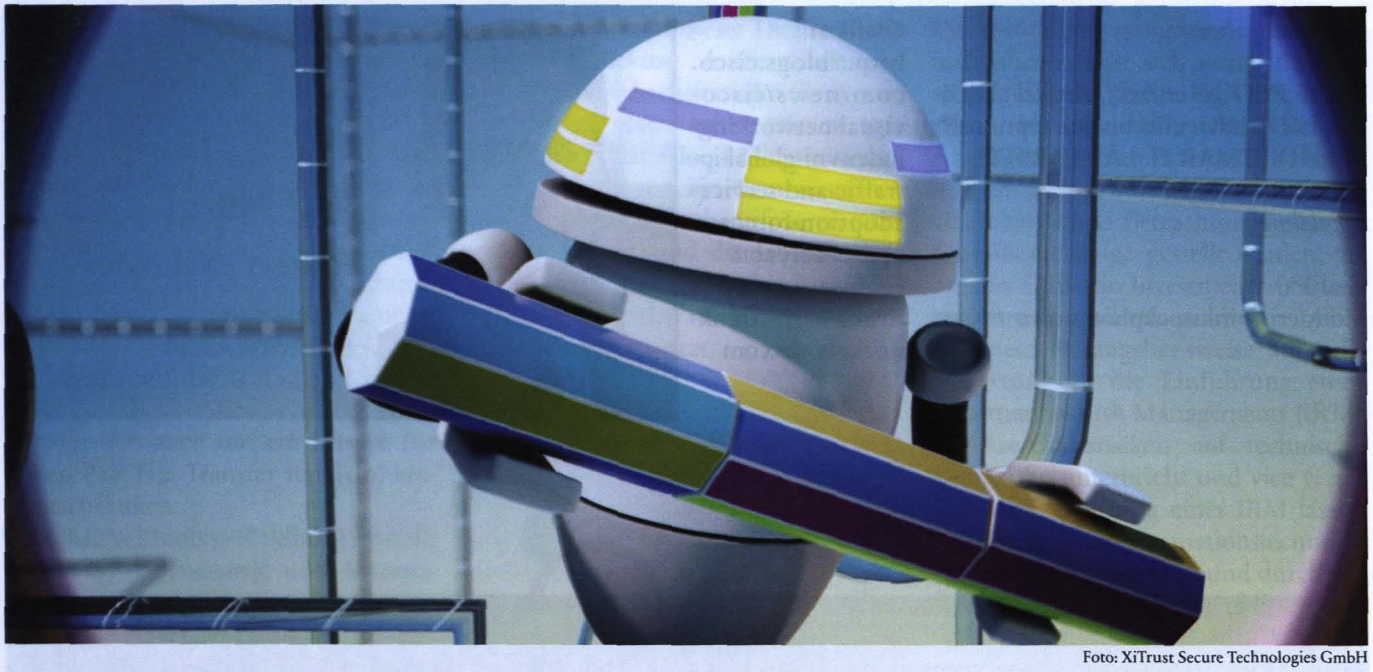

Foto: XiTrust Secure Technologies GmbH

Helmut Aschbacher, Gerhard Fliess, Gerald Wagner

Wie können kostengünstig und sicher Endsysteme für Industrie 4.0 Wartungslösungen angebunden werden?

Datenintegrität, Authentizität, Vertraulichkeit und Konnektivität: Herausfordernde Aufgaenstellungen und kostengünstige Lösungsansätze für die Industrie der Zukunft

Wie aktuelle Forschungsprojekte, wie beispielsweise ASSIST 4.0, zeigen ist das Thema „Konnektivität mit technischen Systemen/Anlagen" eine große Herausforderung der Industrie 4.0 (Industrie der Zukunft). Besonders im Umfeld der Aufgabenstellung „Wartung und Instandhaltung". Die Konnektivität mit den Endsystemen ermöglicht neben klassischen vorbeugenden Wartungs- und Instandhaltungsmaßnahmen auch die Erschließung neuer innovativer Dienstleistungsgeschäftsmodelle, z.B.: Smart Services, proaktive Dienstleistungserbringung für die Industrie. Allerdings müssen dabei Datenintegrität, -authentizität und Vertraulichkeit garantiert werden. In diesem Artikel wird daher die Fragestellung an Hand eines Beispiels geklärt, wie dies zu ermöglichen ist. Dabei wird eine Lösung vorgestellt, die kostengünstig Maschinenteile fälschungssicher kennzeichnen kann und dabei auch die zu Grunde liegende Basistechnologie für eine sichere Kommunikation mit dem Endsystem nutzt.

Einleitung

XiTrust wurde 2002 gegründet und ist ein kompetenter und innovativer Partner im Bereich für die Entwicklung und Erweiterung von sicheren und effizient gelösten Geschäftsprozessen. Entsprechend dem Missionstatement „Creating security ... developing quality" setzt XiTrust laufend innovative Projekte mit namhaften Projektpartnern im dynamischen Umfeld der Datensicherheit um. Das XiTrust Leistungsangebot bietet Kunden ein breites Portfolio in den Bereichen Datensicherheit, digitale Signatur, Langzeitarchivierung, medienbruchfreie Geschäftsprozesse und Healthcare. Das Kernstück der Produktpalette stellt der modulare XiTrust Business Server (XBS) dar, der ein weites Spektrum an Funktionen (XiTrust) bietet und der für Kundenprojekte ständig weiterentwickelt wird.

Im Rahmen des vom FFG geförderten Forschungsprojektes Assist 4.0 werden neue innovative Assistenzsysteme von den Unternehmen KNAPP AG, AVL GmbH und Infineon Technologies AG in Kooperation mit XiTrust entwickelt, die den Einsatz von Produktions- und Servicemitarbeitern revolutionieren sollen. Ein zentrales Softwaresystem in Kombination mit modernen mobilen Endgeräten wie Tablets, Smartphones oder Datenbrillen unterstützen das Servicepersonal situationsangepasst mit Informationen und visualisierten Daten, um Servicefälle besonders effektiv und effizient abzuwickeln.

Einer der insgesamt sechs Anwendungsfälle, welche in diesem Projekt

konzipiert, umgesetzt und evaluiert werden, wird in Kooperation mit dem Industriepartner KNAPP AG entwickelt. Als einer der Weltmarktführer auf dem Gebiet der Lagerautomation und Logistik mit mehr als 1600 Installationen gehören Wartung und Instandhaltung zu den Kerngeschäftsfeldern der KNAPP AG. Durch diese globale Positionierung am Markt steigt jedoch das Risiko, dass die eigenen Produkte und Ersatzteile zum Ziel von Produktfälschern werden.

Daraus resultiert der Bedarf, Maschinenteile fälschungssicher kennzeichnen und nachverfolgen zu können. Bisher eingesetzte analoge wie auch digitale Merkmale können mit geringem Aufwand gefälscht werden. Veränderte digitale Dokumente bzw. nachgebaute digitale Legitimationskennzeichnungen sind immer möglich.

Das FuE Projekt basiert auf dem Ansatz, elektronische Mechanismen zu etablieren, mit Hilfe derer die Gültigkeit von Maschinenteilekennzeichnungen (hinsichtlich Authentizität und Datenintegrität) verifiziert werden kann. Dazu werden elektronische Sicherheitsmerkmale benötigt, mit denen man die Integrität der Maschinenteiledaten überprüfen kann.

Hintergrund: Optische Sicherheitsmerkmale und Public-Key-Kryptographie

Optische Sicherheitsmerkmale werden im analogen Bereich angewandt, da sie leicht an Bauteilen angebracht werden können. Die Merkmale können ausschließlich von einer authentisierten Stelle erzeugt werden. So können beispielsweise die Sicherheitsmerkmale auf Banknoten nur von autorisierten Druckereien angebracht werden. Ein weiteres Beispiel für ein optisches Merkmal ist der QR-Code. QR-Codes sind vergleichbar mit Barcodes, bieten aber die Möglichkeit größere Datenmengen zu codieren und stellen eine Schnittstelle zwischen der digitalen und der analogen Welt dar. Sie werden entweder eingraviert, an der Oberfläche in Form von Etiketten angebracht oder digital dargestellt. Um die codierten Daten auswerten zu können, wird die Darstellung mit Hilfe eines entsprechenden Lesegerätes, wie beispielsweise einem Smartphone, abgefilmt und interpretiert.

Um Daten hinsichtlich ihrer Integrität und Authentizität zu überprüfen, kann die Methodik der digitalen Signatur eingesetzt werden. Die elektronische Signatur ist ein eigenständiges Datenpaket, das für die jeweiligen Bauteildaten berechnet und mit diesen verknüpft wird. Mithilfe der angefügten Signatur können die Daten bezüglich ihrer Gültigkeit validiert werden. Dafür kommt das Verfahren der Public-Key-Kryptographie zum Einsatz, welches sich eines privaten und eines öffentlichen Schlüssels bedient. Dabei werden zwei wesentliche Prozesse unterschieden:

- Das Erstellen einer digitalen Signatur mit dem privaten Schlüssel, der nur der ausstellenden Einheit bekannt ist und
- das Überprüfen der Signatur mit dem öffentlichen Schlüssel.

Nur wer im Besitz des privaten Schlüssels ist, kann die Signatur erzeugen. Der öffentliche Schlüssel kann beliebig verteilt werden (z.B. über eine Public-Key-Infrastruktur) und wird benötigt, um die Signatur auf ihre Gültigkeit zu prüfen.

Die smarte Lösung zur Maschinenteilekennzeichnung – s/QR Code

Im Zentrum der Maschinenteilkennzeichnung steht die Überprüfbarkeit und Nachvollziehbarkeit von Kunden-, Maschinenteil- und Ortsinformationen. Die Informationen werden gesammelt mit einer optionalen Referenz (ein ganzes Bild würde die Kapazität eines QR-Codes überschreiten) zu einer Bauteilabbildung in ein digitales Dokument geschrieben und im XiTrust Business Server für dieses Dokument wird eine digitale Signatur errechnet und abgespeichert.

Signatur und Dokument werden jeweils verschlüsselt und ein QR-Code wird generiert. Durch die Verbindung der Signatur und der Codierung in einen QR-Code (signed QR Code bzw. s/QR Code), ist es möglich eine fälschungssichere Maschinenteilekennzeichnung zu schaffen, welche nur von einer autorisierten Stelle erzeugt und einfach geprüft werden kann.

Prozessablauf

Der Ablauf zur fälschungssicheren Kennzeichnung von Maschinenteilen lässt sich in zwei Systemkomponenten gliedern:

Komponente 1 besteht aus einer Software und der dazugehörigen Serverinfrastruktur zur Generierung des s/QR-Codes unter der Verwendung des privaten Schlüssels. Die zur Speicherung vorgesehenen Informationen werden am Verifikationsserver hinterlegt.

Komponente 2 ist eine Prüf-Applikation auf einem mobilen Endgerät, welche den s/QR-Code interpretieren und sich gegenüber dem Verifikationsserver authentisieren kann, um u.a. auf Maschinenteilebilder oder ergänzende Wartungsinformationen zuzugreifen.

Die Sicherheit der Kommunikation zwischen den Systemkomponenten wird durch die Anwendung standardisierter Verschlüsselungsverfahren garantiert.

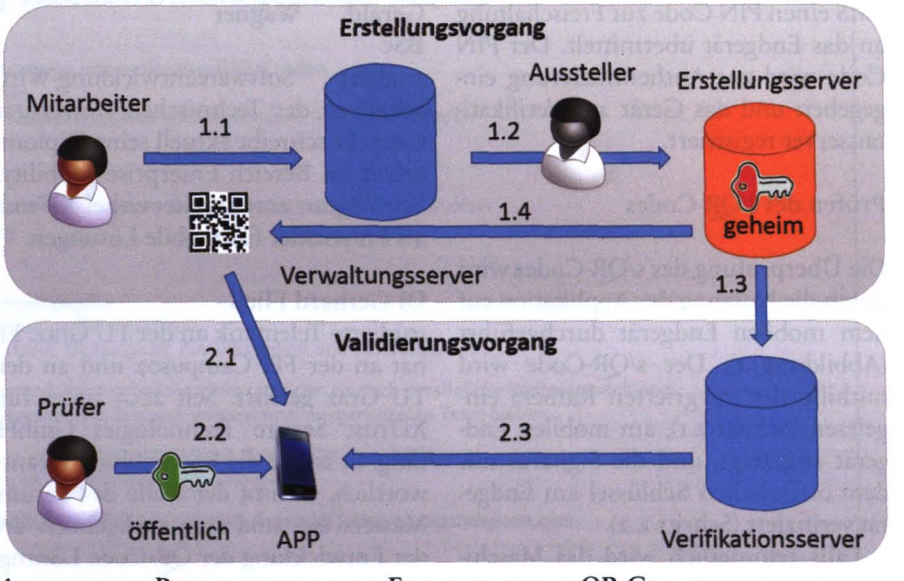

Abbildung 1 Prozessablauf zur Erstellung des QR Codes

Generierung des s/QR Codes

Abbildung 1 zeigt den Prozessablauf zur Ausstellung eines s/QR-Codes. Zu Beginn des Erstellungsvorgangs übergibt ein Mitarbeiter Kunden-, Maschinen- und Ortsangabedaten und, sofern möglich, ein Maschinenteilebild an die firmeninterne Registrierungsstelle.

(Schritt 1.1). Die Daten werden zunächst auf Vollständigkeit und Korrektheit geprüft, woraufhin die Generierung des s/QR-Codes am Erstellungsserver ausgelöst wird (Schritt 1.2). Dabei wird das Maschinenteilebild am Verifikationsserver publiziert (Schritt 1.3). Nach Abschluss des Generierungsprozesses erhält der zuständige Mitarbeiter eine automatisierte Rückmeldung des Systems (Schritt 1.4).

Der s/QR Code kann ab diesem Zeitpunkt zur Maschinenteilemarkierung verwendet werden.

Registrierung der Prüf-Applikation

Die Überprüfung des s/QR-Codes, wie sie beispielsweise im Rahmen von Wartungsarbeiten oder zur Nachbestellung von Maschinenteilen erforderlich ist, wird mittels einer Prüf-Applikation ermöglicht. Diese ist z.B. über die Unternehmenswebsite frei erhältlich. Um die Sicherheit der Daten zu gewährleisten ist eine Registrierung notwendig, um Zugriff auf die Systeme zu erhalten. Die Registrierung erfolgt nach Installation der Applikation am Endgerät und erfordert die Übermittlung der Rufnummer an den Server.

Die Registrierung wird dem Erstellungsserver gemeldet, welcher mittels SMS einen PIN Code zur Freischaltung an das Endgerät übermittelt. Der PIN Code wird zur Authentifizierung eingegeben und das Gerät am Verifikationsserver registriert.

Prüfen des s/QR-Codes

Die Überprüfung des s/QR-Codes wird durch die Nutzung der Applikation auf dem mobilen Endgerät durchgeführt (Abbildung 1). Der s/QR-Code wird mithilfe der integrierten Kamera eingelesen (Schritt 2.1), am mobilen Endgerät angezeigt, und die Signatur mit dem öffentlichen Schlüssel am Endgerät verifiziert (Schritt 2.2).

Falls erforderlich wird das Maschinenteilebild vom Verifikationsserver geladen (Schritt 2.3). Zusätzlich besteht die Möglichkeit ein Ampelsystem einzusetzen, um die Gültigkeit des s/QR Codes visuell darzustellen.

Fazit

Im Zuge des FuE Projekts ASSIST 4.0 konnte XiTrust am Beispiel der sicheren Maschinenteilekennzeichnung aufzeigen, dass durch die innovative Verknüpfung bestehender Basistechnologien die effiziente und kostengünstige Umsetzung von Sicherheitslösungen möglich ist. Das dabei entwickelte System besticht dank standardisierter Systemschnittstellen und Nutzung bewährter Kryptographie-Konzepte durch Robustheit, Verfügbarkeit und gleichzeitige Erweiterbarkeit.

Dipl.-Ing.
Gerhard Fließ
XiTrust Secure Technologies GmbH

Dipl.-Ing. (FH)
Dipl.-Ing. Dr.techn.
Helmut Aschbacher
XiTrust Secure Technologies GmbH

Gerald Wagner BSc
XiTrust Secure Technologies GmbH

Autoren:

Gerald Wagner BSc
studiert Softwareentwicklung-Wirtschaft an der Technischen Universität Graz. Er schreibt aktuell seine Diplomarbeit im Bereich Enterprise Mobility. Seit Beginn 2015 arbeitet er bei XiTrust als Entwickler für mobile Lösungen.

DI Gerhard Fließ
studierte Telematik an der TU Graz. Er hat an der FH Campus02 und an der TU Graz gelehrt. Seit 2003 ist er für XiTrust Secure Technologies GmbH tätig. Er ist für die Entwicklung verantwortlich, nimmt der Rolle des Scrum Masters ein und war maßgeblich an der Entwicklung der QR-Code Lösung beteiligt.

DI (FH) DI Dr.techn. Helmut Aschbacher
studierte IT & IT Marketing an der FH CAMPUS 02 sowie Telematik an der TU Graz. Er schrieb seine Dissertation an der TU Graz zum Thema IKT-basierte Dienstleistungen und Smart Services.
Seit 2013 ist er bei XiTrust Secure Technologies GmbH als Product Owner für Service Innovationsprojekte verantwortlich und als FuE Projektleiter tätig. Er forscht und publiziert seit 2006 zum Thema Service Engineering, Service Design und Smart Services (proaktive IKT basierte Dienstleistungen).