Belgische Regierung hat mit dem Rollout begonnen

Offene, internationale Standards gewÃ¤hrleisten bei der â€žBelgium National ID Cardâ€œ InteroperabilitÃ¤t und Sicherheit

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

Der â€žmoderne und effiziente Staatâ€œ: 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 fÃ¼r die Gesundheitskarte in Deutschland ab und welche internationalen Standards sind relevant fÃ¼r InteroperabilitÃ¤t und Sicherheit?

Die elektronische Gesundheitskarte eGK soll die bisherige Krankenversicherungskarte ersetzen und die mehr als 80 Millionen Patienten, 270.000 Ã„rzte, 77.000 ZahnÃ¤rzte, 22.000 Apotheken, 2000 KrankenhÃ¤user und rund 300 Krankenkassen in Deutschland vernetzen. Das Auslesen personenbezogener Daten ist dabei auf die Nutzerkreise der Ã„rzte und Apotheker beschrÃ¤nkt, die im Rahmen ihrer heilberuflichen TÃ¤tigkeiten Ã¼ber einen Heilberufeausweis HBA verfÃ¼gen werden. Beide Karten, eGK und HBA, sind als Signaturkarten mit zusÃ¤tzlicher Speicherung von Daten, wie Patientenbasisdaten, geplant. FÃ¼r die Patienten besteht die MÃ¶glichkeit, Arzneimittel oder Notfalldaten auf freiwilliger Basis dokumentieren zu lassen. Beide Karten werden eine persÃ¶nliche PIN haben, wie heute Bankenkarten oder Mobilfunkkarten. FÃ¼r den Anwendungsfall der elektronische Abwicklung der jÃ¤hrlich ca. 800 Millionen Rezepte ist die PIN der eGK nicht verwendet.

Vor dem Hintergrund dieser zahlreichen behÃ¶rdlichen und kommerziellen Anwendungen und der damit in Verbindung stehenden Anforderungen besonders auch in Verbindung mit dem Signaturgesetz Â§ SigG hatte sich Anfang 2003 die Public-Private-Partnership â€žBÃ¼ndnis fÃ¼r elektronische Signaturâ€œ (www.signaturbuendnis.de) unter der Aufsicht des Bundesinnenministeriums gegrÃ¼ndet. Das SignaturbÃ¼ndnis ist ein offenes, herstellerunabhÃ¤ngiges BÃ¼ndnis behÃ¶rdlicher und kommerzieller Organisationen und Unternehmen, die sich zur Aufgabe gestellt haben, Spezifikationen und Standardisierungen im Hinblick auf international akzeptierte Standards und unter besonderer BerÃ¼cksichtigung der nationalen Gesetzesgebung (siehe Datenschutzgesetz, Signaturgesetz) und nationaler Regulierungen (siehe RegulierungsbehÃ¶rde fÃ¼r Telekommunikation und Post, RegTP) sowohl auf der Ebene der GeschÃ¤ftsmodelle und -prozesse als auch aus der Ebene technischer Spezifikationen voranzutreiben. Nicht zuletzt sind diese MaÃŸnahmen darÃ¼berhinaus auch in Bezug auf die auÃŸerordentlich hohe WertschÃ¤tzung auf Eu-Ebene und international zu betrachten in der Form, dass die gewonnenen Spezifikationen Grundlage bilden kÃ¶nnen fÃ¼r Gesetzesvorlagen und Architekturanforderungen insgesamt, wie es bereits vielerseits im Bereich des deutschen Datenschutzgesetzes Ã¼blich ist und war. Die technologischen NormierungsaktivitÃ¤ten des SignaturbÃ¼ndnisses sind niedergefasst in der ISIS-MTT-Spezifikation (www.teletrust.de). ISIS-MTT ermÃ¶glicht erstmals InteroperabilitÃ¤t elektronischer Signaturen, welche den Dreh- und Angelpunkt fÃ¼r die Rechtssicherheit des elektronischen GeschÃ¤ftsverkehrs darstellen. Ihrer Ausbreitung stand bisher die mangelnde InteroperabilitÃ¤t der verschiedenen Signaturprodukte entgegen. Um diese Erfolgsbarriere zu beseitigen, hat der TeleTrusT e.V. im Rahmen eines vom Bundesministerium fÃ¼r Wirtschaft und Arbeit (BMWA) in Auftrag gegebenen Projektes einen einheitlichen InteroperabilitÃ¤tsstandard fÃ¼r elektronische Signaturen und Public Key Infrastrukturen (ISIS-MTT) unter Einbeziehung aller maÃŸgeblichen 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 BÃ¼ndnis fÃ¼r elektronische Signaturen setzt bereits jetzt voll auf ISIS-MTT. Einmal erworbene Signaturanwendungen und Zertifikate kÃ¶nnen Ã¼berall im elektronischen GeschÃ¤ftsverkehr fÃ¼r 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 europÃ¤isches Land die Belgian National ID Card (kurz eID, electronic Identity Card) eingefÃ¼hrt. â€žDie eID Card in Belgien wurde zu dem ersten grossen Projekt unter maÃŸgeblicher Beteiligung von Sun Microsystems in Verbindung mit JavaCardâ„¢-Technologie im Identity Card Sektor in Europa und reprÃ¤sentiert gleichzeitig einen wesentlichen Meilenstein der belgischen eGovernment-Initiativeâ€œ, so Jan Deprest, PrÃ¤sident von Fedict, Federale Overheidsdienst voor ICT, Informatieen communicatie technologie in Belgien. â€žDieses Karte erlaubt es den belgischen BÃ¼rgern sich im Rahmen von eGovernment-Anwendungen auf einfache Art und Weise sicher zu authentifizieren. Das eID Projekt wird auÃŸerdem zukÃ¼nftig fÃ¼r kommerzielle Anwendungen ausgeweitet, so dass BÃ¼rgerinnen und BÃ¼rger Mehrwertdienste wie Bezahldienste, Reservierungsdienste etwa fÃ¼r Kulturveranstaltungen nutzen kÃ¶nnen. Sie werden auch in der Lage sein mittels einer persÃ¶nlichen, elektronischen Signatur elektronische Dokumente und z.B. Formulare zu signieren, so dass diese mit derselben Rechtssicherheit akzeptiert werden kÃ¶nnen wie mit einer handschriftlichen Unterschrift.â€œ WÃ¤hrend bislang einige zehntausend Karten auf Basis von JavaCardâ„¢-Technologie ausgegeben wurden bestÃ¤tigte das Ministerium das komplette Deployment der Karten

mit Beginn zum Dezember 2005. â€žDie JavaCardâ„¢-Technologie ermÃ¶glicht es dabei, dass multiple Anwendungen in einer jeweils sicheren Ablaufumgebung innerhalb einer einzigen Smard Card koexistieren kÃ¶nnen. Die JavaCardâ„¢-Technologie ist ein offener Standard und zusÃ¤tzlich 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 Ã¶ffentlichen Auftraggebern, deren besondere WertschÃ¶pfung sich aus dem hohen Mass an Sicherheit, den MÃ¶glichkeiten der InteroperabilitÃ¤t, der Multiple-Application-FÃ¤higkeit und dem schlÃ¼ssigen Einhalten Offener Standards ableitetâ€œ, so Jan Deprest. Der Vorteil dieser dynamischen Kartenplattform ist es, dass neue Kartenanwendungen sukzessive ins Feld gebracht werden kÃ¶nnen ohne gleichzeitig neue Karten herausgeben zu mÃ¼ssen. Ausserdem kÃ¶nnen Anwendungen, die nicht mehr benÃ¶tigt werden vom Karteninhaber gelÃ¶scht 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 verlÃ¤ngert und die Kosten insgesamt gesenkt werden. Mehr als eine Milliarde JavaCardsâ„¢ sind derzeit im Umlauf.

Auch das Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG), eine BehÃ¶rde des hollÃ¤ndischen Gesundheitsministeriums, hat sich bei der Implementierung der hollÃ¤ndischen Gesundheitskarte im September 2004 fÃ¼r die JavaCardâ„¢-Plattform entschieden. Ebenso ist im September 2004 die Entscheidung fÃ¼r die finnische eID-Karte fÃ¼r offene Standards und die JavaCardâ„¢ getroffen worden.

Im Rahmen der Gesamtarchitekturen von IT-Projekten, die auf JavaCardâ„¢-Technologien aufsetzen, stehen aus der Erfahrung immer zusÃ¤tzliche, besonders auch Signatur-relevante Technologien im Einsatz wie z.B. das Java Cryptographie Modul, das Betriebssystem selbst, hÃ¶here Infrastrukturdienste wie Directory und Identity Services und schlieÃŸlich die eigentlichen Anwendungen oder Fachverfahren. Durch die konsequente BerÃ¼cksichtigung internationaler Identity- und Security-Spezifikationen kann eine Sicherheitszertifizierung z.B. in Deutschland durch das Bundesamt fÃ¼r Sicherheit in der Informationstechnik BSI der Gesamtarchitektur vorgenommen werden. Die Zertifizierung dieser IT-Technologien des Security-Frameworks trÃ¤gt im Wesentlichen Masse zur GewÃ¤hrleistung der grÃ¶ÃŸtmÃ¶glichen Sicherheit, zur internationalen InteroperabilitÃ¤t und somit auch zum Investionsschutz bei. Aus diesem Grund unterstÃ¼tzen die weltweit fÃ¼hrenden 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 JavaCardâ„¢, 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 behÃ¶rdlicher Organisationen bzw. Unternehmen die sich zum Ziel gesetzt hat internationale Standards und Spezifikationen, sowohl auf der Ebene der GeschÃ¤ftsmodelle als auch der technologischen Ebene zu definieren. Weltweit nahezu jedes in dem Bereich IT-Security tangiertes Unternehmen oder Organisation ist Mitglied der Liberty Alliance â€“ als Anbieter von Hard- oder Software, als Dienstleistungsanbieter oder letztlich auch als Anwender oder sogar als staatliche Einrichtung (BehÃ¶rdenstellen, Institute, KrankenhÃ¤user 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 GeschÃ¤ftsprozesse angewiesen. Bereits heute stellt die Liberty Alliance einen umfassenden Satz an Spezifikationen und GeschÃ¤ftsfeldregulierungen dar, zu deren Implementierung und Umsetzung sich seine Mitgliedsunternehmen und -organisationen weltweit verstÃ¤ndigt und commited haben. Einige dieser Sicherheits- und Kommunikationsmechanismen sind heute bereits soweit in dem Verbreitungsgrad fortgeschritten, dass diese Technologien auch aus kommerzieller Sicht bereits als â€žCommodityâ€œ-Verfahren angesehen werden kÃ¶nnen. So hat z.B. Sun Microsystems den Source Code seiner IT-LÃ¶sungen zu Single-Sign-On und zur Web-Authentifizierung im Juli 2005 der Open Source Community zur VerfÃ¼gung gestellt.

Peter Strickx, Chief Technology Officer von Fedict, Belgien unterstreicht in einem Interview im September 2005 nochmals die drei wichtgsten Entscheidungskriterien der belgischen Regierung: â€ž1) Skalierbarkeit im Deployment 2) Sicherheit 3) Investionsschutz durch offene Standards. Wir gehen von einem Lebenszeitraum der Karte von 5 Jahren aus. Durch die JavaCardâ„¢-Technologie sind wir dabei unabhÃ¤ngig vom eigentlichen Chip-design der Karte. Sollten also im Fortlauf der eGovernment-Anwendungen Ã¼ber die Jahre hinaus z.B. hÃ¶here Anforderung an starke Authentifizierung entstehen und Ã„nderungen im Chipdesign der Karte notwendig machen, dann hat dass keine Auswirkung auf unsere Fachverfahren. Die Forderung nach offenen Standards erÃ¶ffnet uns auÃŸerdem den Zugang zu einer elitÃ¤ren Entwickler-Community bei unterschiedlichen Software-Unternehmen. Java - es ist ein offener Markt auf qualitativ sehr hohem Niveau.â€œ Die erste Phase ist sehr erfolgreich abgeschlossen, so dass die belgische Regierung die Ausgabe der ersten 1,8 Millionen eID Karten bis Ende 2005 bestÃ¤tigen konnte und letztendlich dann alle 11 Millionen BÃ¼rgerinnen und BÃ¼rger ab dem 12. Lebensjahr die Vorteile und Services dieser Infrastruktur nutzen kÃ¶nnen. â€žDer wesentliche Unterschied z.B. zur in Deutschland geplanten eGK besteht darin, dass auf der belgischen eID Karte auÃŸer den eigentlichen Credentials zur Authentifizierung keine zusÃ¤tzlichen Informationen gespeichert werden. Die belgische eID Karte dient also ausschlieÃŸlich der Authentifizierung und hÃ¤lt beispielsweise keine Patientendaten vor fÃ¼r den Notfall. Technologisch wÃ¤re dieses zwar kein Problem, doch zum Zeitpunkt unserer Projektierung im Jahre 2003 war das nicht Gegenstand unserer Betrachtungen,â€œ so Peter Strickx weiter.

Nur internationale offene Standards, idealerweise akzeptiert durch die Adaption nationaler Regulierungen fÃ¶rdern InteroperabilitÃ¤t, fÃ¶rdern die FÃ¶deration von Diensten und gewÃ¤hren Sicherheitsanforderungen auf hÃ¶chstem Niveau und sie bilden die Grundlage fÃ¼r kommerzielle und behÃ¶rdliche Anwendungen und Fachverfahren â€“ international, in Deutschland und auch bei der elektronischen Gesundheitskarte.

Kontakt
Dipl.-Ing. Heinz Strauss
Chief Vision Officer
Sun Microsystems
Mitglied im
â€žBÃ¼ndnis fÃ¼r elektronische
Signaturâ€• und Sprecher der
Liberty Alliance