SMART WORLD

Der globale Bürger im Scheckkartenformat - überall “greifbar“ nahe?

Von Marlene Neudörffer

Darmstadt, den 14.09.06

Die Welt tickt smart. Dabei kann das Attribut irreführend sein, denn wenn es um den Einsatz moderner Smart Chip Technologie geht, mag die bestechend kleine Größe der Chips angesichts der darin steckenden Leistungsfähigkeit einen gewissen Charme versprühen, doch sorgt eben diese Hochtechnologie für immensen Diskussionsstoff über die Sicherheit der hier gespeicherten Daten.

Einerseits soll der mit einem Funkchip ausgestattete elektronische Reisepass (ePASS) die Identifikation von Reisenden sicherer machen, andererseits stecken in den geplanten Hightech-Reisedokumenten noch Sicherheitslücken, die es zu schließen gilt. Es muss sichergestellt sein, dass die Personendaten etwa gegen heimliches Auslesen geschützt sind. Eine Lücke tut sich zwischen Pass und Lesegerät auf, wenn die Hochfrequenz-Kommunikation zwischen diesen beiden Komponenten abgehört werden kann.

Besonders sensible Informationen enthält der Chip der elektronischen Gesundheitskarte (eGK), auf dem sich Daten zur Person und ihrer jeweiligen Krankenakte verewigen lassen. Auch hier sind mit der Einführung der Karte hohe Anforderungen an die Zuverlässigkeit, Sicherheit und Performanz des Gesamtsystems – der eingesetzten Komponenten und Dienste sowie der Telematikinfrastruktur – verbunden.

Um diesen Themenkreis SmartCard-basierter Ausweissysteme ging es in dem Forum, zu dem das Competence Center for Applied Security Technology CAST am 14. September 2006 in das Fraunhofer-Institut für Graphische Datenverarbeitung IGD nach Darmstadt eingeladen hatte.

INTEROPERABILITÄT VON PASSLESEGERÄTEN UND PÄSSEN

Welche besonderen Anforderungen an den elektronischen Reisepass und die Lesegeräte gestellt werden, erläuterte Michael Schlüter von der secunet Security Networks AG, die in dieser Thematik mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammenarbeitet.

Reisedokumente sind hoheitliche Dokumente. Da bleibe es nicht aus, dass unterschiedliche Länder unterschiedliche Interessen verfolgten, erläuterte Schlüter. Die Passhersteller wiederum hätten wenig Verbindung zur IT und den neuen Herausforderungen hinsichtlich Datensicherheit und Verschlüsselung. Nicht zuletzt müsse die Technik für eine lange Nutzungsdauer ausgelegt sein, da Pässe in der Regel bis zu zehn Jahren Gültigkeit besäßen, skizzierte Schlüter die Ausgangssituation.

Um dieser Problematik zu begegnen, wurde 2004 von der International Civil Aviation Organization (ICAO) eine Spezifikation für Datenstrukturen und Sicherheitsmechanismen maschinenlesbarer Reisedokumente veröffentlicht. Sie beschreibt, wie die Daten in Form einer Logical Data Structure (LDS) auf dem Reisedokument gespeichert und wie die Public Key Infrastructure (PKI) aussieht, um diese Daten zu schützen und zu authentisieren.

Über das von secunet entwickelte Golden Reader Tool (GRT) wird das ICAO-Layout gelesen. In zahlreichen internationalen Tests wurde in dem äußerst aufwändigen Cross-Over Verfahren die Interoperabilität von Pass und Lesegerät untersucht, zuletzt im Mai 2006 in Berlin mit rd. 450 Teilnehmern aus 38 Ländern. Es hat sich gezeigt, dass diese Methode inzwischen an ihre Grenzen gestoßen ist. In Zukunft sind separate Tests geplant, in denen jede Komponente für sich auf Konformität mit vorgegebenen Standards getestet und zertifiziert werden soll (Conformity Test). Hier arbeitet das BSI an einem Zertifizierungsschema und einer Testspezifikation für Pass und Passleser, die international weiterentwickelt werden soll.	**Conformity Test löst Cross-Over Methode ab**

EUROPEAN CITIZEN CARD (ECC) – SACHSTAND DER EUROPÄISCHEN SPEZIFIKATION UND MÖGLICHE UMSETZUNGEN

Bequemes Reisen innerhalb Europas und sichere Identifikation des europäischen Bürgers soll die European Citizen Card (ECC) ermöglichen. Und damit nicht genug. Auch die Einbindung von eGovernment- und eBusiness-Anwendungen ist geplant. Wie weit die Reise der einzelnen europäischen Staaten zur ECC noch ist erläuterte Ingo Liersch von dem Kartenanbieter Giesecke & Devrient.

Zwar haben einige europäische Länder, darunter Belgien, bereits einen digitalen Personalausweis eingeführt, doch sind diese Ausweise proprietär und entsprechen nicht dem ECC Standard. Dieser wird von dem zuständigen europäischen Komitee für Normung (Comité Européen de Normalisation - CEN) festgelegt und umfasst die Bereiche:

- ECC-1: Physikalische Schnittstellen
- ECC-2: Logische Datenstruktur
- ECC-3: Personalisierung und Middleware.

ECC1 und ECC2 befinden sich in der finalen Abstimmung, ECC3 in der Anfangsphase. Hier soll durch eine standardisierte Middleware (CEN TC 224 WG17) sichergestellt werden, dass neben ECCs auch die nicht spezifikationskonformen Ausweise europaweit digital gelesen werden können.

Neben dem französischen Industriekonsortium GIXEL sind das deutsche Industrieforum (DIF) und die Gesellschaft für Telematikanwendungen der Gesundheitskarte - gematik an der Erarbeitung des europäischen Standards beteiligt. Giesecke & Devrient, die Bundesdruckerei und Infineon gehören zu den Gründungsmitgliedern des am 07. Oktober 2004 etablierten DIF. Unter Berücksichtigung der vom BMI /BSI vorgegebenen Anforderungen erstellt das DIF die Spezifikation für den deutschen elekronischen Personalausweis (ePA), die Schnittstellen-Dokumente für Terminal und Middleware und ist verantwortlich für die Umsetzung auf Basis der europäischen und international relevanten Standards.

Europäische Bürgerkarte mit nationalem Profil

Damit zusätzliche eBusiness- und eGovernment-Funktionen sicher in das elektronische Reisedokument eingebunden werden können, müssen Services für die Identifkation, Authentisierung und digitale Signatur (IAS) festgelegt werden. Dies betrifft die Benutzerauthentisierung ebenso wie die Geräteauthentisierung. Verschiedene technische Optionen werden diskutiert. Elliptische Kurven oder RSA, Benutzerauthentisierung per Biometrie und/oder Passwort, kontaktorientiertes und/oder kontaktloses Interface.

Dass die europäische Bürgerkarte eine große Herausforderung für eine einheitliche technische Realisierung darstellt, zeigt sich auch darin, wie heftig über die in Frage kommenden Technologien gestritten wird. Uneinigkeit herrscht zwischen den französischen und den deutschen SmartCard Herstellern. Während die einen Java favorisieren, setzen die anderen auf die Native SmartCard. Es bleibt abzuwarten, ob am Ende tatsächlich ein europäisches Produkt herauskommt. Schließlich erlaubt die ECC Spezifikation verschiedene Ausprägungen. So werde es zum Beispiel ein deutsches und ein französisches “Profil“ geben, so Liersch in seinen Ausführungen.

SICHERE RFID-IDENTIFIKATION

Dass die Wahl der adäquaten Technik über Ländergrenzen hinweg kein leichtes Unterfangen ist, wurde auch in den Vorträgen über den Einsatz von On-Card- und Off-Card-Matching von Dr. Dirk Scheuermann vom Fraunhofer-Institut für Sichere Informationstechnologie und zum Thema Sichere RFID Identifikation von Dr. Michael Braun von der Siemens AG deutlich.

Braun erläuterte in seinem Vortrag die Vorteile elliptischer Kurven-Kryptographie und bestätigte damit die von Ingo Liersch erwähnte Tendenz zum Einsatz dieser Technik in der European Citizen Card. Um Ausweisdokumente besser vor Missbrauch zu schützen, werden biometrische Erkennungsverfahren herangezogen. Die Einbindung biometrischer Daten im Ausweis stärke die Bindung zwischen Ausweis und Ausweisinhaber, betonte Scheuermann. Während die wissensbasierte Benutzer-Verifikation über PIN und Passwort personen*bezogen* ist und diese IDs auch mal verloren gehen können, ist das biometrische Merkmal personen*gebunden* und fix.

NATIONALE AUSWEISDOKUMENTE MIT BIOMETRISCHEM ON-CARD-MATCHING

In der Biometrie unterscheidet man zwischen den „statischen“ physiologischen Merkmalen – Fingerabdruck, Gesichtsbild, Iris und Retina, Handgeometrie, Venenmuster – und den „dynamischen“ Verhaltensmerkmalen – Unterschriften-Dynamik, Tippverhalten (Keystroke), Sprache. Die ICAO schreibt für maschinenlesbare Reisedokumente (MRTDs) die Speicherung des Gesichtsbildes vor, Fingerabdruck und Iris können optional gespeichert werden. Deutschland plant die Integration des Fingerabdrucks ab 2007.

Die technischen Möglichkeiten sind gegeben – allein es fehlt der Glaube

Beim biometrischen On-Card-Matching – nach der neuen Standarddefinition inzwischen On-Card-Comparison genannt – werden die Daten der biometrischen Merkmale mit den auf der Chipkarte gespeicherten Referenzdaten verglichen. Die biometrische Verifikation findet nur auf der Karte statt. Dieses Verfahren ist insbesondere auch dann sinnvoll, wenn der Ausweis zusätzliche, individuell zu schützende Sicherheitsfunktionen enthält – Beispiel elektronische Gesundheitskarte. Beim Off-Card-Matching führt das Kontrollsystem den biometrischen Vergleich durch und entscheidet über Annahme oder Rückweisung der Person.

Noch gibt es Defizite bei den Testverfahren und der Festlegung von Standards. So gibt es standardisierte Merkmalsdaten bisher nur für den Fingerabdruck (ISO/IEC 19794-2). Standardisierte Formate für extrahierte Merkmalsdaten sind jedoch erforderlich, da komplette Bilddaten in der Karte nicht verarbeitet werden können. Technisch gesehen, so das Resümee von Dirk Scheuermann, erfüllten die modernen SmartCards die Voraussetzungen für On-Card-Matching für verschiedene Biometrien. Auch die rechtlichen Rahmenbedingungen zum Einsatz von On-Card-Matching für elektronische Signaturen seien gegeben. Da das gegenseitige Vertrauen der Staaten jedoch fehle, würde das Verfahren noch nicht für MRTDs im grenzüberschreitenden Verkehr eingesetzt.

TEST DER ELEKTRONISCHEN GESUNDHEITSKARTE UND IHRER TELEMATIK-INFRASTRUKTUR

Um für alle Beteiligten verbindliche rechtliche, organisatorische und nicht zuletzt technische Verfahren geht es auch bei der Einführung der elektronischen Gesundheitskarte (eGK). Dieter Hovemeyer von der gematik erläuterte in seinem Vortrag das umfangreiche Testverfahren als wesentliche Voraussetzung für die Zulassung der einzelnen Komponenten.

Aufgabe der gematik ist es, die Einführung der elektronischen Gesundheitskarte im Auftrag der Selbstverwaltungen des Gesundheitswesens durchzuführen sowie die Interoperabilität und den Betrieb der eGK und Telematik-Infrastruktur sicherzustellen. Das Testverfahren umfasst vier Stufen, die jeweils wiederum in vier Funktionsabschnitte unterteilt sind:

Stufe 1	Stufe 2	Stufe 3	Stufe 4
Zentraler Labortest mit einer Referenz-Muster-Umgebung	Anwendungstest – Projektumgebung mit Testdaten	10.000er Test – Feldtest mit realer Umgebung und Echtdaten; regional festgelegt mit bis zu 10.000 Teilnehmern (Ärzte, Apotheken, Krankenhäuser, Kassen) pro Region	100.000er Test – Vorstufe zum Rollout mit bis zu 100.000 Teilnehmern pro Region

In der Laborumgebung werden die Prozessabläufe über Simulation sowie zum Teil mit Realkomponenten getestet. Zum Einsatz kommen handelsübliche Multifunktionale KartenTerminals (MKT). Wenn die Simulationen nach und nach durch Realkomponenten ausgetauscht werden, könne der Test in den Regionen beginnen, so Hovemeyer. In acht ausgewählten Testregionen wird die Gesundheitskarte vor der bundesweiten Einführung in jeweils vier Funktionsabschnitten erprobt.

Im Funktionsabschnitt 1 wird die Fähigkeit der Karte getestet, die Krankenversichertendaten des Versicherten zu transportieren. Er beinhaltet ebenfalls die Speicherung der Notfalldaten sowie des elektronischen Rezeptes auf der eGK.

In Funktionsabschnitt 2 werden die Versichertendaten über einen Versichertenstammdatendienst online abgerufen und auf der Karte aktualisiert.

Funktionsabschnitt 3 ermöglicht den durchgehend elektronischen Transport apothekenpflichtiger Rezepte über einen Verordnungsdatendienst.

Funktionsabschnitt 4 beinhaltet die Speicherung von Verordnungen für Heil- und Hilfsmittel und die Arzneimitteldokumentation.

Laut Gesellschafterbeschluss vom 18. Juli 2005 ist die gematik nicht nur für die Etablierung eines einheitlichen Testverfahrens zuständig, sondern auch für „die Abnahme und Zulassung der Komponenten und Dienste der Telematik-Infrastruktur“. Verfahren hierzu sind in Vorbereitung.

Es ist noch ein weiter Weg zur eGK – die umfangreichen Tests stehen noch am Anfang

EINSATZMÖGLICHKEITEN DES HEILBERUFSAUSWEISES

Eng gekoppelt an die Einführung der elektronischen Gesundheitskarte ist der elektronische Heilberufsausweis (HBA), den Ärzte und Apotheker in diesem Fall benötigen. Georgios Raptis von der Bundesärztekammer machte auf die Besonderheiten des chipkartenbasierten HBA und das komplexe Identity Management System im Hinblick auf den turnusmäßigen Wechsel der Zertifikate aufmerksam.

Für den Zugriff auf die eGK müssen sich Arzt und Apotheker mit dem HBA identifizieren. Der Ausweis steuert auch die digitale Unterschrift des Arztes für das elektronische Rezept bei. In der Apotheke wird das elektronische Rezept eingelöst und erst gelöscht, wenn der Patient sein Medikament erhalten hat. Ohne diese Legitimation durch den HBA ist es nicht möglich, Daten von der Gesundheitskarte zu lesen oder elektronische Rezepte und medizinische Daten der freiwilligen Anwendungen, zum Beispiel Notfalldaten und Arzneimitteldokumentation, zu speichern.

Der Arztausweis verfügt über Zertifikate und Schlüssel für Authentisierung, Verschlüsselung und qualifizierte Signatur sowie über rollenspezifische Card Verifiable Certificates (CVCs) für die Authentisierung zwischen HBA und eGK. Das CVC enthält die Attribute des Besitzers des HBA. Auf Basis dieser Attribute steuert die eGK den lesenden oder schreibenden Zugriff auf die gespeicherten Daten. Die Attributsprüfung der Ärzte erfolgt durch die Landesärztekammern. Umgekehrt müssen diese auch die Karte sperren – beispielsweise im Falle des Entzugs der Approbation.

Der HBA – vielseitig aber höchst sensibel

Noch arbeitet man an Lösungsmöglichkeiten für die Zuordnung der neuen Zertifikate zu den alten Zertifikaten bei einem Kartenwechsel. Eine Option ist, dass der Zertifizierungsdiensteanbieter (ZDA) entsprechende Dienste für das Mapping anbietet, wobei zu beachten ist, dass der Datenschutz gewährleistet ist. Eine andere Option ist ein automatisiertes Mapping im Rahmen einer erneuten Registrierung.

Raptis stellte weitere Anwendungen des HBA außerhalb der Telematikinfrastruktur des Gesundheitswesens vor. So gebe es zunehmend Hersteller von Praxisverwaltungssystemen (PVS), die eigene eHealth-Plattformen als Dienstleistung anbieten. Es muss sichergestellt sein, dass die medizinischen Daten geschützt sind und nicht in die “freie Wildbahn“ des Internets gelangen können. Dies lässt sich über die Nutzung der Zertifikate auf der Karte realisieren.

Eine weiteres Einsatzgebiet ist der Austausch mit Kollegen über dedizierte Web-Portale – Foren für Ärzte, Datenübertragung von Arztbriefen, Befunden Röntgenbildern an Ärzte und Krankenhäuser. Die dahinter stehende Sicherheitstechnik ist eine Browser-basierte SSL-Client-Authentisierung mit dem AUTH-Zertifikat der Chipkarte.

Grundsätzlich sei der HBA „multiapplikativ, erweiterbar und mehrkanalfähig“, so Raptis. Da bleibt abzuwarten, inwieweit die Ärzteschaft von den vielfältigen technischen Möglichkeiten Gebrauch machen wird.

DIE EGK AUF DER SIM-KARTE IM MOBILTELEFON

Nach Zukunftsmusik hörte sich das Projekt von Vodafone an, das Christoph Reiß von der Abteilung New Business Development vorstellte: Die elektronische Gesundheitskarte auf der SIM-Karte des Handys.

Man stelle sich die SIM-Karte unterteilt in verschiedene Anwendungspartitions vor, die – so das Geschäftsmodell von Vodafone – entsprechend vermietet werden. Reiß zeigte die folgenden Anwendungsbereiche auf: POS-Systeme, Mobile Ticketing, eGovernment, Banking, Gesundheitswesen (eGK auf SIM), Zutrittskontrolle, Video und sonstige Dienstleistungen. Den Vodafone Planungen zur mobilen eGK ging eine Marktbefragung über die Einstellung zur Gesundheitskarte voraus. Das Ergebnis aus der Befragung von rd. 11.000 Teilnehmern ergab, dass knapp über 30% der Befragten es als sehr wichtig bezeichneten, bei Bedarf direkt auf die auf der Karte gespeicherten Daten zugreifen zu können. 49% gaben an, einen Zugriff über beide Medien zu bevorzugen – sowohl über das Internet als auch über das Handy. Nun soll im Oktober der erste Feldversuch in der Region Bochum / Essen starten, in dem die technischen Komponenten und deren Integration sowie die Akzeptanz der Mobilfunklösung bei den Krankenhäusern, Ärzten, Patienten, Versicherungen, Pharmaunternehmen und Verbänden geprüft werden soll. Gleichzeitig sucht Vodafone die Zusammenarbeit mit leistungsfähigen Partnern für den späteren bundesweiten Rollout.

Der Markt ist da – die technische Realisierung noch nicht ganz ausgereift

Laut einer secunet Untersuchung sind die von der Basisarchitektur geforderten Sicherheitsfunktionen der eGK auch für die mobile eGK realisierbar, so Reiß. Den spezifischen Bedrohungen der mobilen Architektur könne man durch zusätzliche Maßnahmen, darunter die NFC-Zugangsautorisierung durch den Benutzer, entgegenwirken.

Near Field Communication (NFC) steht für drahtlose Nahfunkübertragung für Datenverbindungen über kurze Strecken (< 5 cm) mit sehr schnellem Verbindungsaufbau (~0,1s) zwischen den Kommunikationspartnern. Hierzu werden zwei sehr kleine Chips integriert - ein Funkchip und ein SecureChip, auf welchem die Anwendungsdaten sicher gespeichert werden.

Ungeklärt ist die Problematik der optischen Merkmale (Lichtbild, Unterschrift, europäische Rückseite) und die Frage der notwendigen Zulassung. Zwecks Einbindung der Technologie und der damit verknüpften Sicherheitsfragen in die Spezifikationen sollen Gespräche mit der gematik aufgenommen werden.

Noch gibt es viel zu tun, bis das Geschäftsmodell eGK mobil Früchte trägt und dem Unternehmen die gewünschten Umsätze generiert – denn dies ist nicht zuletzt das Ziel von Reiß´ New Business Development Abteilung.

DIE TUD CHIPKARTE

Weitere Referate widmeten sich dem Elektronischen Führerschein und der Chipkarte für Studierende und Bedienstete der TU Darmstadt.

Der Rollout von 18.000 multifunktionalen Studenten-Chipkarten, die die Funktion der digitalen Identität und eines modernen bargeldlosen Zahlungsmittels miteinander vereinen, konnte nach nur 18 Monaten Projektdauer erfolgen mit dem erstaunlichen Ergebnis, dass – nur – 5.500 Karten aktiviert wurden. Da bleibt abzuwarten, wie die Bediensteten auf die Karte reagieren, die sich aktuell im Rollout befindet.

Über CAST – Competence Center for Applied Security Technology

Das CAST-Forum bündelt die Kompetenzen der Abteilung Sicherheitstechnologie für Graphik und Kommunikationssysteme am Fraunhofer-IGD mit dem Fachgebiet Kryptographie, Computeralgebra und Verteilte Systeme an der TUD und dem Institut für Sichere Informationstechnologie Fraunhofer-SIT. Es versteht sich als offenes Netzwerk von Kompetenzträgern, an das industrielle Partner sowie eine Reihe von kleinen und mittleren Unternehmen angeschlossen sind. Zielsetzung des Forums ist es, den Transfer von Technologie und Know-How zwischen Forschung und Praxis über ein breites Dienstleistungsangebot im Bereich der Sicherheit moderner Informationstechnologien zu realisieren. Das Angebot umfasst Aus- und Weiterbildung, Bereitstellung von Beratungskompetenz, Evaluierung von Sicherheitslösungen, sowie den Austausch und Zugang zu Forschung und Entwicklung.

Kontakt:

Marlene Neudörffer
marlene neudoerffer | communications
Im Fasanengarten 11b
D-64342 Seeheim-Jugenheim
Tel.: +49 (0) 6257- 6 94 12
E-Mail: marlene.neudoerffer@mn-communications.de

Ulrich Pinsdorf
Competence Center for Applied Security Technology
CAST e.V.
Fraunhoferstraße 5
D-64283 Darmstadt
Tel.: +49 (0) 6151-155 533
E-Mail: ulrich.pinsdorf@cast-forum.de