

eCard-Strategie der Bundesregierung



Bernd Kowalski

Bundesamt für Sicherheit in der Informationstechnik

Berliner Signaturkonferenz

28. Februar 2007

Ziele der Bundesregierung (1)

- ❑ Abgestimmte **Einführung der eCard-Projekte** des Bundes.
- ❑ **Einheitliche Nutzung** von Chipkarten im eGovernment, eBusiness und im elektronischen Rechtsverkehr.
- ❑ Elektronische Dienstleistungen sollen **einfach, kostengünstig und sicher** sein.
- ❑ **Schub** für den elektronischen Geschäftsverkehr.
- ❑ Beitrag zur **Modernisierung der öffentlichen Verwaltung**, des Arbeits-, Sozial- und Gesundheitswesens.



Ziele der Bundesregierung (2)

Eckpunkte des Kabinettsbeschlusses vom 9.03.2005

- ❑ **Interoperable Sicherheitsfunktionen** Signatur und Authentisierung **für alle Chipkarten**, alle Anwendungen und alle Marktteilnehmer.
- ❑ Die Karten-emittierenden Projekte stellen ihre Karten mit einer **optional aktivierbaren Qualifizierten Signatur (QS)** aus.
- ❑ Alle **eGovernment-Anwendungen** akzeptieren **für die QS die einheitlichen Standards** des Signaturlbündnisses bzw. der eCard-Strategie.
- ❑ Verwaltungsverfahren für die Nutzung elektronischer Prozesse vorbereiten, d.h. **Formerfordernisse prüfen und abbauen**.
- ❑ Herstellung und Bereitstellung **interoperabler Karten und Zertifikate (Trust Center)** sind Aufgabe der Privatwirtschaft.

eCard-Projekte des Bundes (2)

- ❑ **eGK** - elektronische Gesundheitskarte für 80 Mio. Patienten plus Heilberufeausweis (HBA) für etwa 500 Tsd. Leistungserbringer, Einführungsjahr 2006, zuständig: BMG.
- ❑ **ePA** - Digitaler Personalausweis für 80 Mio. Bundesbürger, geplante Einführung 2008, zuständig: BMI.
- ❑ **eLena (JobCard)** - Anwendung für >30 Mio. Arbeitnehmer, zuständig: BMWi.
- ❑ **ELSTER** - Elektronische Steuererklärung, zuständig: BMF.

Weitere Kartenprojekte großer Wirkbreite

- ❑ ec-Karten der deutschen Banken, ePass, Digitaler Dienstausweis, elektronischer Fahrtenschreiber, EU-Mautkarten, ÖPNV / VdV-Karten.

Elektronischer Reisepass „ePass“



- VERORDNUNG (EG) Nr. 2252/2004 des Rates der EU vom 13. Dezember 2004. Zwei Stufen:
 - elektronische Ausweisfunktion incl. Gesichtsbild
 - + zwei Fingerabdruckbilder
- Europäische Spezifikation basiert auf technischen Empfehlungen der International Civil Aviation Organization
- elektronische Ausweisfunktion (personenbezogene Daten, Gesichtsbild [JPEG]).
- Kontaktlose RF-Schnittstelle nach ISO 14443.
- Die Bundesdruckerei produziert den ePass seit dem 01.11.2005.
- Zusätzlich 2 Fingerabdruckbilder ab dem 1.11.2007 in Deutschland.

ePA-Sicherheitsfunktionen



Optische Authentisierung – klassische Ausweisfunktion

- ❑ Staatlicher Bereich (Grenzübertritt, polizeiliche Kontrollen)
- ❑ Bereich der Wirtschaft (Kontoeröffnung, Hotelaufenthalt)

Biometrische Verifikationsmöglichkeit - neue Funktion

Online Authentisierung – neue Funktion

- ❑ E-Government-Anwendungen (Steuer, Antragsverfahren).
- ❑ E-Business-Anwendungen, z.B. Altersverifikation.

Qualifizierte elektronische Signatur – optionale Funktion

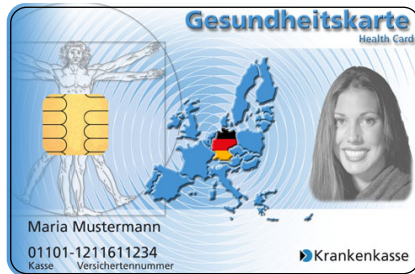
- ❑ Elektronisches Äquivalent zur eigenhändigen Unterschrift.



Elektronische Gesundheitskarte „eGK“

Sicherheitskomponenten

- ❑ **eGK** - Versichertenkarte für 80 Mio. Versicherte. Sie löst die KVK ab und enthält:



- ❑ Administrative Daten
 - ❑ elektronisches Rezept
 - ❑ Patientennotfalldaten, Medikamentierung
 - ❑ qualifizierte Signatur (Option)
- ❑ **HBA/HPC** - Heilberufeausweis für ca. 500 Tsd. Leistungserbringer im Gesundheitswesen.
 - ❑ **SMC** - Institutionskarte zur Nutzung durch autorisierte Hilfskräfte bei einem Leistungserbringer.
 - ❑ **Konnektor** - Netz- und Anwendungszugang zur zentralen Telematik-Infrastruktur beim Leistungserbringer.

Realisierung der QES-Option für eGK (und ePA)

Qualifizierte elektronische Signatur als Option heißt:

- ❑ Karte ist mittels eines „Sicherheitsankers“ für die QES „vorbereitet“.
- ❑ Ein qualifiziertes Zertifikat wird erst nach dem Roll Out der Karte aufgebracht.
- ❑ Alle ZDA müssen vorab vertragliche Vereinbarungen zur Nachladung der QES mit allen Kartenherausgebern abschließen.

Vorteil:

- ❑ Eine eigene Kartenemission für jede Anwendung einer qualifizierten Signatur ist nicht mehr erforderlich. Vielmehr nutzen diese Anwendungen die QES-Funktion von bereits emittierten Karten, z. B.: ePA, eGK.

Technische Anforderungen an eCard-API und eCard-Middleware

□ Anforderungen aus eCard-Projekten

- Unterstützung der Funktionalität von eGK, HBA und SMC (u.a. „Trusted Channel“ für z.B. CAMS, QES-Aktivierung im Feld, SICCT-Leser)
- Unterstützung der Funktionalität des ePass und ePA (u.a. BAC, EAC, EC-Crypto, auch ISO14443)
- Unterstützung beliebiger Signaturkarten (für ELSTER und eLena)
- Unterstützung von High-Level-PKI- und Signaturfunktionen

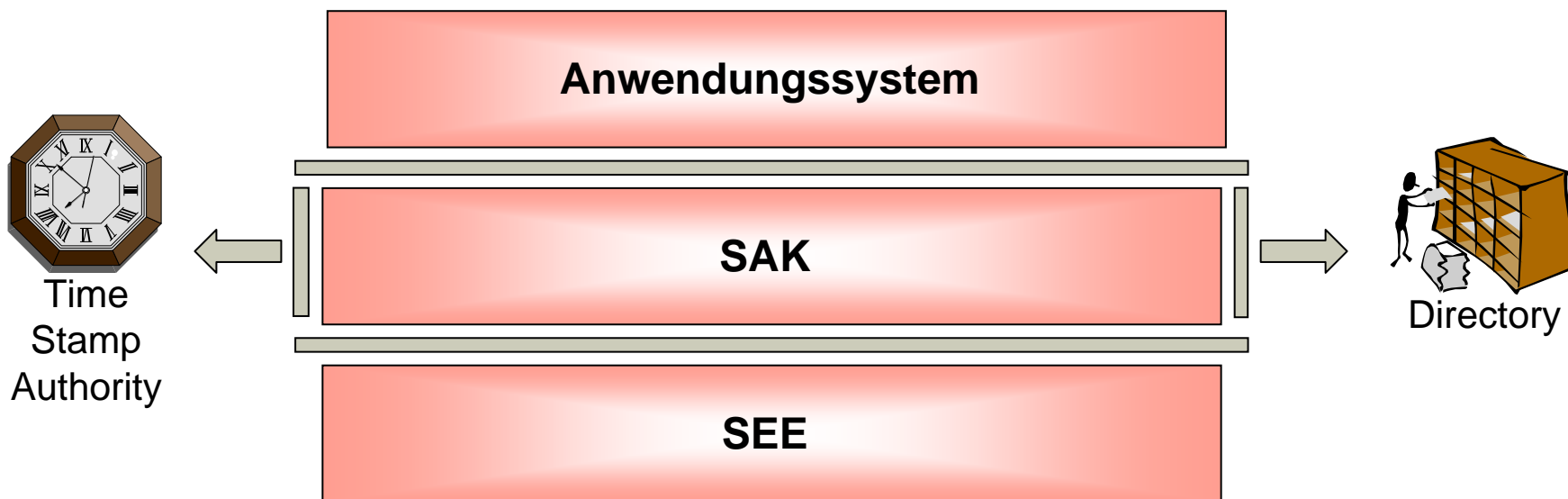
□ Sicherheit und Evaluierbarkeit

□ Plattformunabhängigkeit (Java, C auf diversen OS)

□ Skalierbarkeit (Einplatzsystem, mobile Geräte, Serverumgebung)

□ Kompatibilität zu ISO u. existierenden Lösungen im Markt (Microsoft)

SigG-relevante Komponenten im eCard-Framework



Existierende APIs

Anwendungssystem

Java XML Digital Signature API

SAP Secure Store and Forward (SSF) API

Microsoft CryptoAPI

CCES-Signature-API

Acrobat Digital Signature API

Generic Security Services API (GSS-API)

GSS-Independent Data Unit Protection (GSS-IDUP)

Generic Cryptographic Service API (GCS-API)

Simple Cryptographic Program Interface (Crypto API)

VPS Document Interface

SAK

ePassport-Crypto-API

Microsoft CryptoSPI

Java Cryptographic
Architecture (JCA)
und Extension (JCE)

Common Data Security
Architecture / Common Security
Services Manager (CDSA / CSSM)

US Government SC Interoperability Specification (GSC-IS)

PKCS#11

Open Card Framework (OCF)

ISO 24727

SASCIA

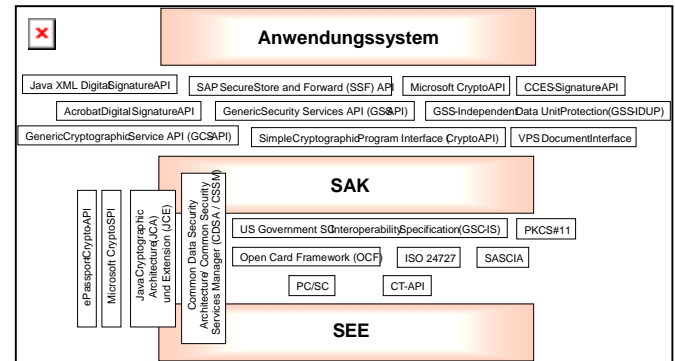
PC/SC

CT-API

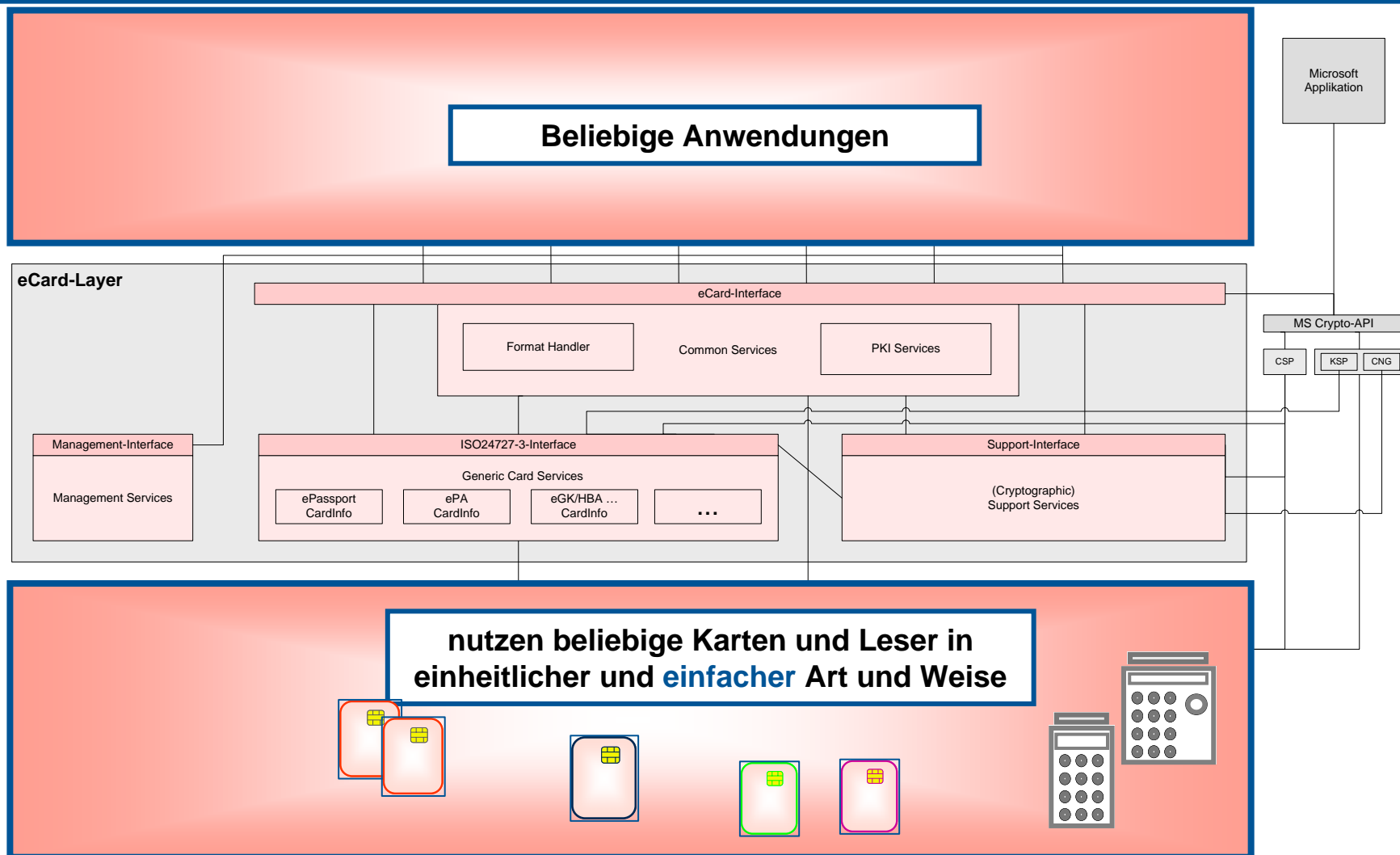
SEE

Existierende APIs ...

- Decken jeweils nur einen Teilbereich der notwendigen Funktionalität ab
 - Keine Kompatibilität
 - Keine Plattform-Unabhängigkeit
 - Jeder ZDA hat eigene Lösung
 - Erfordern die Änderung des ausführbaren Codes in der Middleware zur Unterstützung einer neuen Karte
 - hoher Aufwand durch RE-Evaluierung
 - Hoher Integrationsaufwand
 - Unverträglichkeit koexistierender SAKs,
z. B. bei gleichzeitiger Nutzung unterschiedlicher Kartentypen
- Erschweren die Verbreitung der Kartenanwendungen des Bundes**



Das Ziel



Wesentliche Eigenschaften des eCard-API-Framework

- ❑ **Unterstützung beliebiger Karten ohne Änderung** des ausführbaren Codes
- ❑ **Leichte Integration in Anwendungen** (“High-Level“-API)
- ❑ **Plattformunabhängig** und skalierbar (Webservice-Schnittstellen)
- ❑ Unterstützung und Abstraktion von **verschiedenen Kartenterminal-Technologien** (PC/SC, SICCT, Klasse 1-3, ISO 14443, NFC)
- ❑ Berücksichtigt wesentliche **Standards** im eCard-Umfeld und z.B. Microsoft’s (CNG) CryptoAPI
 - ❑ Z.B. CEN/CWA 14171, CEN/CWA 14890, ETSI TS 101733, ETSI TS 101903, (Ziel:), OASIS Digital Signature Service, PC/SC, RFC2560, RFC3161, SICCT und XML-Encryption
- ❑ Derzeit erfolgt Abstimmung mit aktuellen Standardisierungsaktivitäten (z.B. ISO24727 und prCEN/TS 15480)

eCard-API - Die nächsten Schritte

- ❑ Erstellung der eCard-API-Spezifikationen als **Technische Richtlinie**
--> derzeit i.d. Abstimmung mit gematik und DIF (bis Ende März 07)
- ❑ **Abstimmung** mit Vertretern von Behörden, Wirtschaft und Verbänden (bis Ende April 07)
- ❑ Bereitstellung von **Prüfkriterien und Testtools** durch das BSI (bis September 07)
- ❑ **Internationale Standardisierung** über CEN TC224 WG15 (fortlaufend), später auch ISO

eCard-Strategie

Zusammenfassung

- ❑ Mit ePass, ePA / eAK und eGK **setzt der Bund Standards** in einem signifikant großen Marktbereich.
- ❑ Konkurrierende technische Schnittstellen werden vermieden.
- ❑ Die technische Umsetzung der **QES wird wesentlich vereinfacht**.
- ❑ **Reduktion der Integrations- und Evaluationskosten** für die SAK.
- ❑ **Aktuelle technologische Entwicklungen**, wie z.B. kontaktlose Karten / Leser inkl. NFC werden berücksichtigt.
- ❑ Die **Nutzung von ePA, eGK und eCard-MW** durch andere Anwendungen **wird einfach** und kostengünstig.

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)



Bernd Kowalski
Godesberger Allee 185 - 189
53175 Bonn

Tel: 0228-9582-5700
Fax: 0228-99-10-9582-5700

Bernd.Kowalski@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de