

Belgische Regierung hat mit dem Rollout begonnen

Offene, internationale Standards gewährleisten bei der Belgium National ID Card Interoperabilität und Sicherheit

Heinz Strauss, Chief Vision Officer und Sprecher der Liberty Alliance, Sun Microsystems

Der moderne und effiziente Staat: diese aktuellen Attribute leiten die politischen und technologischen Entwicklungen nicht nur in Deutschland und im Gesundheitswesen sondern in ganz Europa und weltweit und in einer Vielzahl von Projekten und Fachverfahren allgemein. Zentrale Bausteine bei der Architekturgestaltung hierbei sind intelligente Chipkarten, WebServices, Identity Management und Security im Rahmen sogenannter Service-orientierter-Architekturen SOA. Der Gesetzgeber hat die Ausgabe der Gesundheitskarten ab 2006 festgelegt. Was sind die Entwicklungstrends besonders in Europa in Bezug auf die technologischen Architekturgestaltungen? Welchen Trends zeichnen sich für die Gesundheitskarte in Deutschland ab und welche internationalen Standards sind relevant für Interoperabilität und Sicherheit?

Die elektronische Gesundheitskarte eGK soll die bisherige Krankenversicherungskarte ersetzen und die mehr als 80 Millionen Patienten, 270.000 Ärzte, 77.000 Zahnärzte, 22.000 Apotheken, 2000 Krankenhauser und rund 300 Krankenkassen in Deutschland vernetzen. Das Auslesen personenbezogener Daten ist dabei auf die Nutzerkreise der Ärzte und Apotheker beschränkt, die im Rahmen ihrer heilberuflichen Tätigkeiten über einen Heilberufsausweis HBA verfügen werden. Beide Karten, eGK und HBA, sind als Signaturkarten mit zusätzlicher Speicherung von Daten, wie Patientenbasisdaten, geplant. Für die Patienten besteht die Möglichkeit, Arzneimittel oder Notfalldaten auf freiwilliger Basis dokumentieren zu lassen. Beide Karten werden eine persönliche PIN haben, wie heute Bankenkarten oder Mobilfunkkarten. Für den Anwendungsfall der elektronische Abwicklung der jährlich ca. 800 Millionen Rezepte ist die PIN der eGK nicht verwendet.

Vor dem Hintergrund dieser zahlreichen behördlichen und kommerziellen Anwendungen und der damit in Verbindung stehenden Anforderungen besonders auch in Verbindung mit dem Signaturgesetz § SigG hatte sich Anfang 2003 die Public-Private-Partnership zwischen für elektronische Signatur (www.signaturbuendnis.de) unter der Aufsicht des Bundesinnenministeriums gegründet. Das Signaturbündnis ist ein offenes, herstellerunabhängiges Bündnis behördlicher und kommerzieller Organisationen und Unternehmen, die sich zur Aufgabe gestellt haben, Spezifikationen und Standardisierungen im Hinblick auf international akzeptierte Standards und unter besonderer Berücksichtigung der nationalen Gesetzgebung (siehe Datenschutzgesetz, Signaturgesetz) und nationaler Regulierungen (siehe Regelungsbehörde für Telekommunikation und Post, RegTP) sowohl auf der Ebene der Geschäftsmodelle und -prozesse als auch aus der Ebene technischer Spezifikationen voranzutreiben. Nicht zuletzt sind diese Maßnahmen darüber hinaus auch in Bezug auf die außerordentlich hohe Wertschätzung auf EU-Ebene und international zu betrachten in der Form, dass die gewonnenen Spezifikationen Grundlage bilden können für Gesetzesvorlagen und Architektur Anforderungen insgesamt, wie es bereits vielerseits im Bereich des deutschen Datenschutzgesetzes möglich ist und war. Die technologischen Normierungsaktivitäten des Signaturbündnisses sind niedergefasst in der ISIS-MTT-Spezifikation (www.teletrust.de). ISIS-MTT ermöglicht erstmals Interoperabilität elektronischer Signaturen, welche den Dreh- und Angelpunkt für die Rechtssicherheit des elektronischen Geschäftsverkehrs darstellen. Ihrer Ausbreitung stand bisher die mangelnde Interoperabilität der verschiedenen Signaturprodukte entgegen. Um diese Erfolgsbarriere zu beseitigen, hat der TeleTrust e.V. im Rahmen eines vom Bundesministerium für Wirtschaft und Arbeit (BMWA) in Auftrag gegebenen Projektes einen einheitlichen Interoperabilitätsstandard für elektronische Signaturen und Public Key Infrastrukturen (ISIS-MTT) unter Einbeziehung aller maßgeblichen Partner in Wirtschaft und Verwaltung erarbeitet. Akzeptierte, internationale Standards (wie ESTI, CEN, PKI/IX und PCKS, Liberty Alliance,...) bilden dabei die Grundlage der Betrachtungen und werden im Hinblick auf nationale Anforderungen adaptiert. Auch das Bündnis für elektronische Signaturen setzt bereits jetzt voll auf ISIS-MTT. Einmal erworbene Signaturanwendungen und Zertifikate können überall im elektronischen Geschäftsverkehr für Kommunikation, Interaktion und Transaktion mit beliebigen Partnern im staatlichen, kommerziellen und privaten Bereich genutzt werden. Standardisierungsinitiativen wie SAGA und OSCI bauen auf diese Vorgaben auf.

Der internationale Trend zu offenen Standards ist besonders auch in Europa und in Deutschland klar vorgegeben. Bereits im April 2003 hatte die belgische Regierung als erstes europäisches Land die Belgian National ID Card (kurz eID, electronic Identity Card) eingeführt. Die eID Card in Belgien wurde zu dem ersten grossen Projekt unter maßgeblicher Beteiligung von Sun Microsystems in Verbindung mit JavaCard-Technologie im Identity Card Sektor in Europa und repräsentiert gleichzeitig einen wesentlichen Meilenstein der belgischen eGovernment-Initiative, so Jan Deprest, Präsident von Fedict, Federale Overheidsdienst voor ICT, Informatieen communicatie technologie in Belgien. Diese Karte erlaubt es den belgischen Bürgern sich im Rahmen von eGovernment-Anwendungen auf einfache Art und Weise sicher zu authentifizieren. Das eID Projekt wird außerdem zukünftig für kommerzielle Anwendungen ausgeweitet, so dass Bürgerinnen und Bürger Mehrwertdienste wie Bezahlendienste, Reservierungsdienste etwa für Kulturveranstaltungen nutzen können. Sie werden auch in der Lage sein mittels einer persönlichen, elektronischen Signatur elektronische Dokumente und z.B. Formulare zu signieren, so dass diese mit derselben Rechtssicherheit akzeptiert werden können wie mit einer handschriftlichen Unterschrift. Während bislang einige zehntausend Karten auf Basis von JavaCard-Technologie ausgegeben wurden bestatigte das Ministerium das komplette Deployment der Karten

mit Beginn zum Dezember 2005. Die JavaCard-Technologie ermöglicht es dabei, dass multiple Anwendungen in einer jeweils sicheren Ablaufumgebung innerhalb einer einzigen Smart Card koexistieren können. Die JavaCard-Technologie ist ein offener Standard und zusätzlich eine durch international zahlreiche Projekte ausgereifte Technologie mit Einsatzbereichen in verschiedenen Marktsegmenten wie z.B. bei Finanzdienstleistern, im Bereich der Telekommunikationsdienstleister und auch weltweit bei öffentlichen Auftraggebern, deren besondere Wertschöpfung sich aus dem hohen Mass an Sicherheit, den Möglichkeiten der Interoperabilität, der Multiple-Application-Fähigkeit und dem schlüssigen Einhalten Offener Standards ableitet, so Jan Deprest. Der Vorteil dieser dynamischen Kartenplattform ist es, dass neue Kartenanwendungen sukzessive ins Feld gebracht werden können ohne gleichzeitig neue Karten herausgeben zu müssen. Ausserdem können Anwendungen, die nicht mehr benötigt werden vom Karteninhaber gelöscht und durch neue Anwendungen ersetzt werden. Dadurch bleibt die Karte seiner aktuellen Verwendungsform immer angepasst und kann an die jeweilige Verwendungsrolle adaptiert werden, wodurch der Lebenszeitraum der Karte verlängert und die Kosten insgesamt gesenkt werden. Mehr als eine Milliarde JavaCards sind derzeit im Umlauf.

Auch das Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG), eine Behörde des holländischen Gesundheitsministeriums, hat sich bei der Implementierung der holländischen Gesundheitskarte im September 2004 für die JavaCard-Plattform entschieden. Ebenso ist im September 2004 die Entscheidung für die finnische eID-Karte für offene Standards und die JavaCard getroffen worden.

Im Rahmen der Gesamtarchitekturen von IT-Projekten, die auf JavaCard-Technologien aufsetzen, stehen aus der Erfahrung immer zusätzliche, besonders auch Signatur-relevante Technologien im Einsatz wie z.B. das Java Cryptographie Modul, das Betriebssystem selbst, höhere Infrastrukturdienste wie Directory und Identity Services und schließlich die eigentlichen Anwendungen oder Fachverfahren. Durch die konsequente Berücksichtigung internationaler Identity- und Security-Spezifikationen kann eine Sicherheitszertifizierung z.B. in Deutschland durch das Bundesamt für Sicherheit in der Informationstechnik BSI der Gesamtarchitektur vorgenommen werden. Die Zertifizierung dieser IT-Technologien des Security-Frameworks trägt im Wesentlichen Masse zur Gewährleistung der größtmöglichen Sicherheit, zur internationalen Interoperabilität und somit auch zum Investitionsschutz bei. Aus diesem Grund unterstützen die weltweit führenden Unternehmen sowohl die internationalen und nationalen Spezifikationen und Zertifizierungen wie z.B. auch den OASIS Standard (www.oasis-open.org/news/oasis_news_03_02_05_a4.pdf) und speziell auch der Standardisierungen auf Basis nach CERT. Bereits im Januar 2002 wurde auf der internationalen Sicherheitskonferenz der OpenGroup unter dem Vorsitz von Allan Brown, President und CEO, The Open Group, die strategisch wichtige Bedeutung in der Kombination JavaCard, Identity Management, Liberty Alliance und offener Standards herausgestellt (www.opengroup.org/security/idm.htm). Heute ist aus den aktuellen Standardisierungsgremien genau diese Kombination nicht mehr wegzudenken und fester Bestandteil jeder Gesamtarchitektur. Die Liberty Alliance (www.projectliberty.org) ist ein internationales Konsortium kommerzieller und behördlicher Organisationen bzw. Unternehmen die sich zum Ziel gesetzt hat internationale Standards und Spezifikationen, sowohl auf der Ebene der Geschäftsmodelle als auch der technologischen Ebene zu definieren. Weltweit nahezu jedes in dem Bereich IT-Security tangierte Unternehmen oder Organisation ist Mitglied der Liberty Alliance als Anbieter von Hard- oder Software, als Dienstleistungsanbieter oder letztlich auch als Anwender oder sogar als staatliche Einrichtung (Behördenstellen, Institute, Krankenhäuser etc.). Die Organisation der Liberty Alliance bildet dabei internationale, normierte Identity-, Trust- und Security-Spezifikationen auf Businessmodelle wie z.B. das Gesundheitswesen ab. Hierzu ist die Liberty Alliance auf das Spezialwissen seiner Mitglieder besonders im Bereich der Geschäftsprozesse angewiesen. Bereits heute stellt die Liberty Alliance einen umfassenden Satz an Spezifikationen und Geschäftsfeldregulierungen dar, zu deren Implementierung und Umsetzung sich seine Mitgliedsunternehmen und -organisationen weltweit verpflichtet und committed haben. Einige dieser Sicherheits- und Kommunikationsmechanismen sind heute bereits soweit in dem Verbreitungsgrad fortgeschritten, dass diese Technologien auch aus kommerzieller Sicht bereits als Commodity-Verfahren angesehen werden können. So hat z.B. Sun Microsystems den Source Code seiner IT-Lösungen zu Single-Sign-On und zur Web-Authentifizierung im Juli 2005 der Open Source Community zur Verfügung gestellt.

Peter Strickx, Chief Technology Officer von Fedict, Belgien unterstreicht in einem Interview im September 2005 nochmals die drei wichtigsten Entscheidungskriterien der belgischen Regierung: 1) Skalierbarkeit im Deployment 2) Sicherheit 3) Investitionsschutz durch offene Standards. Wir gehen von einem Lebenszeitraum der Karte von 5 Jahren aus. Durch die JavaCard-Technologie sind wir dabei unabhängig vom eigentlichen Chip-design der Karte. Sollten also im Fortlauf der eGovernment-Anwendungen über die Jahre hinaus z.B. höhere Anforderung an starke Authentifizierung entstehen und Änderungen im Chipdesign der Karte notwendig machen, dann hat das keine Auswirkung auf unsere Fachverfahren. Die Forderung nach offenen Standards eröffnet uns außerdem den Zugang zu einer elitären Entwickler-Community bei unterschiedlichen Software-Unternehmen. Java - es ist ein offener Markt auf qualitativ sehr hohem Niveau. Die erste Phase ist sehr erfolgreich abgeschlossen, so dass die belgische Regierung die Ausgabe der ersten 1,8 Millionen eID Karten bis Ende 2005 bestmöglichste konnte und letztendlich dann alle 11 Millionen Bürgerinnen und Bürger ab dem 12. Lebensjahr die Vorteile und Services dieser Infrastruktur nutzen können. Der wesentliche Unterschied z.B. zur in Deutschland geplanten eGK besteht darin, dass auf der belgischen eID Karte über den eigentlichen Credentials zur Authentifizierung keine zusätzlichen Informationen gespeichert werden. Die belgische eID Karte dient also ausschließlich der Authentifizierung und hält beispielsweise keine Patientendaten vor den Notfall. Technologisch wäre dieses zwar kein Problem, doch zum Zeitpunkt unserer Projektierung im Jahre 2003 war das nicht Gegenstand unserer Betrachtungen, so Peter Strickx weiter.

Nur internationale offene Standards, idealerweise akzeptiert durch die Adaption nationaler Regulierungen fördern Interoperabilität, fördern die Federation von Diensten und gewährleisten Sicherheitsanforderungen auf höchstem Niveau und sie bilden die Grundlage für kommerzielle und behördliche Anwendungen und Fachverfahren "international, in Deutschland und auch bei der elektronischen Gesundheitskarte.

Kontakt

Dipl.-Ing. Heinz Strauss

Chief Vision Officer

Sun Microsystems

Mitglied im

„Bündnis für elektronische

Signatur“ und Sprecher der

Liberty Alliance

Rechtlicher Hinweis:

Ein Herunterladen des Dokuments ist ausschließlich zum persönlichen Gebrauch erlaubt. Jede Art der Weiterverbreitung oder Weiterverarbeitung ist untersagt. [Freier Download \(hier klicken\)](#)