Link

In response to this request, the registration service (web application) asks the voter to present her Identity-Link. This is done by displaying an initial web page that contains a hidden HTML form that references the voter's Citizen Card. Through the HTML form, an *InfoboxReadRequest* following the Austrian Citizen Card Concept [91] is sent to the Citizen Card software running locally on the voter's computer.

3) Provide Identity-Link

As a result, the Citizen Card sends the Identity-Link to the requesting web application (registration service) directly.

4) Verify Identity-Link and pre-fill the form

The web application verifies the electronic signature of the Identity-Link (for signature verification the web application makes use of MOA-SP[3]). If the signature on the Identity-Link can be verified successfully, the web application creates the voter's $ssPIN(v)$ and tries to find the voter in the electoral list[4]. If the voter is found, the web application retrieves all relevant personal data of the voter. The application pre-fills the web form with the personal data that was retrieved and then displays it to the voter.

5) Present pre-filled form

The web application presents the pre-filled form to the voter. The layout of the form was borrowed from existing e-Government application for requesting paper based ballot cards[5] (as seen on 23 July 2007). Figure 9.2 shows a screenshot of the registration form.

6) Fill-in data

The voter has to complete the form and send it back to the web application. The demonstration asks the voter to enter her e-mail address, even though it is an optional field. Since the goal is only to evaluate the main principle of the proposed e-voting schema, there is no need to delve further into the registration process in terms of what kind of personal information is maintained in the electronic electoral roll.

7) Submit form

After the voter has completed the form, she sends it to the web application. The web application takes the submitted form and checks the information provided by the voter with the information stored within the electronic electoral roll.

[3]MOA-SP is the standard module for server-side signature verification. MOA-SP is freely available under a certain OpenSource license for Austrian e-Government applications. Most Austrian e-Government applications are based on this module.

[4]For the sake of this prototype, a fictive electronic electoral roll was created that contained all eligible voters identified by their $ssPIN(v)$.

[5]The form layout was taken from the application for requesting ballots cards as provided by the city of Bruck an der Großglocknerstraße, https://link.help.gv.at/pilotweg/db/formallg.form?behoerde=924&verf=164

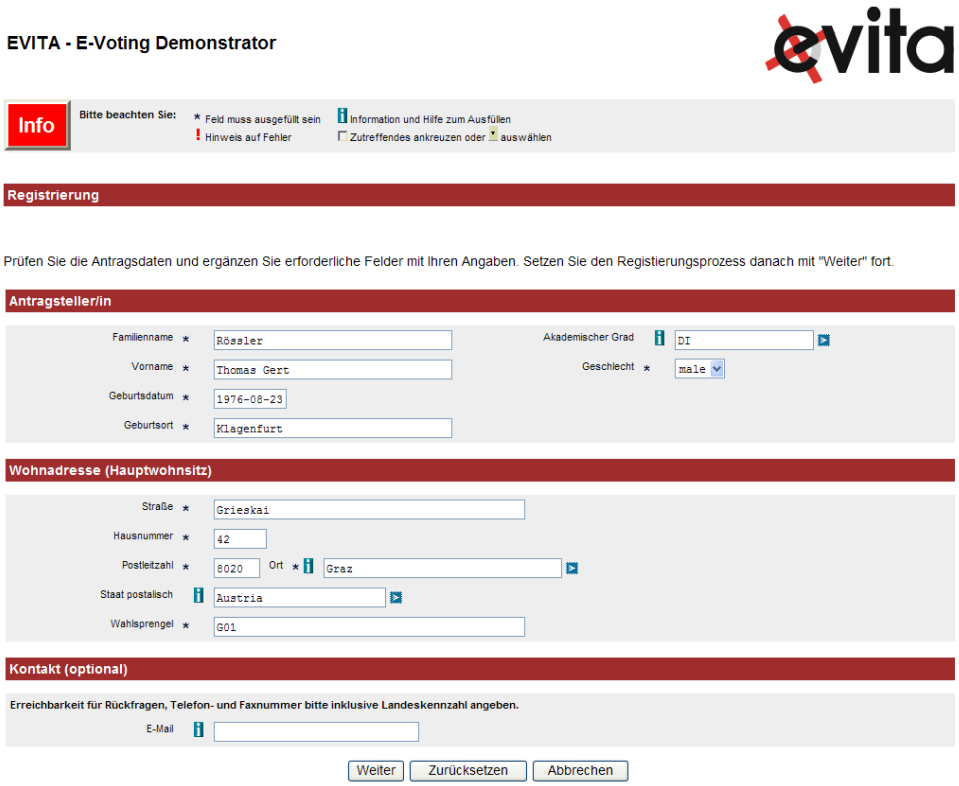

Figure 9.2: Screenshot of the registration form (pre-filled with the voter's personal information stored in the electronic electoral roll).

8) Present form to sign

The web application displays a form that the voter must sign using her Citizen Card.

9) Sign form with Citizen Card

The voter signs the form using her Citizen Card. The web application displays a web site as before that contains a hidden HTML form. The HTML form contains a *CreateSignatureRequest* for the voter's Citizen Card. Using this signature the voter confirms her personal data provided by the form and the voter explicitly agrees to vote electronically.

10) Return signed form

After the signature has been created, the Citizen Card software returns the resulting signature, i.e. the signed form, to the registration application directly.

11) Verify signature and authenticate voter

The registration application receives the signed form and verifies the signature. In order to authenticate the voter, the registration application checks whether the Identity-Link provided in step 3) matches to the

signature provided by the voter.

12) Create encrypted voting credentials and register voter

After the signature has been verified successfully and the voter is authenticated, the registration application creates the personal voting credentials for her. The voting credentials consist of the voter's blank ballot card and the ballot envelope as defined in section 8.3.5. Since the process of creating voting credentials is the most crucial step in the proposed voting schema, it has been fully implemented according to the process model (see description of the sub-process for creating voting credentials in section 8.3.5). As a result of this step, the registration application marks the voter in the electronic electoral roll as an e-voter. Then, the registration application generates a list of $vPIN$s encrypted exclusively for the Election Authority. Since this prototype is only used for demonstration, no hardware security module is used. Instead of a hardware security module, the necessary functionality is simulated using a Java class. However, for the sake of verifying the proposed concept, this shortcut is acceptable.

13) Return encrypted voting credentials

The voting credentials that were created are encrypted for the voter by applying her public key provided by her Identity-Link. This ensures that only the voter will be able to decrypt her voting credentials using her Citizen Card.

14) Store encrypted voting credentials

In the final step, the voter is asked to "download" her encrypted voting credentials and save it on her computer (or on any arbitrary data storage media). Since the voting credentials are encrypted using the voter's public encryption key, storing the credentials on her computer does not pose a security risk.

9.4 Election Phase

After completing the registration phase, the voter holds her encrypted electronic ballot. The encrypted electronic ballot becomes the input for the succeeding election phase. The implementation of the election phase covers all required steps from opening the encrypted ballot to making a decision and casting the vote. Although the Citizen Card application is used to decrypt and verify the voter's ballot and web applications are used to assert and cast the vote, an e-voting client was implemented to orchestrate all the required steps. The e-voting client is a slim client application that runs on the voter's local computer. It presents the ballot to the voter and asks her to make a decision.

The consequences and implications of such client software with regards to accessibility and interoperability—interoperability between different computer systems—are well known. However, for the sake of this prototype and for the purpose of evaluating the proposed e-voting schema, an e-voting client in form of a software component is acceptable.

Figure 9.3 shows the sequence of all steps implemented by the e-voting client prototype. All actions of the "voter"-actor are executed through the e-voting client. In order to have a seamless demonstration of the proposed e-voting schema, the voting process covers all three sub-processes of the election

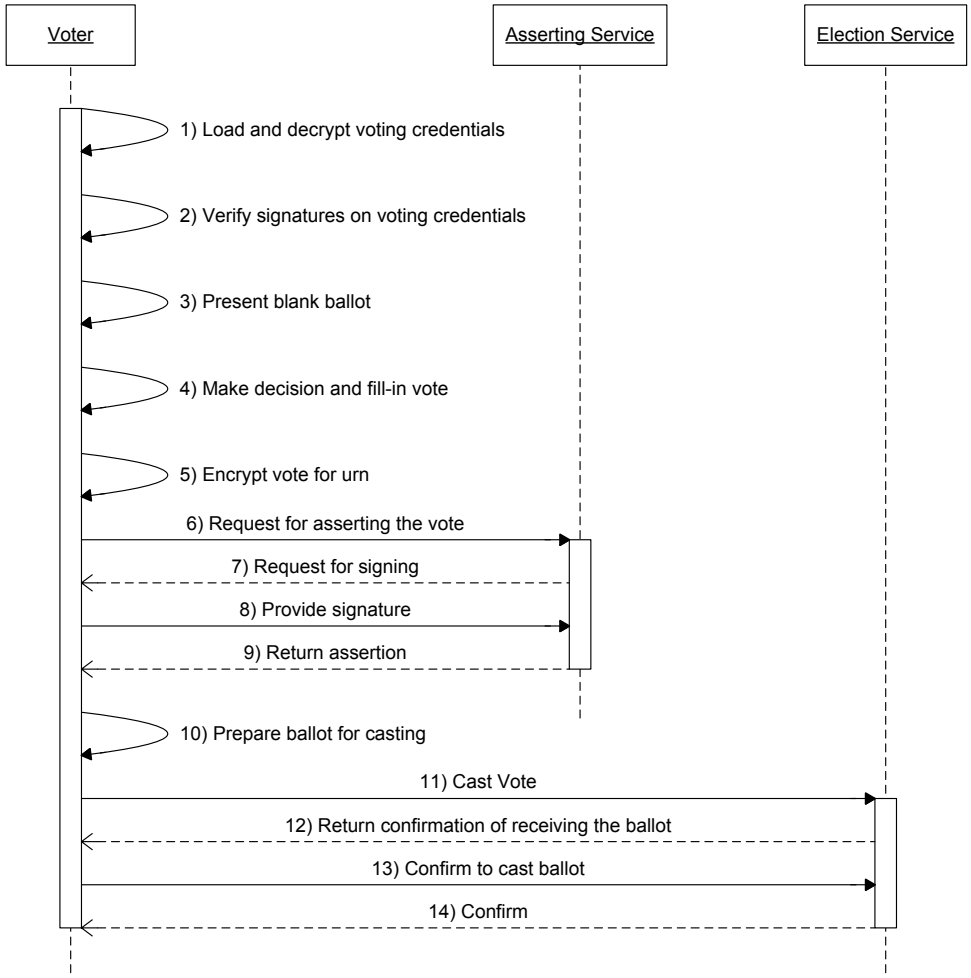

Figure 9.3: The sequence of the implemented voting procedure.

phase: filling-in the vote, asserting the vote and casting the vote. The following paragraphs describe how these sub-processes as defined in chapter 8.4 might be implemented using existing e-Government technologies.

1) Load and decrypt voting credentials

Initially, the e-voting client asks the voter to load her encrypted voting credentials. The e-voting client opens the given file and starts to load it. The client uses the voter's Citizen Card to decrypt her voting credentials by sending a decrypt-request to the Citizen Card software. As a result, the e-voting client holds the decrypted voting credentials. Figure 9.4 shows a screenshot of the voting client after loading and decrypting the voter's voting credentials (left-most image).

2) Verify signatures on voting credentials

The voting credentials consist of the voter's ballot card and the ballot envelope. As described in section 7.2.3.1, both the ballot card as well as the entire ballot package is signed by the issuing authority. Thus, the voting client verifies both signatures using the voter's Citizen Card Environment being an independent software component which might be trusted by the voter. Only if the e-voting client is able to verify both signatures successfully will the e-voting client proceed.

Figure 9.4: Left: the initial e-voting client; middle: the e-voting client asking the voter for her vote; right: the e-voting client after casting the vote.

3) Present blank ballot

The e-voting client displays the verified blank ballot card to the voter. The prototype displays the options provided on the voter's ballot card using standard graphical user interface elements such as buttons. Although sufficient for this prototype, accessibility issues for a real implementation would have to be thoroughly addressed. The middle screenshot in figure 9.4 shows how the prototype displays ballot cards.

4) Make decision and fill-in vote

The voter is asked to make a decision. The voter declares her decision simply by choosing the appropriate button. As a result, the chosen option will be marked with an "X". The e-voting client does not limit the voter in how she is allowed to express her decision. The voter is free to choose no option, one option or several options. Thus it is possible to create an invalid vote. It would even be possible to vote for a certain option by selecting all other options[6]. However, after the voter has made her decision she is asked again to review her decision and then confirm it before the e-voting client proceeds.

[6]Depending on the legal framework, such form of inverse selection could be accepted as well.

5) Encrypt vote for urn

The voter's decision is expressed by an XML fragment that represents all options chosen by the voter. After the voter has made her decision, the e-voting client immediately encrypts her decision for the electronic urn (the hardware security module of the urn).

6) Request for asserting the vote

The e-voting client contacts the web application in order to request for asserting the vote. Therefore, the e-voting client creates a digest value from the encrypted ballot ready to be cast which will then be blinded according to David Chaum's blinding schema as defined in [112]. The blinded digest value is sent to the asserting web application (asserting service). In addition to the blinded digest value, the e-voting client requests the Citizen Card software to send the voter's Identity-Link to the asserting service as well. The asserting service verifies the Identity-Link and thus identifies the voter.

7) Request for signing

In response to the Identity-Link being sent, the asserting application asks the Citizen Card software to create an electronic signature. This signature is not only used to authenticate the voter in question but also to ask her to confirm that she has been uninfluenced and unattended during voting.

8) Provide signature

The Citizen Card software creates the electronic signature by asking the voter to enter her secret code and sends the resulting signature to the asserting service.

9) Return assertion

If the provided signature could be verified successfully and the signing certificate could be matched to the key information provided in the Identity-Link, the voter is identified and authenticated. Thus, the asserting service validates the vote by signing the blinded digest value representing the voter's encrypted ballot. Furthermore, the asserting service stores the signed document confirming that the voter has been uninfluenced and unattended during voting. Finally, the asserting service returns the blindly signed digest value—the resulting blind signature—to the requesting e-voting client. Since this prototype uses David Chaum's blinding mechanism for RSA-algorithms, the Asserting Authority generates an RSA signature.

10) Prepare ballot for casting

The e-voting client receives the blind signature and unblinds it. It adds the unblinded signature to the voter's ballot. From this moment, the ballot is ready to be cast and contains the voter's encrypted decision as well as her ballot envelope and the unblinded signature value of the Asserting Authority.

11) Cast vote

The e-voting client prototype allows a vote to be cast immediately by sending it to the Election Authority. This step may be done at a later stage as well.

12) Return confirmation of receiving the ballot

The e-voting prototype implements a very simple confirmation protocol in order to ensure that the vote has been transmitted unmodified and completely. After the Election Service has received the voter's ballot, it answers with a simple confirmation request containing the digest value of the received ballot.

13) Confirm casting of ballot

The e-voting client compares the digest of the cast ballot with the digest of the sent ballot that has been created before sending. If both digest values are equal, the e-voting client sends a final confirmation message to cast the ballot.

14) Confirm

If the election service receives confirmation from the e-voting client, then the cast ballot becomes accepted. Otherwise, the ballot will be discarded. In accepted, the Election Authority sends a simple confirmation to the e-voting client confirming that the ballot has been accepted. This final asserting serves to let the voter know that her vote has been accepted, however it cannot be used as a proof in front of third parties.

9.5 Counting Phase

After all votes have been cast, the counting procedure can be started. In a real e-voting scenario, the Election Authority would start counting at a designated point in time after the voting services have been closed. After the count has been started, no further ballots would be accepted and the set of ballots to be counted must remain unchanged.

However, with respect to the e-voting prototype implemented, some limitations have been set in order to demonstrate the functionality of the whole e-voting prototype more easily. It is possible in this prototype to count at any time without stopping the election. Furthermore, although the hardware security module is an important element of the proposed EVITA e-voting concept, for the sake of demonstrating the proposed processes, this prototype does not make use of a real hardware security module.

Figure 9.5 depicts a report of the results created by the counting module of the EVITA prototype. It displays a sample selection showing details of interest in the counting result. Also a graphical interpretation of the result is provided in form of a bar chart. The bar chart illustrates the relative results for each party up for election as well as the relative amounts of invalid votes cast and voters who did not cast any vote. In addition, a table shows the number of votes cast and a list of relevant meta information, such as a fingerprint of the set of votes counted, start and end time, etc. The following paragraphs briefly outline the most important steps in the counting process. The counting process adheres to the theoretical definition of the counting process as given in section 8.5. The entire counting procedure is conducted solely by the Election Authority.

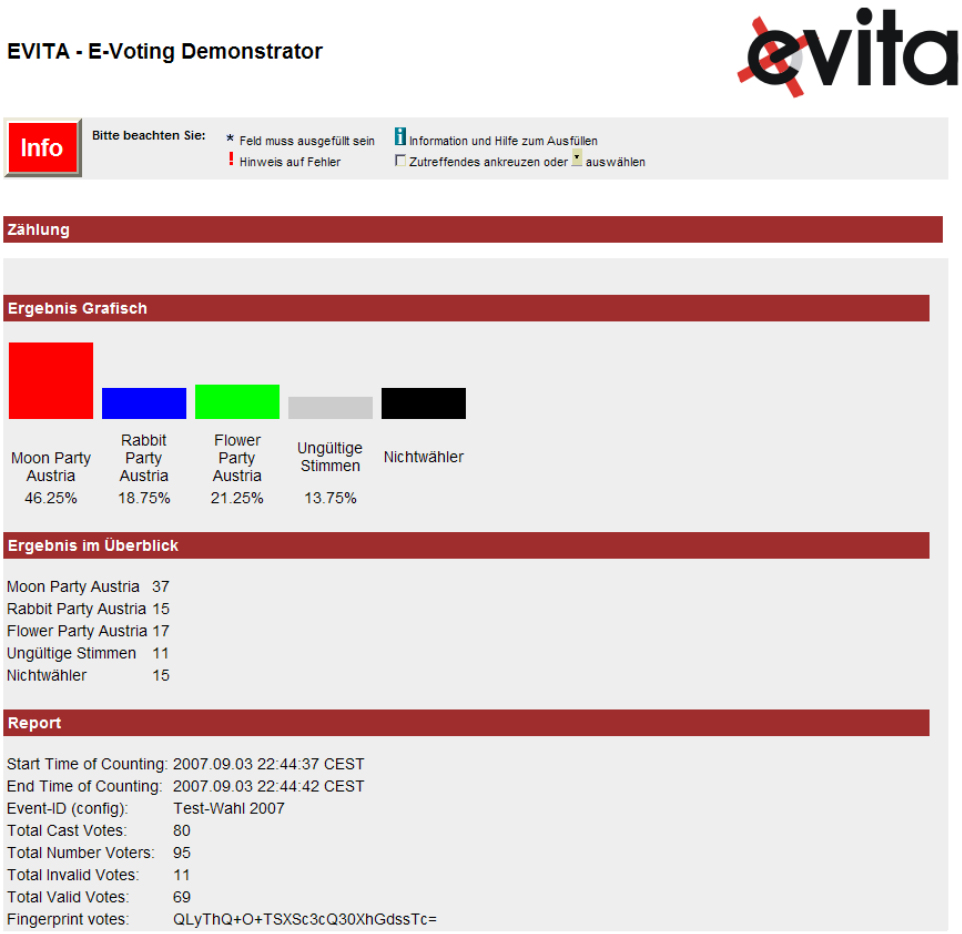

Figure 9.5: Screenshot of the counting result.

1) Load all ballots cast

The counting module loads all ballots cast from the database. It sorts the set of ballots according to $vPIN$. Since this prototype only serves one election district, no further sorting is required. During this step, multiple ballots carrying the same $vPIN$ will be detected and sorted out. Ballots carrying the same $vPIN$ are marked as invalid.

2) Verify signatures

The counting module verifies all electronic signatures provided on a cast ballot. The ballots handled in this prototype carry three signatures as defined in section 7.2.3.1 which describe the structure of a ballot and all its elements. If verification of the signatures fails, the affected ballot is sorted out and marked as invalid.

3) Separate vote from ballot card

The portion of the ballot that contains the actual vote is separated from the rest of the ballot.

4) Decrypt vote

This step decrypts the separated portion of the vote that holds the voter's decision. If the vote part cannot be decrypted for any reason, the entire ballot is sorted out and marked as invalid.

5) Count vote

If the vote passes all steps so far, it becomes a candidate for being a valid vote. The counting module retrieves the decision given in the vote. If the vote is empty, i.e. it does not contain any decision, the vote is sorted out and marked as invalid. If the vote contains the descriptor of exactly one party that is up for election, the according counter is increased and the vote is marked as valid. If the vote contains descriptors for more than one party or a descriptor for a party that is not up for election the vote is sorted out. This prototype does not accept arbitrary write-in votes or an "inverse decision"[7].

6) Generate result report

Finally, a detailed report is created. The report not only shows the number of votes cast for the parties up for election but also provides a set of meta-data. The most important meta information is the incremental HASH value that represents the set of ballots counted. This fingerprint represents the exact set and order of all ballots considered in this count. The result is displayed as a web site page.

9.6 Results and Experiences

The implementation of the prototype yielded much experience in terms of lessons learned. It even highlighted a weakness in the concept which could be quickly eliminated. In the end, the prototype demonstrates that existing e-Government technologies and components are ready to be used for the proposed e-voting scenario and that they behave as expected.

In a real implementation of the proposed e-voting schema, many additional aspects that were not covered by the prototype would have to be addressed. The most important of these would be an all-embracing risk management scenario, redundancy and backup measurements, and emergency procedures. Furthermore, if e-voting client software is required within a real scenario, this client software has to be thoroughly tested and must be compatible with a variety of operating systems and platforms. Usability and accessibility also have to be considered.

To summarize, the prototype was intended to be a vehicle for evaluating the core elements of the proposed e-voting schema. The prototype perfectly served this purpose. Moreover, it yielded valuable lessons learned especially with respect to the applicability of the proposed e-voting concept from a practical point of view. Therefore it can be concluded that the proposed schema is very feasible and suits the defined requirements, namely that the proposed e-voting schema can be built on top of today's Austrian e-Government framework.

[7] In the event of an "inverse decision" the voter would mark all options except the one she aims to elect.

Chapter 10

Analysis, Summary and Conclusions

This chapter provides a rudimentary analysis of the EVITA e-voting concept introduced by this thesis. The next section compares the requirements defined in section 5.4 with the e-voting concept introduced. Furthermore, this chapter summarises the findings and conclusions presented in this thesis.

10.1 Security Objectives Achieved

Section 5.4 presents a resulting set of requirements compiled from requirements and election fundamentals discussed in chapter 5. The compiled requirements—the overall security objectives—are taken as the basic requirements for the introduced EVITA e-voting concept. Thus, the presented concept should address the security objectives raised.

All the underlying fundamentals are the same as the election principles as given by the Venice Commission in [11]. Although these fundamentals are very abstract, they address the most important issues of democratic elections. Based on these fundamentals and under consideration of additional security requirements and objectives, a generic set of security objectives has been created. With respect to the EVITA e-voting concept, the fundamentals of this concept are laid down by the requirements given in chapter 7. In the course of the description of the core elements of the EVITA concept, the main statements are expressed as technical requirements for the e-voting concept introduced. In respect to the following comparison between security objectives and the proposed EVITA e-voting concept, all requirements have been numbered. Therefore, figure 10.1 gives a comparison between the security objectives compiled in 5 and the requirements of the EVITA e-voting concept defined throughout chapter 7.

The bottom row of the diagram in figure 10.1 gives the resulting security objectives sorted according to the voting phases—the pre-voting phase, the voting phase and the post-voting phase respectively. The right-most column of this diagram lists the requirements of the EVITA voting concept. An 'X' indicates that the security objective represented by the according column is addressed by the concept requirement represented through the corresponding row.

Most of the security objectives are not addressed by any of the concept's basic requirements. On closer examination, this is not surprising since the basic requirements of the EVITA concept focus on protecting election secrecy. The remaining security objectives that are not yet addressed by the core elements of this e-voting concept have to be addressed either by the elements surrounding this e-voting concept or

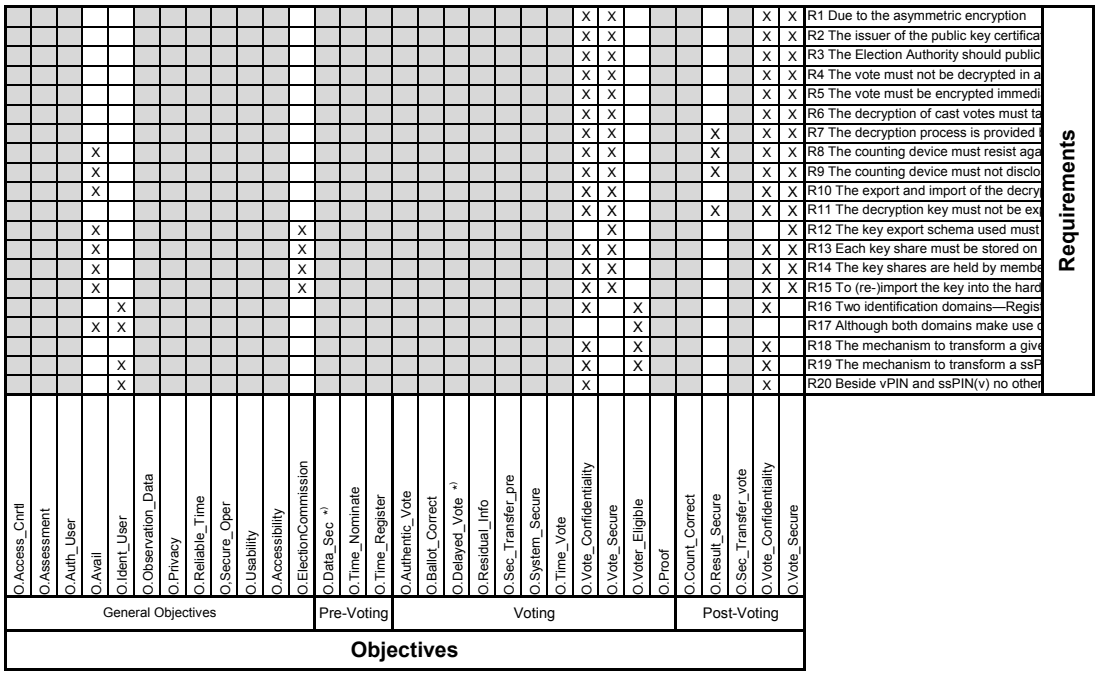

Figure 10.1: Comparison between the security objectives compiled in 5 and the requirements of the EVITA e-voting concept defined throughout chapter 7.

by the implementation of this e-voting concept itself. Therefore, considering the basic requirements of the EVITA concept alone is not sufficient. Instead, the comparison between the security objectives and the activities of the processes of the EVITA voting concept should be more informative. Figure 10.2 shows the comparison between the security objectives and the activities of the EVITA e-voting processes defined throughout chapter 8. An 'X' indicates that the security objective represented by the corresponding column is addressed by the activity represented through the according row. Furthermore, an '!' indicates that the affected activity should especially take the according security objective into consideration.

In contrast to the comparison given before, the activities cover more security objectives although not all of them. The EVITA processes introduced deal with conceptual elements only. They describe core elements of the proposed e-voting concept from a process-oriented point of view. In contrast, the security objectives are more comprehensive and thus affect implementation and operational issues as well. On the contrary, the process description does not comprehensively cover implementation and operational aspects unless they are crucial with respect to the core principle of the EVITA concept. With this in mind, it can be expected that the core activities of the EVITA process model do not fully cover of all security objectives. Moreover, the security objectives which are not covered by the core principles and activities of the proposed e-voting concept have to be addressed through the implementation of the e-voting system and its operational environment. The latter includes not only technical but also non-technical measures, such as legal and organisational provisions. In other words, the remaining security objectives uncovered so far are objectives and requirements for the final implementation of the e-voting schema.

Seen from this angel, the remaining objectives are:

1. General Objectives:
   ... O.Assessment, O.Avail, O.Reliable_Time, O.Secure_Oper, O.Usability, O.Accessibility

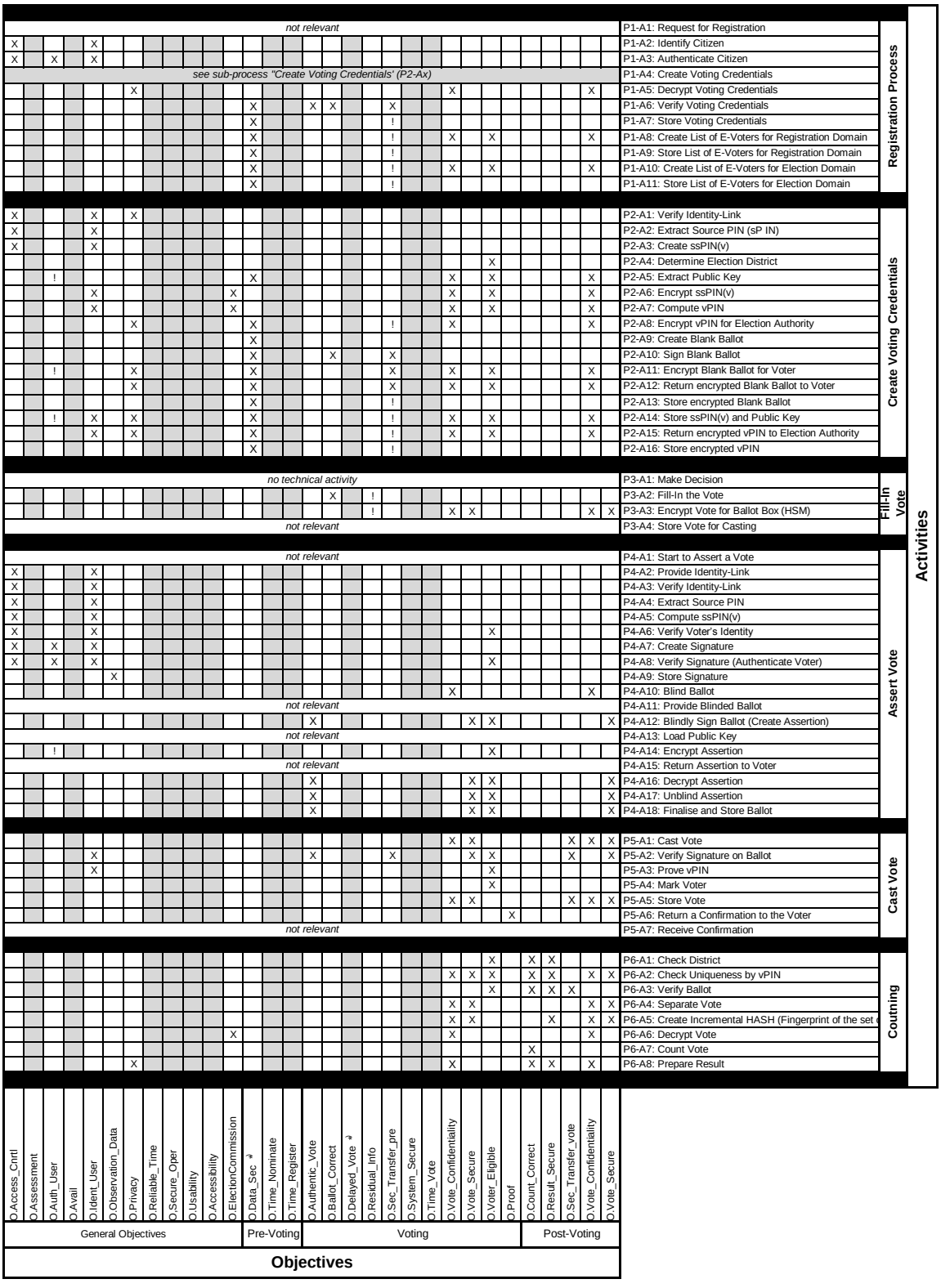

Figure 10.2: Comparison between the security objectives compiled in 5 and the activities of the EVITA e-voting processes defined throughout chapter 8.

2. Pre-voting Objectives:
   ... O.Time_Nominate, O.Time_Register

3. Voting Objectives:
   ... O.Delayed_Vote, O.System_Secure, O.Time_Vote

The objectives O.Reliable_Time, O.Time_Nominate, O.Time_Register and O.Time_Vote generally require being able to accurately determine the time certain actions take place. This is important in order to decide about the legal acceptance of an action, e.g. in order to decide whether to accept a cast vote or a candidate nomination. These aspects are important, although they do not touch the core elements of the proposed EVITA voting concept. It is a requirement for implementation to provide an accurate timestamp, as required by O.Reliable_Time, and to accurately and verifiably record the time a crucial actions was taken. An additional time issue is objective O.Delayed_Vote. This objective requires taking delays into consideration in the passing of votes over the communication channel at the end of the cast-vote period. This objective closely relates to the other time-related objectives and leads to specific operational regulations that define how long to keep accepting cast votes.

The same applies to the general objectives O.Assessment, O.Avail, O.Usability, O.Accessibility, O.Secure_Oper and O.System_Secure. Any implementation has to consider them. The objectives O.System_Secure, O.Secure_Oper and O.Assessment in particular address implementation of a maximum amount of security, which has to be confirmed by a comprehensive assessment. Furthermore, O.Usability as well as O.Accessibility are requirements that aim not only to simplify use but also to raise the acceptance of the e-voting system. Good usability might reduce invalid or erroneous votes due to operating errors as well. Both objectives have to be covered by the implementation and its user interfaces; the basic principles of the voting schema does not address these objectives directly as long as the schema does not require activities from the voter that are deemed to be infeasible.

To summarize, the remaining objectives are requirements for the implementation and the operation of the EVITA voting concept. Following a shell model, the core elements of the e-voting concept covers a few core objectives only. Going one step deeper, the main elements of the EVITA processes address more security objectives since the processes consider additional issues of the e-voting workflow as well. In the end, a few objectives remain that are taken care of in the next shell, i.e. the implementation. The prototype of the EVITA voting concept rudimentarily demonstrates how this can be done with respect to a few details. For example, the web interface provided by the registration application adheres to the style guide for Austrian E-Government web forms. This style guide explicitly requires developers of web applications to provide web interfaces that are compliant with accessibility guidelines. However, on the one hand, different implementations require different approaches to cover certain security objectives depending on the technology used. On the other hand, additional local requirements might emphasize the requirements given by security objectives, leaving a margin of interpretation in the implementation. The concept can only emphasize and expand on the minimum requirements represented by the security objectives.

This follows the perception asserted throughout this thesis: secure e-voting, and secure e-voting over the Internet in particular, can only be achieved by a comprehensive and all-embracing security concept that addresses technical, organisational and legal aspects. With regards to technical aspects, these can be further divided into conceptual, implementational and operational issues. Only when all layers and aspects of an e-voting system are taken into consideration will the e-voting solution be deemed suitable for elections on a large scale. The security considerations covered in this thesis should serve as a mini-

mum basis only and should rather highlight the methodology used. Thus, the security objectives given in this thesis represent a minimum set of requirements which have to be further elaborated on according to the specific needs of a real election scenario. Furthermore, the comparison between the security objectives and the proposed e-voting concept emphasises the need for further security considerations in the course of implementation and operation. Although there may be a secure e-voting schema as a basis for the solution, further security considerations still need to be implemented on the remaining levels. This conclusion can be applied to all e-voting approaches in general.

10.2 Summary

This thesis described e-voting as being a supreme discipline of e-Government. It tackled the question, whether existing e-Government technologies and approaches are sufficient to serve e-voting requirements, and if so, discussed what an e-voting solution might look like. To be more precise, the question was to develop an e-voting concept using the Internet as the voting channel that is based on Austrian e-Government elements. Like any other e-Government application, e-voting requires a comprehensive handling of all legal, organisational and technical aspects respectively. Therefore, this thesis treated e-voting at different abstraction layers.

Firstly, this thesis analysed and discussed requirements of elections from a legal perspective. It investigated the meaning of elections in general by researching international standards and legal fundamentals. The legal fundamentals discussed pointed to fundamental characteristics of elections from a very abstract point of view. The discussion led to a number of election fundamentals that are internationally accepted as being the base for democratic decision making. It came to the conclusion that remote voting, and remote e-voting especially, does not contravene existing election fundamentals. Moreover, international election fundamentals explicitly name e-voting as an acceptable alternative form of voting.

Since the resulting e-voting concept is aimed at being used in a major Austrian election, the outcome of the legal analysis at an international level has been compared with the legal background in Austria. The thesis summarised the legal background of major elections and highlighted the turbulent history of remote voting in Austria. It discussed the possibility of introducing e-voting in Austria and emphasised the advantages expected to come from the introduction of e-voting and remote voting in general. The discussion came to the conclusion that there is no valid reason to ban remote voting, and e-voting in particular, especially considering how the practice works in other democratic countries. Although e-voting is not yet allowed for major Austrian elections, the thesis covered two types of elections for which Austrian law explicitly allows e-voting technologies to be used. Thus, election for the Austrian National Union of Students was taken as the target scenario for the e-voting system introduced by this thesis. The legal requirements of this type of election were elaborated on in-depth.

After discussing the legal background, the thesis surveyed existing e-voting approaches and schemes from a scientific point of view. Two ways of categorising e-voting systems were covered. The thesis proposed categorising e-voting approaches according to their underlying e-voting schema, i.e. schemes based on homomorphic encryption, schemes based on mixing nets, and schemes based on blind signatures. It also proposed categorising e-voting systems according to their number of phases. In additionally to the academic snapshot of existing e-voting solutions, a selection of notable e-voting solutions was provided. As the scope of this thesis was targeted at creating an e-voting solution that would be suitable for major Austrian elections, the selection of notable e-voting solutions included e-voting solutions that have

been already used by countries in real elections. The thesis discussed two e-voting projects in detail; the Estonian e-voting solution and the e-voting system of the University of Economics Vienna. The former was chosen for two reasons. Firstly, it is one of the few Internet-based e-voting systems which have been used in real nationwide elections. Secondly, some of the elements of the Estonian e-voting concept are comparable with the e-voting concept introduced by this thesis. The latter example was chosen as it claims to be a suitable solution for major Austrian elections, thus, a closer investigation was necessary.

Discussing existing e-voting approaches and solutions led to the compilation of an intial set of requirements for the e-voting concept to be developed. Based on this and the results of the legal and general discussions held at the beginning of this thesis, a generic and reusable set of requirements for the e-voting scenario was created. The thesis proposed to adhere to existing methodologies not only for formulating the requirements but also for assessing their compliance with them. The thesis recommended conforming to the methodologies provided by the Common Criteria schema, and thus the requirements formulated in this theses adhere to the style of a Common Criteria protection profile. At this point, the thesis summarised the achievements and the outcome of the legal, technical and academic considerations covered before. It came to the conclusion that any e-voting solution that aims to be used in major elections on a large scale must be an all-embracing solution addressing not only technical issues, but legal and organisational issues as well. Thus, this work identified an urgent need to analyse the requirements for a specific e-voting scenario in a comprehensive way.

The requirements for the e-voting solution introduced by this thesis have been formulated according to the Common Criteria methodology based on related work, e.g. considering the recommendations of the Council of Europe, the protection profile for e-voting systems of the German BSI, etc., including the legal requirements retrieved from the legal discussion. As a result, a rudimentary but comprehensive catalogue of security objectives for e-voting systems intended to be used in major Austrian elections was presented. However, the security objectives presented serve as a basis only and have to be further developed according to the needs of a concrete election event. Following the conclusion requiring an all-embracing approach, it has been stated that only when all these aspects are taken into consideration can a suitable e-voting solution be achieved. This is especially applicable to e-voting solutions using the Internet since the risks and threats of the Internet cannot be completely eliminated by technical means.

Since the e-voting solution is based on the Austrian e-Government framework, this thesis introduced and summarised the most relevant Austrian e-Government elements. First of all, the Austrian identity management approach was explained. The separation of identities within e-governmental applications influenced the way in which identities are treated in the proposed e-voting concept. Furthermore, the thesis described the Austrian Citizen Card concept and its technical implementations. The Citizen Card is the citizen's security element that is kept in her possession and it serves as the voter's core element with respect to the e-voting system described in this thesis. Finally, to round up the e-Government chapter, other notable e-Government functions were envisaged in order to demonstrate the complexity of the Austrian E-Government framework.

The core elements of the proposed e-voting schema EVITA were developed based on the security objectives proposed and building on the e-Government elements introduced. The thesis described the basic principles of the proposed e-voting schema: strong end-to-end encryption and a stringent separation of identity domains. The former principle guarantees that a cast vote remains encrypted except for the single moment of counting. As discussed in this thesis, strong encryption might be an adequate method for protecting cast votes today, but protection by strong encryption has an expiration date. Therefore, the EVITA voting concept makes use of an additional stringent domain separation concept with respect to

identities. By introducing two different identity domains, the proposed EVITA e-voting schema provides unique identification of voters during the registration procedure and repetitive identification of the voter by their cast vote. This concept was developed in order to prevent double votes and to enable e-voters to vote at a conventional polling station on election day as well. The latter reason is a very important characteristic of the EVITA e-voting schema. By enabling e-voters to cast their vote conventionally as well, the proposed e-voting solution is able to handle a series of threats inherent to Internet-based e-voting system that are not addressable by technical measures only. As this thesis pointed out, in the event of a break down of central elements of the e-voting system or a partial break down of the Internet (e.g. in consequence of a successful denial-of-service attack) the e-voter is still able to cast her vote conventionally. To do so, there must be a way to determine whether or not the voter in question has already cast her vote electronically. Thus, the thesis introduced an identification model separated into two domains which securely solves this problem. The example of handling difficulties of the Internet using a combination of technical and organisational measures adheres to the all-embracing methodology proposed in this thesis.

Based on the introduction of the core elements of the EVITA schema, the thesis further worked out the underlying processes of the e-voting schema. Thus the thesis approached a deeper level of abstraction. The thesis described the proposed registration, election, and counting processes in detail. In the course of these descriptions, technical as well as organisational requirements were defined and—if required—refined. The process description should serve as a basis for any implementation following the EVITA e-voting schema. The thesis further pointed out that the proposed processes of the EVITA concept are intended as a recommendation and that variations may exist. For example, it has been emphasised that the authorities introduced by the processes might be varied. In particular, the role of the proposed Asserting Authority might be moved to the Registration Authority. Furthermore, it would also be conceivable to lessen the link between both identity domains. However, the thesis strongly recommends following the defined processes; variations have to be carefully discussed with regards to the background of the security objectives formulated.

In addition to the theoretical definition of the EVITA concept, the core parts of it were implemented in form of a prototype. The thesis described the implemented elements of the concept as well as the lessons learned.

Finally, the thesis gave a short comparison between the security objectives postulated and the e-voting concept developed. It pointed out that the most of the security objectives are covered by the technical and organisational measures defined by the e-voting concept. However, a few security objectives still remain to be addressed. As the discussion further pointed out that by nature the e-voting concept cannot address all objectives; the objectives that remain unaddressed have to be seen as requirements for both the implementation of the proposed EVITA e-voting concept and the operation of the system. This conclusion leads back to the all-embracing methodology: a secure e-voting solution has to consider all aspects—technical, organisational and legal aspects in particular—in all of its facets—conceptional, implementational and operational.

10.3 Conclusions

The work presented by this thesis aimed to develop an Internet e-voting concept based on existing Austrian E-Government technologies by following an embracing security concept. The e-voting concept

should further be suitable for use in major elections on a large scale, capable of handling millions of voters. During the work, this question was addressed on several levels step by step.

First of all, the analysis of the legal background bore the conclusion that remote e-voting in general does not stand in contradiction to established election fundamentals from a legal perspective. On the contrary, the legal considerations yield a set of election fundamentals which have to be addressed by any election model, and by an e-voting system in particular. Taking the fundamentals from legislation—from Austrian legislation as well as from international legal basis agreements—the base requirements for e-voting concepts that suit the specific needs of Austrian elections was set out.

The comparison of the base requirements given by law and the aimed e-voting solution—under consideration of the results from investigating existing e-voting concepts and systems—emphasises the conclusion that e-voting solutions can only be compliant with the existing election fundamentals if they satisfy comprehensive and all-embracing security considerations. Therefore, a base catalogue of abstract but all-embracing security objectives was developed in this work. Although this catalogue was specifically directed towards Austrian elections, it was kept universal in order to be reusable as a basis for other types of elections. This work further proposes applying a methodology, e.g. the Common Criteria methodology, when creating an all-embracing security concept for e-voting systems; all-embracing not only with respect to the different aspects of an e-voting system but also with respect to the different abstraction layers of an e-voting system.

Based on the basic security objectives compiled, a concrete e-voting concept was developed. The proposed e-voting solution EVITA relies on two core principles: strong end-to-end encryption and stringent domain separation. Both principles are closely coupled to Austrian e-Government solutions. The latter principle especially is an extension of the Austrian identity management concept. Due to the domain separation concept introduced in this thesis, the e-voting concept is able to handle unique identification of voters while protecting the anonymity of cast votes with the simultaneous possibility of gaining knowledge about whether a given voter had cast a vote already (during the election event). Thus, the proposed e-voting scenario allows voters to cast their vote conventionally at a polling station on election day even though the voter might have registered for e-voting. Allowing e-voters to cast their vote at the polling station as well—under extenuating circumstances—is a result of following an all-embracing security concept as claimed before. The use of the Internet inherently brings with it some risks that cannot be addressed by technical measures alone, however they can be tackled by having a comprehensive technical, organisational, and legal security concept.

To summarize, it was concluded that due to the nature of the technologies used and the sophisticated fundamentals and requirements of elections, an exhaustive and all-embracing security concept that follows an established methodology must exist. An initial set of security objectives suited to the needs of Austrian elections was compiled as a base. The Austrian e-Government framework—the Austrian identity management and the Austrian Citizen Card especially—serves as a perfect basis for introducing remote e-voting over the Internet. The e-voting concept developed during this work has been built entirely on top of this framework. Moreover, some e-government processes were refined even further in the process.

Appendix A

Security Objectives

For the ease of reading, this appendix holds a copy of the security objectives defined in the explanatory memorandum of [4]:

General objectives:

O.Access_Cntrl *Access control*

The E-Voting system shall restrict access to its services, depending on the user identity or the user role, to those services explicitly assigned to this user or role. User authentication shall be effective before any action can be carried out.

O.Assessment *Independent assessment*

Election authorities have overall responsibility for compliance with these security requirements which shall be assessed by independent bodies.

Application note: In case evaluated and certified CC / ISO 15408 Protection Profiles are developed based on this security recommendations, independent assessment is given under the CC scheme.

O.Auth_User *User authentication*

The E-Voting system shall protect authentication data so that unauthorized entities can not misuse, intercept, modify, or otherwise gain knowledge of authentication data or part of it. In uncontrolled environments, authentication based on cryptographic mechanisms is advisable.

Application note: The objective refers to all subjects. Services such as information services for the voter prior to entering the voting process, which (clearly do not need authentication) are outside the scope of this document.

O.Avail *Availability of the e-election processes*

Technical and organisational measures shall be taken to ensure that no data will be permanently lost in the event of a breakdown or a fault affecting the E-Voting system. The E-Voting system shall contain measures to preserve the availability of its services during the E-Voting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.

Application note: Service level agreements (SLAs) usually lay down availability and failure rates. A certain level of service degradation may be acceptable during failure periods, e.g. when a server in a

cluster breaks. In registration processes short periods of service disruptions or maintenance periods may be tolerable. The system developer however needs to consider deliberate denial of service attacks and shall document the contingency reserve in system performance that has been designated. Independent penetration tests can reduce the probability of successful deliberate service disruption.

Refinement: The services to be preserved in availability depend on the stage - Pre-voting,. Voting, Post-Voting. In the Pre-voting Stage, the nomination and the registration processes and its services are to be available, in the Voting Stage the voting processes and its services, and in the Post-Voting Stage the counting and reporting processes and its services. Auditing processes need to be available in all stages. The pre-defined limits for SLAs, tolerable failure rates, or service degradation may however be different for the various stages or services.

O.Ident_User *Identity-based user authentication*

Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured.

Application note: Authentication can be identity based or role-based. While identity-based authentication is advisable for voters registering or casting a vote, or candidates accepting / declining a nomination, it might be sufficient to have role-based authentication for administrators, Auditors, etc.

O.Observation_Data *Observation data*

E-Voting systems shall generate reliable and sufficiently detailed observation data so that election observation can be carried out. The time at which an event generated observation data shall be reliably determinable. The authenticity, availability and integrity of the data shall be maintained.

O.Privacy *Privacy of voters and candidates*

The E-Voting system shall maintain the privacy of individuals. Confidentiality of voters registers stored in or communicated by the E-Voting system shall be maintained.

Refinement: When stored in or communicated to uncontrolled environments, the voters registers should be sealed.

Application note: Depending on domestic practices there might be further confidentiality requirements with respect to the candidate's decision. In that case confidentiality is required.

O.Reliable_Time *Reliable time source*

The E-Voting system shall maintain reliable synchronised time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observation data, as well as for maintaining the time limits for registration, nomination, voting, or counting.

Application note: There may be different accuracy requirements for different consumers of the time source, such as different tolerances for the registration event and casting a vote. This may lead to multiple time sources or a single time source that provides the highest accuracy. The term ”time mark” has been used as an indication for marking the data. There are several means depending on the situation: Secure time stamps might be needed for critical events, whereas e.g. continuous sequence numbers or preserving the sequence may be sufficient for log entries. Note, that exact time stamps on votes may also jeopardise the confidentiality of the voter's decision.

O.Secure_Oper *Secure operation and system integrity*

The E-Voting system shall perform regular checks to ensure that its components operate in accordance

with its technical specifications and that its services are available.

Pre-Voting-Stage:

O.Data_Sec *Availability and Integrity of the election or referendum, options, lists of candidates*

The authenticity, availability and integrity of the voters registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be taken into account.

Refinement: Depending on domestic requirements, practice with respect to confidentiality/publication of candidate's decision or the voters register may differ.

Application note: Data-origin authentication can, e.g., be provided by electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may employ also conventional security measures, such as manual signatures, seals, couriers, etc.

O.Time_Nominate *Timely nomination*

The fact that candidate nomination and, if required, the decision of the candidate and/or the competent electoral authority to accept a nomination has happened within the prescribed time limits shall be ascertainable.

Application note: This can e.g. be provided by time marks or a confirmation of a trustworthy system.

O.Time_Register *Timely registration*

The fact that voter registration has happened within the prescribed time limits shall be ascertainable. Application note: This can e.g. be provided by time marks or a confirmation of a trustworthy system.

Voting-Stage:

O.Authentic_Vote *Ensure authentic vote*

The E-Voting system shall ensure that the voter's choice is correctly represented in the vote and that the sealed vote enters the electronic ballot box.

O.Ballot_Correct *Present an authentic ballot*

It shall be ensured that the E-Voting system presents an authentic ballot to the voter. In the case of remote E-Voting, the voter shall be informed about the means to verify that a connection to the official server has been established and the authentic ballot been presented.

Application note: Aspects to be considered are that counterfeit servers may be given, such as faking an official server by tampering the domain name system (DNS), using a similar domain name to that of official server, man.in.the-middle attacks, or Trojan horses at the voter's system replacing the original ballot or fading in counterfeit ballots. Electronic signatures applied to the ballot by the electoral authority allow for verifying the ballot. This must, however, not violate the confidentiality of the voter's decision. Therefore the data to prove a authentic ballot shall either not lead to uniquely identifiable ballots, or such unique data shall be removed when the voter casts the vote.

O.Delayed_Vote *Accept delayed votes*

After the end of the E-Voting period, no voters shall be allowed to gain access to the E-Voting system. However the acceptance of electronic votes into the electronic ballot box shall remain open for a sufficient

period of time to allow for any delays in the passing of messages over the E-Voting channel.

Application note: In remote voting scenarios, a higher load of the services might occur in the short period right before closing the poll. This may lead to increased load and increased delays until a cast vote enters the electronic ballot box. Votes that have been cast in time however shall be accepted. Thus, server shall not be shut down immediately with the closing time of the service, if such increased delays are to be expected.

O.Sec_Transfer_pre *Secure transfer of communicated data*

Data communicated from the pre-voting stage (e.g. voters registers and lists of candidates) shall be maintained in integrity. Data-origin authentication shall be carried out.

Refinement: Lists of candidates are required in the voting stage, if the ballot is generated in the election stage.

Refinement: The voters register may not be required if in two phase models an anonymous voting token establishes the right to vote. Note that voters registers in the polling station might be needed to prevent multiple votes being cast (electronically and on paper-ballot) or in case of a requirement that voters must vote.

Application note: Data-origin authentication can e.g. be provided by electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may employ also conventional security measures, such as manual signatures, seals, couriers, etc.

O.System_Secure *Secure Voting System*

Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that can modify the vote.

Refinement: In unattended remote voting environments, such as Internet voting, usually the voter or third parties control the environment. There are limited means by which the election or referendum system can control whether a secure environment exists. Means that allow the voters to gain confidence in the system must be provided, such as means to ensure that genuine software is used, or recommendations on how to protect the system environment.

O.Residual_Info *Destroy residual information*

Residual information holding the voter's decision or the display of the voter's choice shall be destroyed when the vote has been cast. In the case of remote E-Voting, the voter shall be provided with information on how to delete, where that is possible, from the device used to cast the vote.

Application note: Residual information may be given in the cache of Internet browsers, data swapped to disks, temporary files, etc. There are some means to, e.g., develop Internet applications in such a way that certain types of residual information can be avoided. However, the effectiveness of such measures is dependent on the voter's application and its configuration. In remote voting environments, such as Internet voting, usually the voter or third parties control the environment. There are limited means by which the e-election system can control whether a secure environment exists. Means that allow the voters to gain confidence in the system may be provided, such as means to ensure that genuine software is used, or recommendations on how to protect the system environment.

O.Time_Vote *Timely casting of a vote*

The fact that a vote has been cast within the prescribed time limits shall be ascertainable.

Application note: This can, e.g., be provided by time stamps or a confirmation of a trustworthy system. A time-stamp attached to the cast vote however may not leave data trails that can reveal the voter's decision (cf. O.Vote_Confidentiality).

O.Vote_Confidentiality ***Confidentiality of a voter***

Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum.

Note: This objective gives technical requirements. It is, however, represented in the legal standards "Reliability and Security", standard 35.

O.Vote_Secure ***Availability, Confidentiality and Integrity of cast votes***

The E-Voting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.

Note: This objective involves technical requirements. It, however, is also represented in the legal standards "Reliability and Seucurity", standard 34.

Application note: Encryption is a technology of choice to seal a vote, particularly in remote voting scenarios or when cast votes are transmitted via public channels. For voting machines in polling stations physical protection may also serve to seal a vote. The explanation for sealing (see Glossary) distinguishes between encryption and e.g. closed channels. In uncontrolled environments, the votes, as the primary asset of an e-elections and the confidentiality of the voter's choice, as being the primary concern of voters, require the highest level of security measures. Accordingly, the requirement explicitly refers to encryption when outside controlled environments.

O.Voter_Eligible ***Authentication of a voter eligible to cast a vote***

The E-Voting system shall at first ensure that a user who tries to vote is eligible to vote. The E-Voting system shall authenticate the voter and shall ensure that only the appropriate number of votes per voter is cast and stored in the electronic ballot box.

Refinement: In cases where anonymous voting tokens are used to prove that a voter is eligible to vote, authentication of the voter may not be required. However, even in such cases it is still necessary to ensure that the casting of multiple votes is prevented.

Post-Voting-Stage:

O.Count_Correct ***Correctness and reproducibility of the counting result***

The counting process shall accurately count the votes. The counting of votes shall be reproducible.

O.Result_Secure ***Availability and Integrity of ballot box and result***

The E-Voting system shall maintain the availability and integrity of the electronic ballot box and the output of the counting process as long as required.

O.Sec_Transfer_vote ***Secure transmission of communicated data***

The integrity of data communicated from the voting stage (e.g. votes, voters registers, lists of candidates) shall be maintained. Data-origin authentication shall be carried out.

Application note: Data-origin authentication can e.g. be provided by electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may also employ conventional security measures, such as manual signatures, couriers, etc. Cast votes or partially counted results are, however, the most valuable asset in an election or referendum. Thus, it is preferable to provide technical measures to protect these assets during the transmission.

O.Vote_Confidentiality *see Voting Stage*

O.Vote_Secure *see Voting Stage*

Appendix B

Processmodels

This appendix illustrates all process models described in section 8 in a higher resolution.

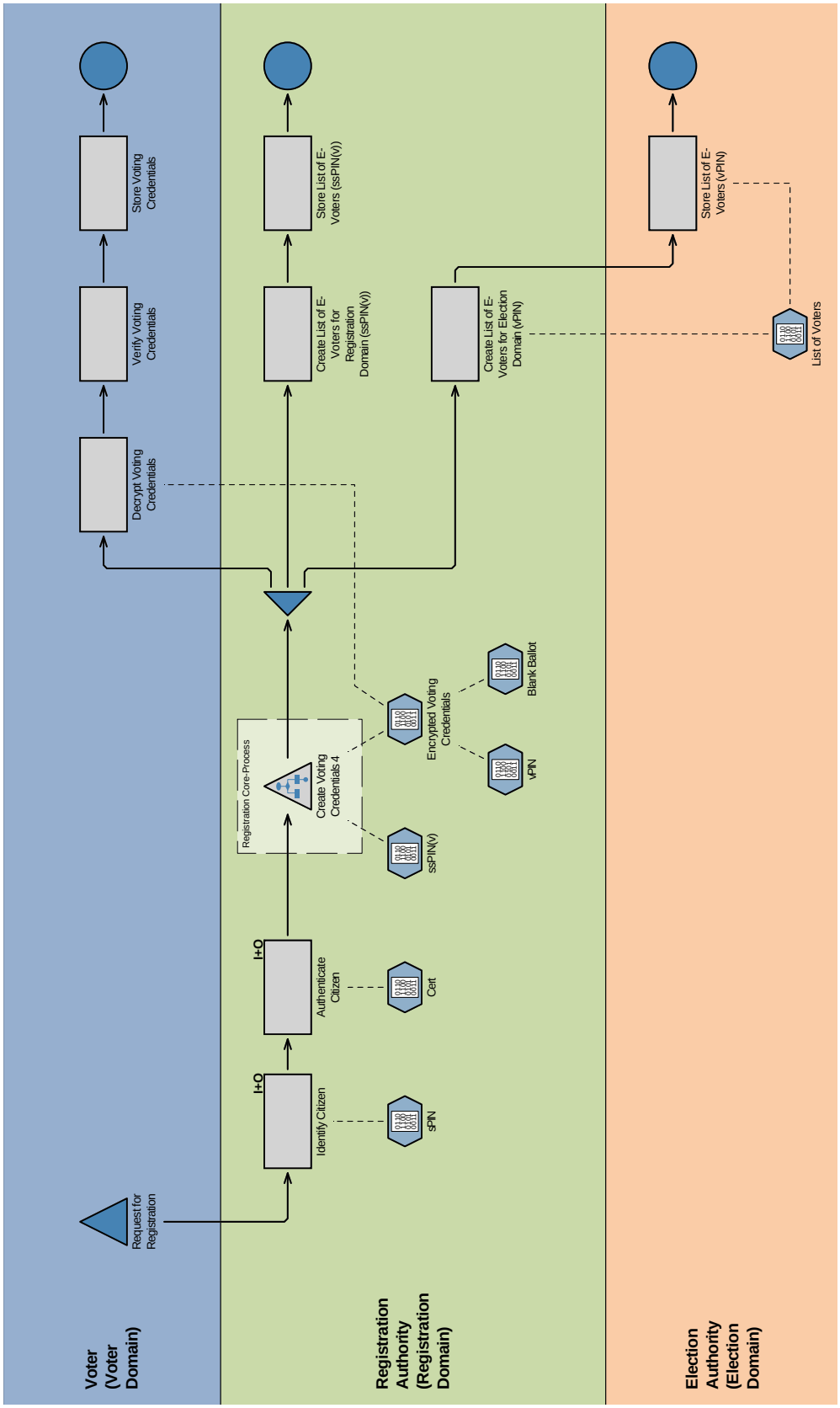

Figure B.1: Registration Process; see section 8.3

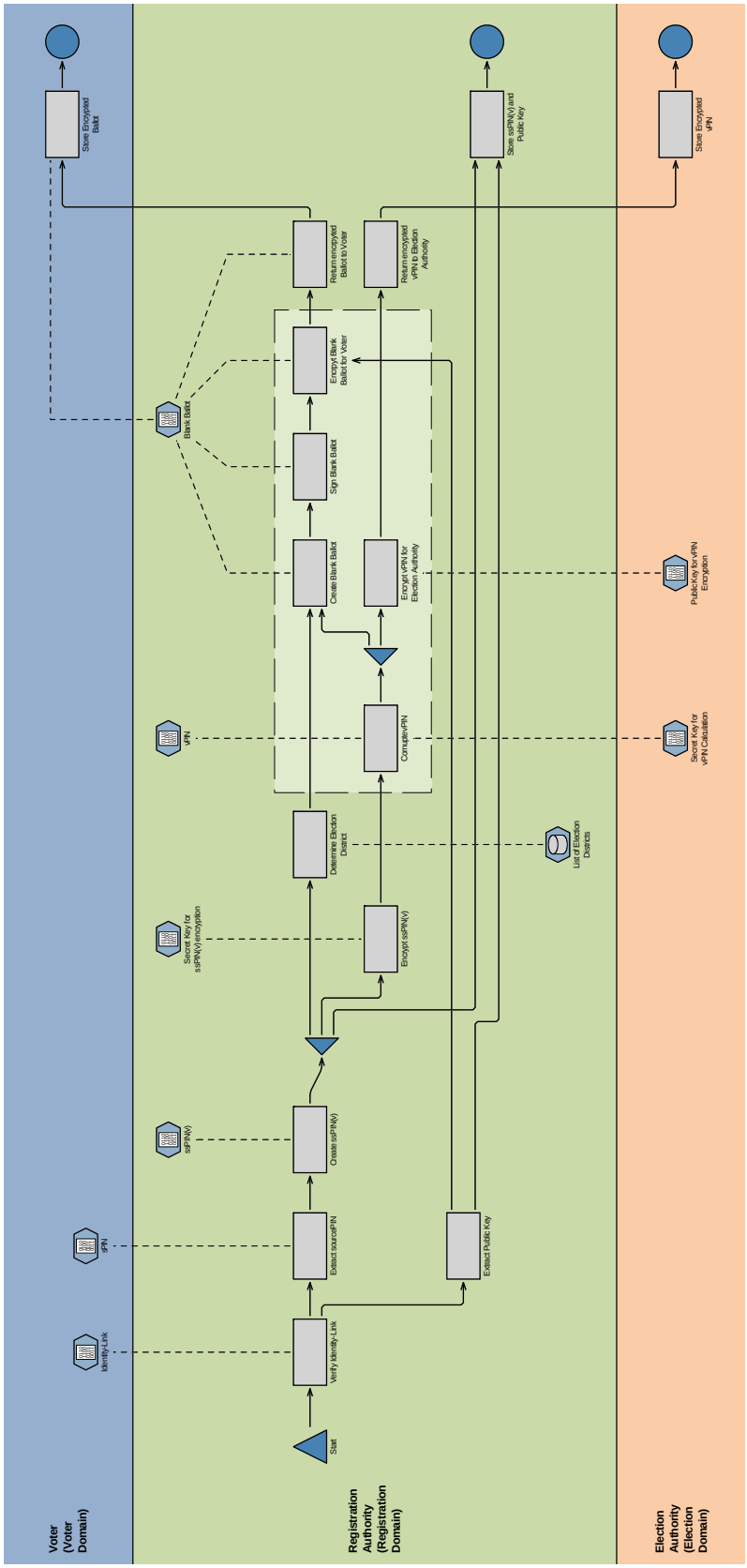

Figure B.2: Sub-Process: Create Voting Credentials; see section 8.3.5

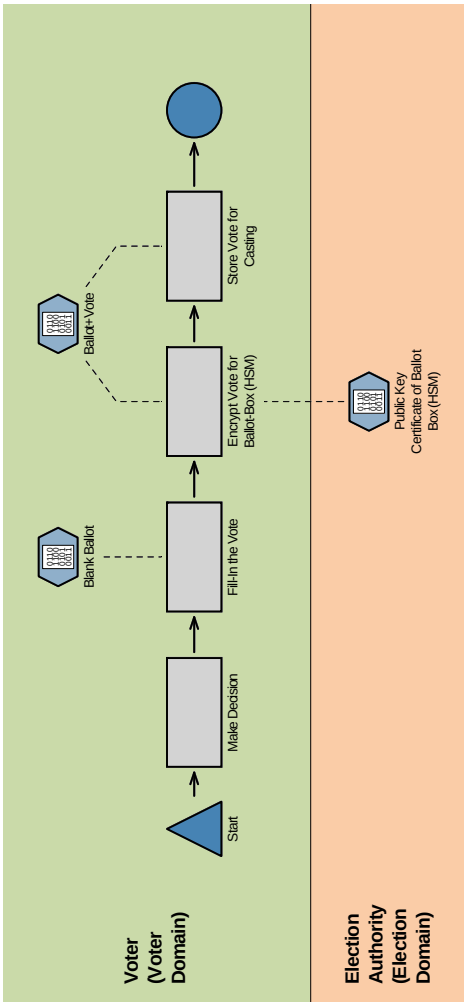

Figure B.3: Fill-In Vote Process; see section 8.4.1

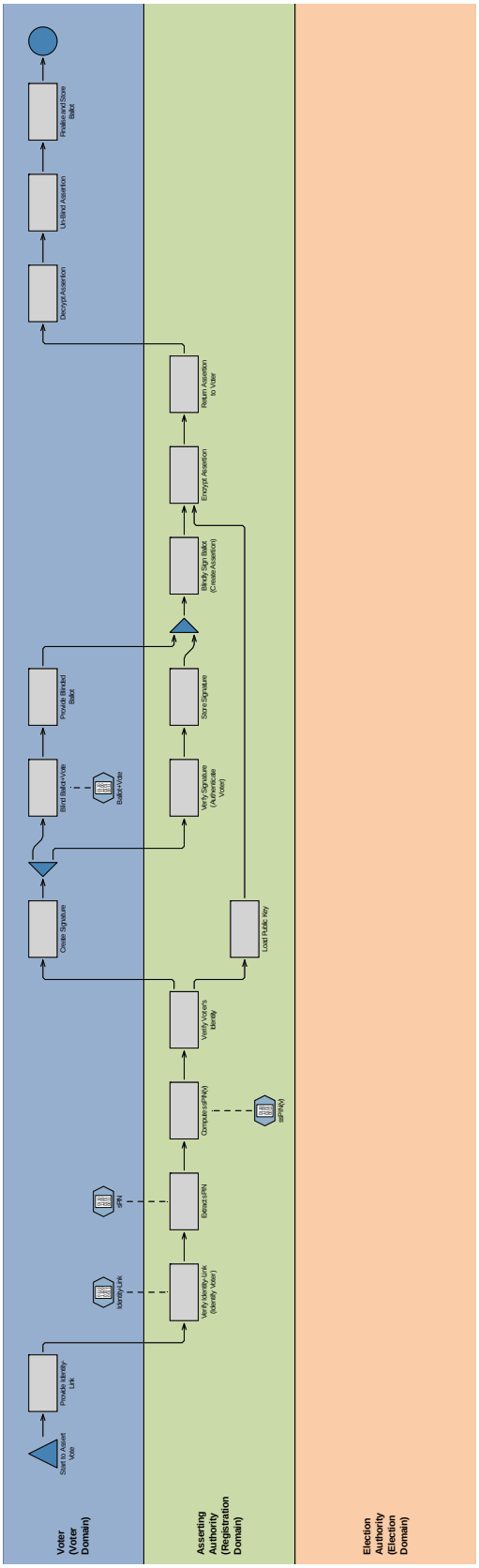

Figure B.4: Assert Vote Process; see section 8.4.2

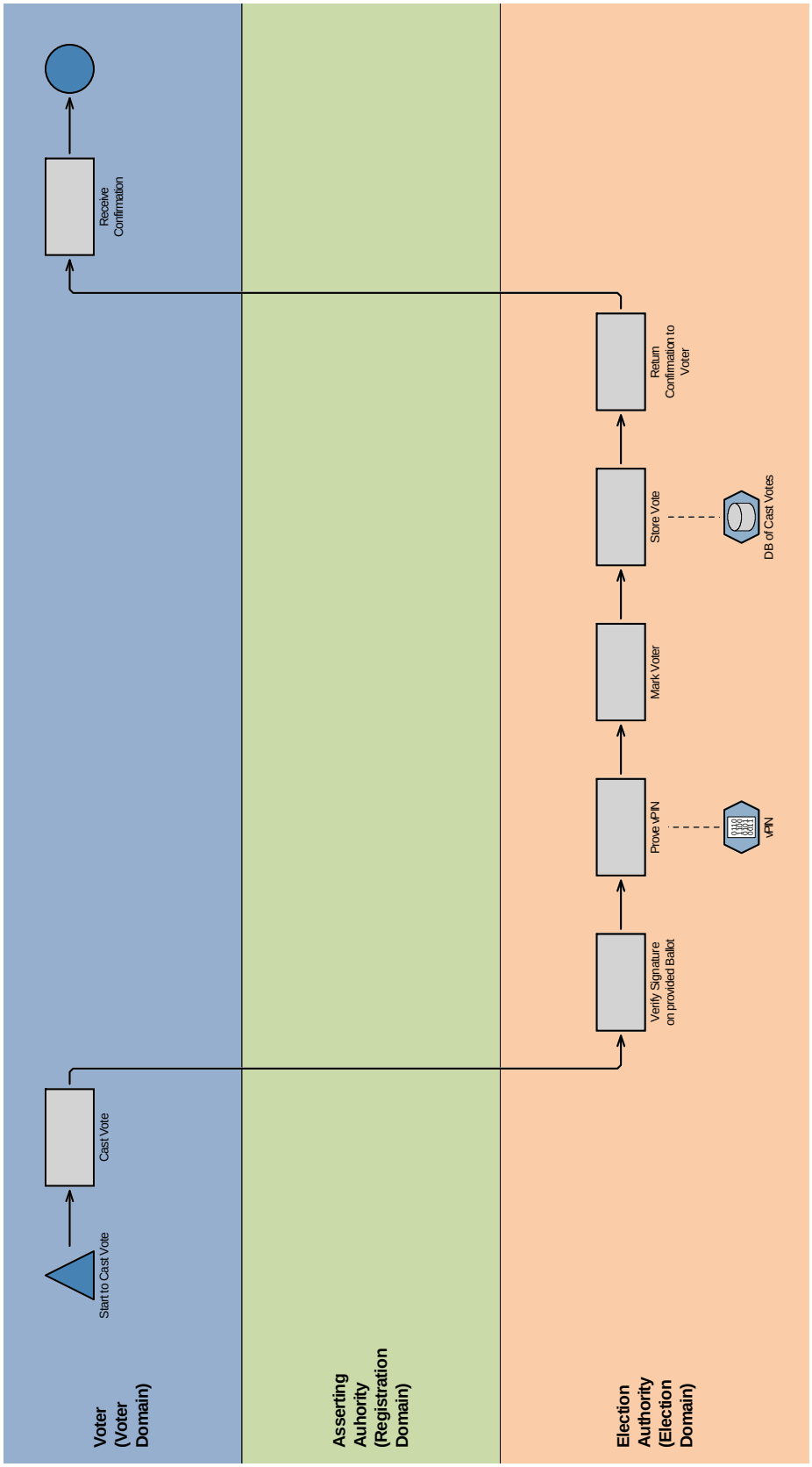

Figure B.5: Cast Vote Process; see section 8.4.3

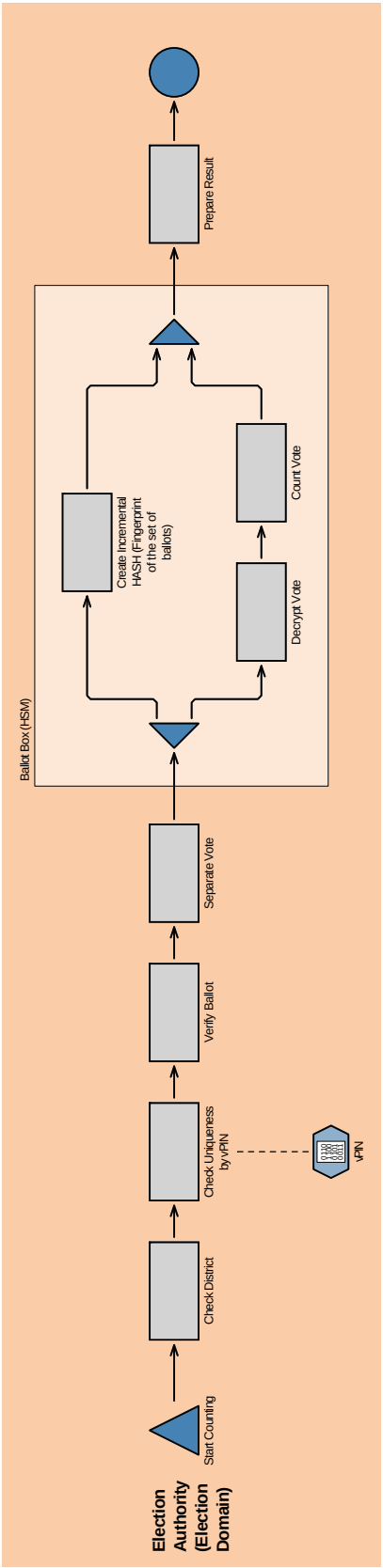

Figure B.6: Counting Process; see section 8.5

Bibliography

[1] Organization for the Advancement of Structured Information Standards (OASIS). *Election Markup Language (EML) 4.0*. http://www.oasis-open.org (as seen on 1 March 2007), January 2005.

[2] National Election Committee (Estonia). *E-Voting System - Overview*. http://www.vvk.ee/engindex.html (on 10 July 2007), 2005.

[3] Council of Europe Committee of Ministers. *Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*. Council of Europe, September 2004.

[4] Multidisciplinary Ad Hoc Group of Specialists (IP1-S-EE). *Explanatory Memorandum to the Draft Recommendation Rec(2004) of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*. Council of Europe, September 2004.

[5] Thomas Rössler. *Bürgerkartenumgebung Neu (Konzept, Modularisierung und Schnittstellen)*. Working Group Citizen Card, as presented on 14 December 2006.

[6] Thomas Rössler, Reinhard Posch, and Herbert Leitold. E-voting: A scalable approach using xml and hardware security modules. In *Proceedings of the 2005 IEEE International Converence on e-Technology, e-Commerce and e-Security (eee2005)*. IEEE, April 2005.

[7] MODINIS-Identity Management Study Team. Common terminological framework for interoperable electronic identity management for egovernment, August 2005.

[8] Council of Europe. *E-Governance-Website*. Council of Europe, http://www.coe.int/T/E/Com/Files/Themes/E-Voting/ (as seen on 29 July 2007), 2007.

[9] Council of Europe. *Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11*, March 1952.

[10] Council of Europe. *Convention for the Protection of Human Rights and Fundamental Freedoms*, November 1950.

[11] European Commission for Democracy through Law (Venice Commission). *Code of Good Practice in Electoral Matters*, October 2002.

[12] European Court of Human Rights Grand Chamber. *Judgment in the Case of Hirst v. The United Kingdom (No.2)*, June 2005.

[13] Christoph Grabenwarter. Briefwahl und E-Voting. *Journal für Rechtspolitik, Jahrgang 12, Heft 2, 2004.*, (ISSN 0943-4011):70–77, 2004.

[14] Klaus Poier. Politikwissenschaftliche Aspekte von E-Voting und Briefwahl. *Journal für Rechtspolitik, Jahrgang 12, Heft 2, 2004.*, (ISSN 0943-4011):85–95, 2004.

[15] Austrian Federal Law. *Bundes-Verfassungsgesetz (B-VG)*. BGBl. Nr. 1/1930 idgF, June 2007.

[16] Austrian Federal Law. *Bundesgesetz über die Wahl des Nationalrates (Nationalrats-Wahlordnung 1992 - NRWO)*. BGBl. Nr. 471/1992, June 2007.

[17] Austrian Federal Law. *Bundespräsidentenwahlgesetz 1971*. BGBl. Nr. 57/1971, June 2007.

[18] Austrian Federal Law. *Bundesgesetz über die Wahl der Mitglieder des Europäischen Parlaments (Europawahlordnung EuWO)*. BGBl. Nr. 471/1992, June 1992.

[19] Thomas M. Buchsbaum. Entwicklungen zu E-Voting in Europa. *Journal für Rechtspolitik, Jahrgang 12, Heft 2, 2004.*, (ISSN 0943-4011):106–118, 2004.

[20] Christopher Drexler. Briefwahl. *Journal für Rechtspolitik, Jahrgang 12, Heft 2, 2004.*, (ISSN 0943-4011):122–123, 2004.

[21] Constitutional Court of Austria. *VfGH Erkenntnis zu Nö. WahlO für Statutarstädte; Verstoß der Bestimmungen über die "Briefwahl" gegen die Verfassungsprinzipien der "geheimen" und "persönlichen" Wahl*, March 1985.

[22] Working-Group "E-Voting". *Abschlussbereicht zur Vorlage an Dr. Ernst Strasser, Bundesminister für Inneres*, November 2004.

[23] Federal Government/Federal Chancellary. Regierungsprogramm für die xxiii. gesetzgebungsperiode, January 2007.

[24] Austrian Federal Law. *Bundesgesetz über die Vertretung der Studierenden (Hochschülerinnen und Hochschülerschaftsgesetz 1998 - HSG 1998)*. BGBl. I Nr. 22/1999, BGBl. I Nr. 95/1999, BGBl. I Nr. 18/2001, BGBl. I Nr. 1/2005, BGBl. I Nr. 19/2005, BGBl. I Nr. 160/2006, BGBl. I Nr. 12/2007, June 2007.

[25] Austrian Federal Law. *Datenschutzgesetz 2000 (DSG 2000)*. BGBl. I Nr. 165/2000, June 2000.

[26] Austrian Federal Law. *Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG)*. BGBl. 1 Nr.190/1999, BGBl. 1 Nr.137/2000, BGBl. 1 Nr.32/2001, BGBl. I Nr. 164/2005, 2005.

[27] ESIGN Workshop Expert Group F. *Protection Profile - Secure Signature-Creation Device (Type1)*. http://www.commoncriteriaportal.org/public/files/ppfiles/pp0004b.pdf (as seen on 10 June 2007), July 2001.

[28] ESIGN Workshop Expert Group F. *Protection Profile - Secure Signature-Creation Device (Type2)*. http://www.commoncriteriaportal.org/public/files/ppfiles/pp0004b.pdf (as seen on 10 June 2007), July 2001.

[29] European Directive. *Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (EU Signature Directive 1999)*. European Union, Official Journal L13/12, 1999.

[30] Austrian Administrative Order. *Verordnung der Bundesministerin für Bildung, Wissenschaft und Kultur, mit der die Hochschülerinnen- und Hochschülerschaftswahlordnung 2005 - (HSWO 2005)*. BGBl. II Nr. 91/2005, June 2005.

[31] Thomas Rössler. E-voting: A survey and introduction. http://www.a-sit.at/pdfs/evoting_survey.pdf (as seen on 1 May 2007), 2004.

[32] Josh Cohen and Michael Fischer. A robust and verifiable cryptographically secure election scheme. In *Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science (FOCS)*, page 372 to 382. IEEE, 1985.

[33] Josh Benaloh. *Verifiable Secret-Ballot Elections*. PhD thesis, Yale University, New Haven, 1987.

[34] Josh Cohen and Moti Yung. Distributing the power of government to enhance the privacy of voters. In *Proceedings of 5th ACM Symposium on Principles of Distributed Computing (PODC)*, page 52 to 62. ACM, 1986.

[35] Ronald Cramer, Rosario Gennaro, and Berry Shoenmakers. A secure and optimally efficient multi-authority election scheme. In *Advances in Cryptology - Eurocrypt 97*, page 103 to 118. Springer Verlag, LNCS, 1997.

[36] David Chaum. Untraceable electronic mail, return adresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–86, 1981.

[37] Wen-Sheng Juang and Chin-Laung Lei. A collision free secret ballot protocol for computerized general elections. *Computers and Security*, 15(4):339–348, 1996.

[38] Martin Hirt and Kazue Sako. Efficient receipt-free voting based on homomorphic encryption. In *Proceedings of the Eurocrypt 2000*, 2000.

[39] David Chaum. Blind signatures for untraceable payments. In *Proceedings of Crypto 82*, page 199 to 203. Plenum Press, New York, 1983.

[40] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. A practical secret voting scheme for large scale elections. In *Advances in Cryptology - Auscrypt 92*, page 244 to 251, 1992.

[41] Kazue Sako. Electronic voting schemes allowing open objection to the tally. In *Transactions of IEICE, vol. E77-A No.1*, 1994.

[42] Tatsuaki Okamoto. Receipt free electronic voting schemes for large scale elections. In *Proceedings of Workshop on Security Protocols 97*, page 25 to 35. Springer Verlag, LNCS, 1997.

[43] Alexander Prosser and R.Müller-Török:. Electronic voting via the internet. In *Proceedings of 3rd International Conference on Enterprise Information Systems (ICEIS), Setubal, Portugal*, page 1061 to 1066, 2001.

[44] Oleg Mürk. *Electronic Voting Schemes*. Institute of Computer Science, Tartu University, June 2000.

[45] Wenbo Mao. *Modern Cryptography - Theory and Practice*. Hewlett-Packard Books, 2004.

[46] Taher Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proceedings of CRYPTO '84*, pages pages 10–18. Springer-Verlag New York, 1985.

[47] Internet Policy Institute. *Report of the National Workshop on Internet Voting: Issues and Research Agenda*. Internet Policy Institute, March 2001.

[48] The Internet Rights Forum. *What is the future of electronic voting in France?* The Internet rights forum, http://www.foruminternet.org (as seen on 1 July 2007), September 2003.

[49] Scytl Secure Electronic Voting. Pnyx.core: The key to enabling reliable electronic elections, December 2005.

[50] Nadja Braun. E-Voting in der Schweiz. In Alexander Prosser, editor, *Collection of Working Papers of the e-Democracy/e-Voting-Workshop at IRIS2003*, 2003.

[51] R.Opplinger. *Addressing the Secure Platform Problem for Remote Internet Voting in Geneva*. eSECURITY Technologies, May 2002.

[52] Schweizer Bundesblatt Nr. 5. *Bericht über den Vote électronique vom 9. Januar 2002: Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte*, Februar 2002.

[53] Michel Chevallier. *Internet voting: Situation, Perspectives and Issues*. Geneva State Chancellery, Presentation available at http://www.geneve.ch/evoting/english/telechargement.asp (as seen on 3 July 2007), April 2007.

[54] Robert Hensler. *The Geneva Internet voting system*. Geneva State Chancellor, Head of the Internet voting project, January 2003.

[55] Statistisches Amt des Kantons Zürich. *Elektronische Stimmabgabe bei Wahlen und Abstimmungen*. Unisys, August 2004.

[56] Elisabeht Prader and David Knori. So funktioniert das Zürcher E-Voting. *InfoWeek.ch*, October 2005.

[57] The Chairmen of the House of Representatives of the States General (Netherlands). *Remote Voting Project*, March 2002.

[58] Invitation to Tender (Netherlands). *Remote Electronic Voting and Voting by Telephone Experiment*, November 2002.

[59] OSCE/ODIHR. *OSCE/ODIHR Election Assessment Mission Report - PARLIAMENTARY ELECTIONS 2006*. OSCE/ODIHR, March 2007.

[60] Lawrence Pratchett. *The Implementation of electronic voting in the UK-Research Summary*. Local Government Associatione, May 2002.

[61] The Crown. *E-Voting Security Study-Issue 1.2*, July 2002.

[62] Department for Constitutional Affairs. *Electoral Modernisation Pilots Local Government Elections 3 May 2007- Details of pilot initiatives*, January 2007.

[63] Open Rights Group. *May 2007 Election Report*. Open Rights Group (ORG), June 2007.

[64] Stephan Brunessaux. *CyberVote: Lessons learned*. Presentation at http://www.eucybervote.org/reports.html (as seen on 2 July 2007), Septemer 2003.

[65] Stephan Brunessaux. *Cybervote - Final Report (D21)*, July 2003.

[66] D.Jefferson, A.D.Rubin, B.Simons, and D.Wagner. A security analysis of the secure electronic registration and voting experiment (serve), January 2004.

[67] Epp Maaten. *Towards remote e-voting: Estonian case*. Elections Department, Chancellery of the Riigikogu (Parliament), July 2004.

[68] Tarvi Martens. *Internet Voting in Practice*, March 2007.

[69] Ülle Madise. *Internet Voting in Estonia Free and Fair Elections*, October 2005.

[70] Sven Dillenseger. *e-Voting in Estland - e-Voting bei politischen Wahlen 2006 ?* Proseminar e-Voting 22.07.2005, 2005.

[71] Alexander Prosser, Robert Kofler, and Robert Krimmer. e-voting.at - Ein Implementierungsbericht. In *OCG e-Gov-Days*, February 2003.

[72] Alexander Prosser. *E-Voting Test 2006 - technischer Hintergrund*. e-voting.at, 2006.

[73] Alexander Prosser. *E-Voting Test 2006*. e-voting.at, 2006.

[74] Robert Krimmer. e-Voting.at: Elektronische Demokratie am Beispiel der österreichischen Hochschülerschaftswahlen. Working papers on Information Processing and Information Management No. 5/2002, 2002.

[75] Alexander Prosser, Robert Kofler, and Robert Krimmer. e-Voting.at - Vom e-Government zur e-Demokratie. In *Internationales Rechtsinformatik Symposion Salzburg 2002*, February 2002.

[76] Lorrie Cranor. *Electronic Voting - Computerized polls may save money, protect privacy*. ACM Crossroads Student Magazine, 1996.

[77] Lorrie Cranor and Ron Cytron. *Design and Implementation of a Practical Security-Conscious Electronic Polling System*. Department of Computer Science, Washington University, June 1996.

[78] Common Criteria for Information Technology Security Evaluation. *Part 1: Introduction and general model Version 3.1 Revision 1*. http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf (as seen on 27 August 2007), September 2006.

[79] Working-Group “E-Voting”. *Bericht der Unterarbeitsgruppe Internationales*, November 2004.

[80] Working-Group “E-Voting”. *Unterarbeitsgruppe 1 (Legistische Belange) - Endbericht*, November 2004.

[81] Working-Group “E-Voting”. *Bericht betreffend technischer Belange des E-Votings - Unterarbeitsgruppe 2 (Technik)*, November 2004.

[82] Bundesamt für Sicherheit in der Informationstechnik. *Basissatz von Sicherheitsanforderungen an Onlinewahlprodukte (Version 0.18)*, May 2007.

[83] Volker Hartmann, Nils Meißner, and Dieter Richter. *Online Voting Systems for Non-parliamentary Elections: Catalogue of Requirements*, April 2004.

[84] Gesellschaft für Informatik e.V. (GI). *GI-Anforderungen an Internetbasierte Vereinswahlen*, August 2005.

[85] Austrian Federal Law. *Federal Act on Provisions Facilitating Electronic Communications with Public Bodies (E-Government-Gesetz - E-GovG)*. BGBl. I Nr. 10/2004, 2004.

[86] Arno Hollosi and Rainer Hörbe. *Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (SZ-bPK-Algo -1.1.1)*. Platform Digital Austria, AG Bürgerkarte, http://www.ref.gv.at (as seen on 12 May 2007), January 2006.

[87] Austrian Federal Law. *Bundesgesetz über das polizeiliche Meldewesen (Meldegesetz 1991-MeldeG)*. BGBl. I Nr. 9/1992 idgF, 1992.

[88] Austrian Administrative Order. *E-Government-Bereichsabgrenzungsverordnung (E-GovBerAbgrV)*. BGBl. II Nr. 289/2004, June 2004.

[89] Donald Eastlake, Joseph Reagle, and David Solo. Xml-signature syntax and processing. W3c recommendation, W3C, February 2004.

[90] Donald Eastlake and Joseph Reagle. Xml encryption syntax and processing. W3c recommendation, W3C, December 2002.

[91] Arno Hollosi and Gregor Karlinger. *Security-Layer für das Konzept Bürgerkarte, V.1.1*. Federal Chancellery, http://www.buergerkarte.at/konzept/securitylayer, 2003.

[92] Thomas Rössler and Kurt Dietrich. MOSAIC - Mobile Creation of Signatures and Identification Credentials. In *First International Conference on M-Government, Budapest, Hungary*, October 2004.

[93] Thomas Rössler, Amir Hayat, Reinhard Posch, and Herbert Leitold. Giving an interoperable solution for incorporating foreign eids in austrian e-government. In *In Proceedings of IDABC-Conference 2005: Cross-Border e-Government Services for Administrations, Businesses and Citizens (February 17th to 18th 2005, Brussels, Belgium)*, pages page 147–156, http://ec.europa.eu/idabc/en/document/3910/5803 (as seen on 10 July 2007), March 2005. European Commission, European Commission (Enterprise and Industry Directorate-General).

[94] Herbert Leitold, Thomas Rössler, and Reinhard Posch. Identification in cross-border e-government. In *4th European Conference on e-Government (ECEG 2004), Dublin, Ireland (June 17th to 18th 2004)*, June 2004.

[95] Austrian Administrative Order. *Stammzahlenregisterverordnung - StZRegV*. BGBl. II Nr. 57/2005, June 2005.

[96] Amir Hayat and Thomas Rössler. Proposed framework for an interoperable electronic identity management system. In *Proceedings of the EGOV 2006 - International Conference on e-Government, Krakow, Poland, September 4th to 8th 2006*, September 2006.

[97] Amir Hayat, Thomas Rössler, and M. Alam. Proposed framework for achieving interoperable services between european public administrations. In *Proceedings of the ARES 2006 - International Conference on Availability, Reliability and Security, Vienna, Austria, April 20th to 22th 2006*, April 2006.

[98] Amir Hayat, Herbert Leitold, Reinhard Posch, and Thomas Rössler. Electronic identity: The concept and its implementation for e-government. In *Proceedings of the ICEG 2005, International Conference on E-Governance, Lahore, Pakistan, December 9th to 11th 2005.*, December 2005.

[99] Thomas Rössler. Das Instrument elektronische Vollmachten. In *Internationales Rechtsinformatik Symposion (IRIS) 2005, Universität Salzburg, Salzburg, February 24th to 26th*, February 2005.

[100] Thomas Rössler. Elektronische Vollmachten. In *Proceedings of the eGOV Days 2005, Vienna, Austria, March 14th to 16th*, page pages 27 to 34, March 2005.

[101] Thomas Rössler and Herbert Leitold. Identifikationsmodell der österreichischen Bürgerkarte. In *Proceedings of the D-A-CH Security Conference 2005, University of Technology Darmstadt, Germany, March 15th to 16th*, page page 121 to 129, March 2005.

[102] Thomas Rössler and Arno Hollosi. *Elektronische Vollmachten - Spezifikation 1.0.0*, May 2006.

[103] Yvo Desmedt. Threshold cryptography. In *European Trans. on Telecommunications*, page 449 to 457, August 1994.

[104] Yvo Desmedt and Yair Frankel. Threshold cryptosystems. In G. Brassard, editor, *Proceedings of Advances in Cryptology - Crypto '89, Lecture Notes in Computer Science 435*, page 307 to 315. Springer-Verlag, 1990.

[105] Yvo Desmedt. Threshold cryptosystems. In J. Seberry and Y. Zheng, editors, *Proceedings of Advances in Cryptology - Auscrypt '92, Lecture Notes in Computer Science 718*, page 3 to 14. Springer-Verlag, 1993.

[106] Thomas Rössler and Silke Palkovits. Elektronische Geschäftsprozesse in der öffentlichen Verwaltung. In *Proceedings of the conference Elektronische Geschäftsprozesse 2004 (EGP2004)*, page 386 to 395, September 2004.

[107] Silke Palkovits, Thomas Rössler, and Maria Wimmer. Process modelling - burden or relief? living process modelling within a public organisation. In *Proceedings of the 6th International Conference on Enterprise Information Systems ICEIS 2004 - Volume 3, Porto, Portugal*, page 94 to 102, April 2004.

[108] Silke Palkovits and Thomas Rössler. Prozessorganisation in der öffentlichen Verwaltung - der Mehrwert aus der Prozessmodellierung. In *eGOV Days: State-of-the-art 2004*, page 102 to 111, March 2004.

[109] Josh Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections (extended abstract). In *26th ACM Symposium on the Theory of Computing (STOC)*. ACM, 1994.

[110] Uwe Danz, Hannes Federrath, Marit Köhntopp, Huberta Kritzenberger, and Uwe Ruhl. Anonymer und unbeobachtbarer Webzugriff für die Praxis. In *IT-Sicherheit ohne Grenzen? Tagungsband 6. Deutscher IT-Sicherheitskongreß des BSI*, pages 59–70. SecuMedia-Verlag, Ingelheim, 1999.

[111] Harald Wiesner and Herbert Pacnik. *E-Government Styleguide für E-Formulare (sg-stg 2.0.0)*. E-Government Bund-Länder-Gemeinden, AG-Styleguide, September 2006.

[112] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.