Die eCard-Strategie der Bundesregierung im Überblick

Bernd Kowalski

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, D-53175 Bonn
bernd.kowalski@bsi.bund.de

Abstract: Die eCard-Strategie zielt auf die Harmonisierung der unterschiedlichen Projekte der Bundesregierung ab, die Chipkarten (eCards) mit Authentisierungs- und Signaturfunktion herausgeben oder nutzen. Der vorliegende Beitrag liefert einen kompakten Überblick über die wesentlichen Aspekte der eCard-Strategie.

1 Einleitung

Das Bundeskabinett hat am 9. März 2005 die Eckpunkte für eine gemeinsame eCard-Strategie beschlossen [Bundesreg05]. Wesentliche Stützpfeiler dieser Strategie sind die elektronische Authentisierung und die qualifizierte elektronische Signatur, die auf Chipkarten unterschiedlicher Ausprägung zum Einsatz kommen.

Für die eCard-Strategie sind insbesondere die folgenden Projekte, die in Abschnitt 2 näher beleuchtet werden, von Bedeutung:

- Die elektronische Gesundheitskarte (eGK)
- Der elektronische Personalausweis (ePA)
- Der elektronische Reisepass (ePass)
- Die elektronische Steuererklärung (ELSTER)
- Der elektronische Einkommensnachweis (ELENA/Jobcard)

Darüber hinaus berücksichtigt die eCard-Strategie weitere in Deutschland ausgegebene Chipkarten mit großer Wirkbreite, wie beispielsweise die ec-Karten der deutschen Banken, den elektronischen Dienstausweis, die elektronische Aufenthaltskarte sowie Chipkarten im Verkehrs- und Mobilfunkbereich. Schließlich finden auch wichtige ausländische Chipkartenprojekte (vgl. [BHK07]) sowie internationale Standardisierungsbestrebungen – beispielsweise die European Citizen Card [prCEN15480] (vgl. [MeDa07]) und ISO/IEC 24727 - entsprechende Beachtung.

Bei der Realisierung der eCard-Strategie spielt das eCard-API-Framework [eCard-API-TR] eine wichtige Rolle, da hierdurch die unterschiedlichen Applikationen auf die unterschiedlichen Chipkarten über einheitliche Schnittstellen zugreifen können. Deshalb soll in Abschnitt 3 die Architektur des eCard-API-Frameworks grob vorgestellt werden. In Abschnitt 4 werden die wesentlichen Aspekte des vorliegenden Beitrags zusammengefasst und ein Ausblick auf zukünftige Entwicklungen gewagt.

2 Die wesentlichen Projekte der eCard-Strategie

2.1 Die elektronische Gesundheitskarte (eGK)

Um die Wirtschaftlichkeit und Leistungstransparenz im Gesundheitswesen zu steigern und die Arbeitsprozesse sowie die Bereitstellung von aktuellen gesundheitsstatistischen Informationen zu optimieren, werden die bisherigen 80 Millionen Krankenversichertenkarten schrittweise durch elektronische Gesundheitskarten ersetzt (siehe [BMG07], [gematik07]). Für den Zugriff auf die sensiblen auf der eGK oder in den Serversystemen der Telematikinfrastruktur gespeicherten medizinischen Daten ist neben der Einwilligung der Versicherten ein Heilberufsausweis nötig. Seit Ende 2006 laufen erste Feldtests mit der elektronischen Gesundheitskarte (vgl.[BMG06]).

2.2 Der elektronische Personalausweis (ePA)

Neben der elektronischen Gesundheitskarte spielt der elektronische Personalausweis (ePA) (vgl. [RRM05] und [Scha07], Abschnitt 3) für die eCard-Strategie eine wesentliche Rolle. Der ePA wird hierbei der grundlegenden Kartenspezifikation der European Citizen Card [prCEN15480] und einem ePA-spezifischen Anwendungsprofil (vgl. [MeDa07]) genügen und somit neben der Funktionalität zur Speicherung biometrischer Merkmale analog zum ePass (vgl. Abschnitt 2.3) insbesondere auch generische Funktionen zur Authentisierung und Signatur bereitstellen. Unter Verwendung der in [EAC-TR] definierten Protokolle (z.B. Password Authenticated Connection Establishment (PACE), Chip Authentication (CA) und Terminal Authentication (TA)) kann der ePA beispielsweise zur sicheren und datenschutzfreundlichen Authentisierung an einem Bürgerportal genutzt werden.

2.3 Der elektronische Reisepass (ePass)

Seit dem 01. November 2005 werden in Deutschland Reisepässe ausgegeben, auf denen biometrische Merkmale gespeichert sind (vgl. [ePass] und [Scha07], Abschnitt 3). Für den standardisierten Zugriff auf den elektronischen Reisepass wurde die ePassport-API entwickelt, die als Grundlage für die Entwicklung des eCard-API-Frameworks [eCard-API-TR] diente und perspektivisch von dieser ersetzt werden kann. Somit ist gewährleistet, dass auch das Golden Reader Tool und die in [NBS07] beschriebene biometrische Middleware auf Basis der BioAPI 2.0 das eCard-API-Framework nutzen können.

2.4 Die elektronische Steuererklärung (ELSTER)

Seit Anfang 2005 müssen Umsatzsteuer-Voranmeldungen und Lohnsteuer-Anmeldungen elektronisch erfolgen. Hierfür wurde im Auftrag der Finanzverwaltung eine neue Sicherheitsplattform für das ElsterOnline-Portal [ELSTER] realisiert, die die Authentisierung, Verschlüsselung und elektronische Signatur für Web-Anwendungen über verschiedene zertifikatsbasierte Verfahren mit beliebigen Chipkarten über die [PKCS#11]-Schnittstelle unterstützt. Zukünftig wird der Zugriff auf die verschiedenen Chipkarten über das eCard-API-Framework geschehen (vgl. [Rand07]). Außerdem sollen zukünftig die im ELSTER-Projekt ausgestellten Zertifikate und die eingesetzte Sicherheitstechnologie auch von anderen Behörden für Ihre (eGovernment-) Zwecke genutzt werden können („OpenElster“).

2.5 Der elektronische Einkommensnachweis (ELENA)

Der elektronische Einkommensnachweis (ELENA), vormals Jobcard-Verfahren [Jobcard], ist ein weiteres wichtiges Anwendungsgebiet von Signaturkarten. Ziel des Projektes ist die Entlastung der Arbeitgeber von der Ausstellung papierbezogener Bescheinigungen (zum Beispiel Verdienstbescheinigungen) und die Modernisierung von Verwaltungsabläufen. Hierbei handelt es sich allerdings nicht um ein Projekt, in dem eine spezielle Karte (wie die elektronische Gesundheitskarte oder der elektronische Personalausweis) ausgegeben werden soll. Statt dessen ist geplant - unter Verwendung des eCard-API-Frameworks - beliebige Signaturkarten mit qualifiziertem Zertifikat nutzen zu können

3 Das eCard-API-Framework im Überblick

Das Ziel des eCard-API-Frameworks [eCard-API-TR] ist das Bereitstellen einer einfachen und homogenen Schnittstelle, um in den verschiedenen Anwendungen eine einheitliche Nutzung der unterschiedlichen Chipkarten zu ermöglichen.

Der Aufbau des eCard-API-Frameworks ist in Abbildung 1 dargestellt. Hieraus wird ersichtlich, dass sich das eCard-API-Framework in die vier folgenden Ebenen untergliedert:

- Application-Layer
- Identity-Layer
- Authentication-Layer
- Terminal-Layer

Die wesentlichen Aspekte der verschiedenen Schichten sollen im Folgenden kurz beleuchtet werden. Für weitere Details sei auf [HBO07], [HüBa07a] und [eCard-API-TR] verwiesen.

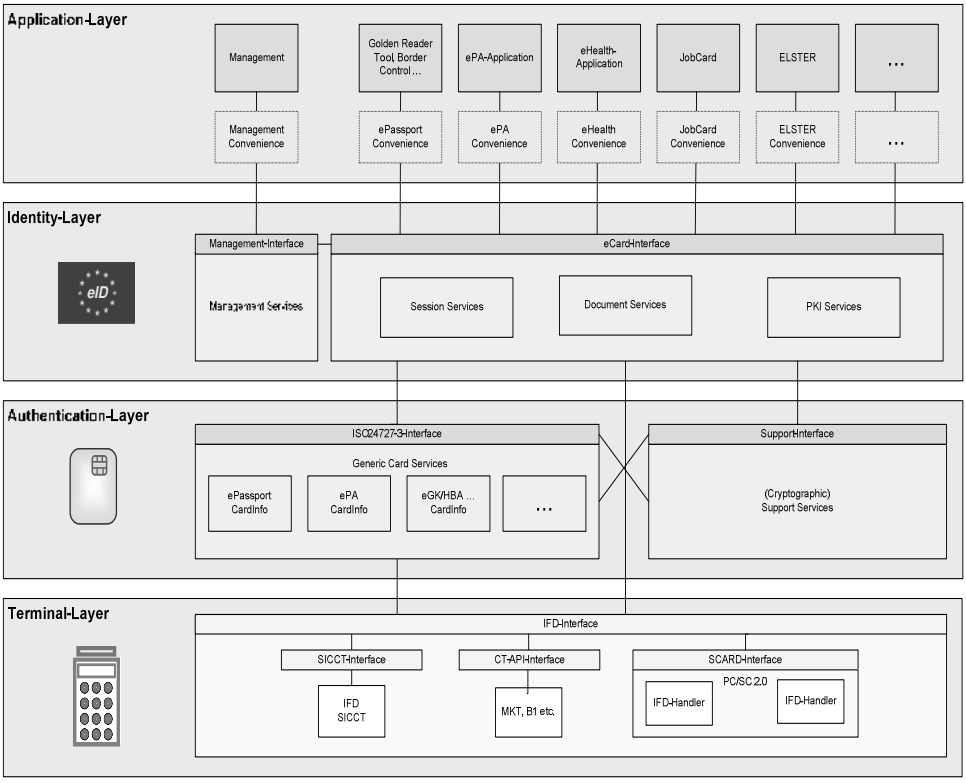

Abbildung 1: Die Architektur des eCard-API-Frameworks

3.1 Application-Layer

Im Application-Layer befinden sich die verschiedenen Anwendungen, die das eCard-API-Framework für den Zugriff auf die eCards und damit verbundene Funktionen nutzen wollen. In dieser Schicht können auch weitere anwendungsspezifische „Convenience-Schnittstellen“ existieren, in denen wiederkehrende Aufruffolgen in applikationsnahen Aufrufen gekapselt werden. Diese Schnittstellen sind jedoch derzeit *nicht* Gegenstand des eCard-API-Frameworks.

3.2 Identity-Layer

Der Identity-Layer umfasst das in Teil 2 bzw. Teil 3 des eCard-API-Frameworks spezifizierte eCard-Interface und das Management-Interface, welche von der Anwendung bei entsprechender Berechtigung als öffentliche Schnittstelle genutzt werden können.

Das *eCard-Interface* stellt die wesentlichen Funktionen des eCard-API-Frameworks in einer anwendungsnahen Art und Weise bereit und bietet insbesondere Funktionen für den Aufbau von gesicherten Netzwerkverbindungen und für den Schutz von Dokumenten mittels Signatur und Verschlüsselung.

Im *Management-Interface* werden wesentliche Management-Funktionen abgebildet. Hierzu gehört das Verwalten von vertrauenswürdigen Zertifikaten, Identitäten, Chipkarten, Kartenterminals und des Default-Verhaltens.

3.3 Authentication-Layer

Der Authentication-Layer bietet insbesondere Funktionen für kryptographische Primitive und biometrische Mechanismen in Verbindung mit kryptographischen Token und umfasst das ISO24727-3-Interface und das Support-Interface.

Das in Teil 4 des eCard-API-Frameworks definierte *ISO24727-3-Interface* ist eine Webservice-basierte Umsetzung des gleichnamigen Standards [ISO24727-3] und bietet eine generische Schnittstelle für alle kartenbasierten Funktionen der verschiedenen eCards.

Das *Support-Interface* ([eCard-API-TR], Teil 5) enthält eine Reihe von unterstützenden (kryptographischen) Funktionen, die nicht auf einer eCard ausgeführt werden.

3.4 Terminal-Layer

Der Terminal-Layer enthält im Wesentlichen das in Teil 6 des eCard-API-Frameworks definierte *IFD-Interface* (vgl. prCEN 15480-3 und ISO/IEC 24727-4). Dieses übernimmt die Generalisierung von konkreten Lesertypen und verschiedenen Schnittstellen sowie die Kommunikation mit der Chipkarte. Für den Anwender ist es somit weder von Bedeutung, ob die eCard via [PC/SC], einem [SICCT]-Leser oder einem herstellerspezifischen Interface angesprochen wird, noch spielt es eine Rolle, ob die Karte kontaktbehaftet oder kontaktlos ist.

4 Zusammenfassung und Ausblick

Dieser Beitrag lieferte einen kompakten Überblick über wichtige Aspekte der eCard-Strategie der Bundesregierung. Neben den wesentlichen Projekten der eCard-Strategie wurde auch die Architektur des eCard-API-Frameworks kurz skizziert, durch welches die verschiedenen Applikationen in einheitlicher Weise auf die verschiedenen Chipkarten zugreifen können. Um die einfache und einheitliche Nutzung der eCards auch über die Grenzen der Bundesrepublik Deutschland hinaus zu ermöglichen, wird das eCard-API-Framework derzeit der internationalen Normung zugeführt und in europaweite Projekte für grenzüberschreitendes eGovernment eingebracht (vgl. [Leym07], [HüBa07b]).

Literaturverzeichnis

[BHK07] B. Bruegger, D. Hühnlein, M. Kreutzer: *Towards global eID-Interoperability*, im vorliegenden Tagungsband

[BMG06] Bundesministerium für Gesundheit: *Start der 10.000er-Testphase in der Region Flensburg: Die Ausgabe der ersten Gesundheitskarten hat begonnen*, Pressemitteilung vom 11.12.2006, via http://www.die-gesundheitskarte.de/presse/pressemitteilungen/2006/pm_2006-12-11_ausgabe_gesundheitskarte.html

[BMG07] Bundesministerium für Gesundheit: *Die elektronische Gesundheitskarte*, via http://www.bit4health.de , 2007

[Bundesreg05] Bundesregierung: *eCard-Strategie der Bundesregierung*, Pressemitteilung vom 09.03.2005, via http://www.bmwi.de/Navigation/Presse/pressemitteilungen,did=60006.html , 2005

[prCEN15480] Comité Européen de Normalisation (CEN): *Identification card systems — European Citizen Card — Part 1-4*, 2007

[eCard-API-TR] Bundesamt für Sicherheit in der Informationstechnik: *eCard-API-Framework – Technische Richtlinie des BSI - TR-03112*, Teil 1 – 6, 2007

[EAC-TR] Bundesamt für Sicherheit in der Informationstechnik: *Advanced Security Mechanisms for Machine Readable Travel Documents Extended Access Control (EAC) - Technische Richtlinie des BSI - TR-03110*, *Version 2.0,* 2007

[ELSTER] Bayrisches Landesamt für Steuern: *ELSTER – die elektronische Steuererklärung*, https://www.elster.de, 2007

[ePass] Bundesamt für Sicherheit in der Informationstechnik: *ePass Der Reisepass mit biometrischen Merkmalen*, via http://www.bsi.bund.de/fachthem/epass/index.htm

[gematik07] Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH – *Homepage*, via http://www.gematik.de

[HBO07] D. Hühnlein, M. Bach, R. Oberweis: *Das eCard-API-Framework*, Tagungsband zum 10. Deutschen IT-Sicherheitskongress, SecuMedia, ISBN 978-3-922746-98-0, 2007, Seiten 51-62

[HüBa07a] D. Hühnlein, M. Bach: *How to use ISO/IEC 24727-3 with arbitrary smart cards*, erscheint bei TrustBus'07, Springer, 2007

[HüBa07b] D. Hühnlein, M. Bach: *From the eCard-API-Framework towards a comprehensive eID-Framework for Europe*, erscheint bei ISSE 2007, Vieweg, 2007

[ISO24727-3] ISO/IEC: *Identification Cards — Integrated Circuit Cards Programming Interfaces — Part 3: Application Interface*, ISO/IEC 24727-3, Committee Draft (2006-09-07), 2006

[ISO24727-4] ISO/IEC: *Identification Cards — Integrated Circuit Cards Programming Interfaces — Part 4: API-Administration*, ISO24727-4, Working Draft (2007-01-08), 2007

[Jobcard] ITSG Informationstechnische Servicestelle der gesetzlichen Krankenversicherung GMBH: *Das JobCard-Verfahren*, via http://www.itsg.de/download/BroschuereJobcard.pdf , 2004

[Leym07] F. Leyman: *e-ID interoperability large scale pilot – STORK*, Vortrag bei EEMA-Konferenz "The European e-Identity Conference", Paris, Juni 2007

[MeDa07] G. Meister, H. Daum: *Anwendungsprofile der European Citizen Card*, im vorliegenden Tagungsband

[NBS07] M. Nuppeney, M. Breitenstein, F. Steffens: *Biometrische Middleware basierend auf BioAPI 2.0*, im vorliegenden Tagungsband

[PC/SC] PC/SC Workgroup: *PC/SC Workgroup Specifications 1.0/2.0*, via http://pcscworkgroup.com

[PKCS#11] RSA Labs: *PKCS#11: Cryptographic Token Interface Standard*, Version 2.11, via http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/index.html

[Rand07] C. Randlkofer: *Die elektronische Steuererklärung (ELSTER) - Status und Ausblick – OpenElster*, im vorliegenden Tagungsband

[RRM05] H. Reichl, A. Roßnagel, G. Müller (Hrsg.): *Digitaler Personalausweis – Eine Machbarkeitsstudie*, Deutscher Universitätsverlag, ISBN: 3835000543, 2005

[Scha07] M. Schallbruch: *Sicherheitspolitik und Verwaltungsmodernisierung: Hand in Hand*, Tagungsband zum 10. Deutschen IT-Sicherheitskongress, SecuMedia, ISBN 978-3-922746-98-0, 2007, Seiten 189-198

[SICCT] TeleTrusT e.V.: *Secure Interoperable ChipCard Terminal (SICCT)*, Version 1.1.0 vom 19.12.2006, via http://www.teletrust.de/fileadmin/files/publikationen/Spezifikationen/SICCT_Spezifikation_1.10.pdf