

media transfer AG

Dolivostr. 11
64293 Darmstadt

www.mtg.de



eCard-PKI

Eine sichere, vertrauenswürdige PKI zur Akzeptanz der eCard-Projekte durch Bürger und Behörden

14. Anwenderforum E-Government, Berlin
12./13. Februar 2008

Erik Neumann, eneumann@mtg.de
media transfer AG, Darmstadt

eCard-Projekte

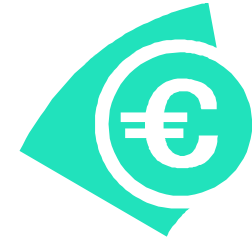
- ePass: elektronischer Reisepass
 - Biometrie
 - kontaktlos
- ePA: elektronischer Personalausweis (auch eID)
 - kommerzielle Nutzung eines Ausweisdokuments
- eGK: elektronische Gesundheitskarte
 - u.a. Notfalldaten, aktuell verordnete Medikamente
 - im Umfeld: eRezept, Arztausweis (HBA), elektronische Patientenakte
- eSign: qualifizierte elektronische Signatur
 - Einsatz bei eGK, ELSTER, eLena usw.
- weitere Einsatzszenarien
 - EC-Karten, ÖPNV usw.

Gemeinsamkeiten der eCard-Projekte

- Bekenntnis zur Chipkarte als Security Token
 - bekanntes (beliebtes) Kreditkartenformat
 - auch kleinere SIM-Karte möglich
 - kostengünstig
- „Der Bürger“ als Zielpublikum
 - sehr große Stückzahlen
 - hohe Anforderungen an Stabilität
 - Bedienbarkeit: Technik muss transparent sein
- Behörden, Privatwirtschaft und weitere Organisationen beteiligt
 - schwierige Abstimmungsprozesse
 - zum Teil widersprüchliche Interessen

Vertrauensanforderungen

- Staat in der Verantwortung
 - Bürger ist hohes Sicherheitsniveau gewohnt
 - Staat ist an den Daten und ihrer zentralen Haltung interessiert
 - technische und organisatorische Vorgaben
- Bürgerinteressen
 - Datenschutz, Vertraulichkeit und Schutz vor Missbrauch
 - Haltbarkeit
 - „sicheres Gefühl“
- Behörden, Institutionen, Industrie
 - Fälschungssicherheit
 - Prozesse und Bedienbarkeit
 - Gesetzgebung (u.a. Verbindlichkeit, Haftung)



Das Vertrauen wird bereits belastet!

- Komplexität
- öffentliche Abstimmungsprozesse
- Nutzung der Medien zur Durchsetzung von Interessen
- Terminverschiebungen
- schlechte Vorbilder im Ausland, teilweise auch im Inland
- Henne-Ei-Problem

Datenschutz?

Bezahlbar?

Zuverlässig?

Machbar?

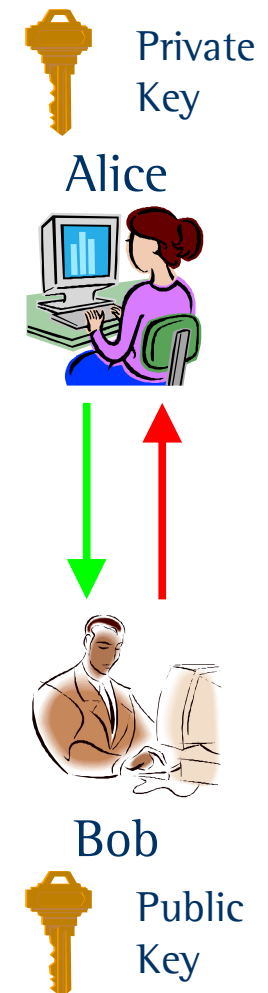
Profile?

Betrachtete Anforderungen

- Vertraulichkeit
 - Daten sind nur berechtigten Personen/Institutionen zugänglich
 - Kommunikation wird ausreichend abgesichert
- Fälschungssicherheit
 - Fälschung und Verfälschung müssen erkannt werden können
 - Resultat ist „Nicht-Abstreitbarkeit“
- Schutz vor Missbrauch
 - Besitz und Wissen zur Nutzung notwendig
 - bei Verlust können geheime Daten nicht ausgelesen werden
 - bei Verlust können geheime Daten nicht genutzt werden
 - Karte kann vollständig gesperrt werden

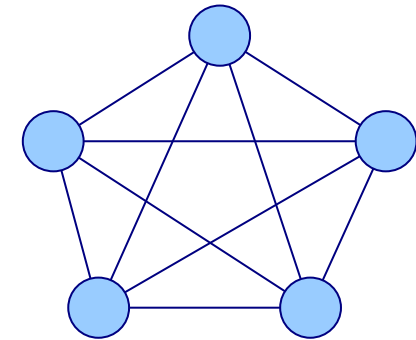
PKI: Schlüsselpaare

- 2 Schlüssel (asymmetrische Schlüssel)
 - Beide Schlüssel eignen sich zum Verschlüsseln.
 - Es wird der jeweils andere Schlüssel zum Entschlüsseln benötigt.
 - Privater Schlüssel verbleibt beim Besitzer
 - Öffentlicher Schlüssel wird ungeschützt bereitgestellt
- Anwendung
 - Verschlüsselung (mit dem öffentlichen Schlüssel)
 - Signatur (mit dem Privaten Schlüssel verschlüsselte Prüfsumme)
- Sicherheit
 - Verfahren mathematisch gesehen sicher
 - Praktische Sicherheit abhängig von der Schlüssellänge
 - Schlüssellängen müssen regelmäßig angepasst werden



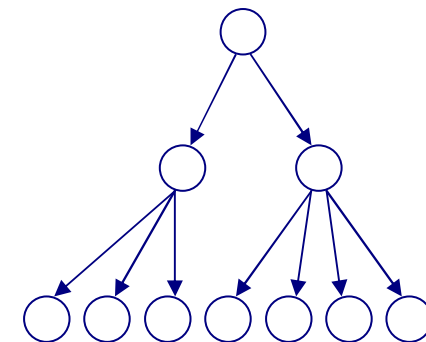
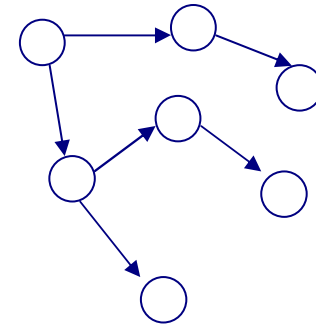
PKI: Zertifikate

- Schlüsselverteilung
 - Kernproblem der sicheren Infrastruktur
 - Asymmetrische Schlüssel lösen Verteilungsproblem
 - Aber woher weiß ich, von wem der öffentliche Schlüssel stammt?
- Zertifikat
 - Verknüpfung einer Identität mit einem öffentlichen Schlüssel
 - Datensatz aus
 - Beschreibung der Identität
 - Öffentlicher Schlüssel
 - Signatur einer vertrauenswürdigen Instanz



PKI: Zertifikatshierarchie

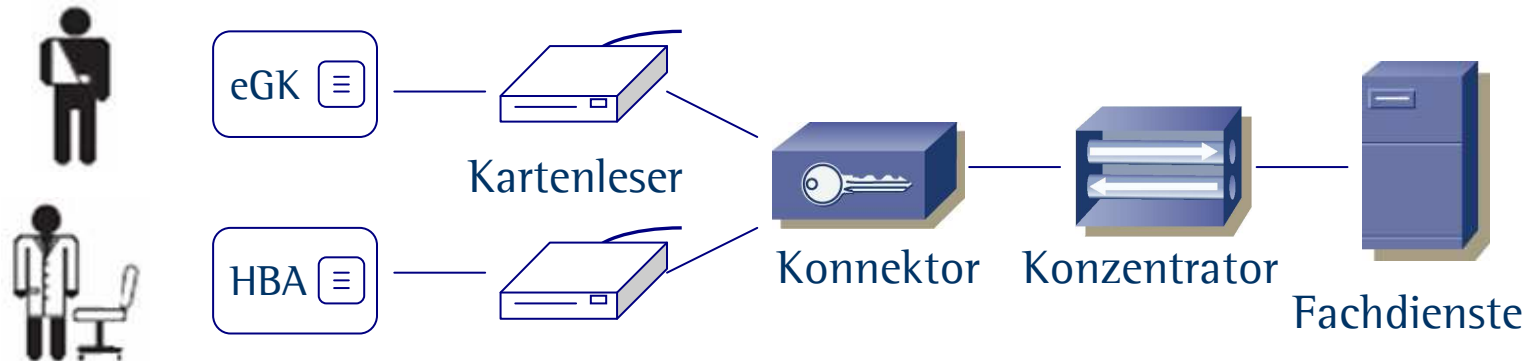
- Vertrauen wird weitergegeben
 - Netzwerk: PGP, Web of Trust
 - Zertifikatshierarchie: z.B. X.509 / RFC3280
- Zertifikatshierarchie
 - Trennung Nutzer-Zertifikate (EE) von Certification Authorities (CA)
 - Baumstruktur mit einer Root-CA
 - meist nur 1-3 Stufen, Tiefe je PKI fest
 - Hierarchie ermöglicht Kontrolle und Verantwortlichkeit
- Prozesse
 - Registrierung, Produktion, Ausgabe, Freischaltung
 - Statusprüfung
 - Sperrung, Ablauf, Erneuerung / Verlängerung



PKIs der eCard-Projekte: Prinzipien

- Anker staatlich oder zumindest staatlich geprüft
- gesetzliche Auflagen auch für die nächste Hierarchiestufe
- Hierarchie aus 2 Stufen
- Verknüpfung mehrere Hierarchien durch TSL
- detaillierte Vorgaben für Zertifikatsinhalte und Prozesse
- Private Schlüssel der EE-Zertifikate auf Chipkarten
- Hoheit der Privaten Schlüssel beim Besitzer (PIN)
- Zertifikatsbasierte Authentifizierung für die gesamte Kommunikation
- Statusprüfung wo immer möglich

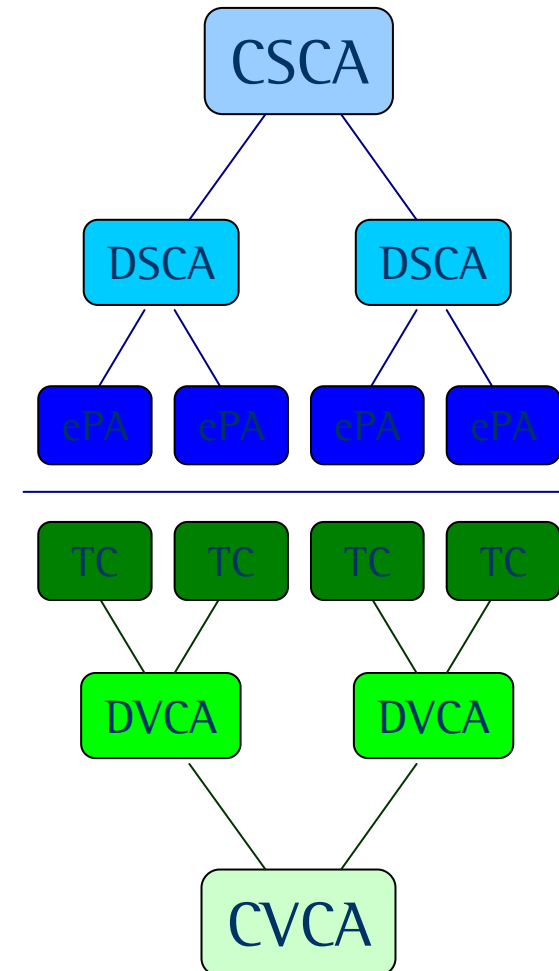
PKIs der eCard-Projekte: Beispiel eGK



- eGK: 5 Zertifikate, u.a. für anonymisierte Operationen
- HBA: 5 Zertifikate, u.a. für qualifizierte (rechtsverbindliche) Unterschrift
- Zertifikate für Kartenleser, Konnektoren, Konzentratoren, Fachdienste ...
- Organisationszertifikate
- annähernd jede Authentifizierung durch Zertifikate
- nicht eine PKI, sondern viele mit verschiedenen Roots und Betreibern

PKIs der eCard-Projekte: Beispiel ePA

- Anlehnung an den Reisepass, aber
 - mehr Daten (insb. Adresse)
 - Daten änderbar
- Zertifikate für „Leseberechtigte“
 - verschiedene Rollen vorgesehen
 - feingranulare Rechteverwaltung möglich
 - Rechte in Zertifikaten abgebildet (signiert)
 - Rechtebeschränkung mit der Zertifikatshierarchie
- Datenhoheit
 - Identität und Schlüssel getrennt signiert
 - komplexe Authentifizierungsverfahren
 - zur Gewährleistung des Datenschutzes: teilweise Abweichung/Erweiterung von internationalen Normen



Features der PKI: Fälschungssicherheit

- Fälschung durch Kopie
 - privater Schlüssel wird im Idealfall von der Karte selbst berechnet
 - privater Schlüssel nicht kopierbar, verlässt die Karte nie
 - kein Backup möglich !
 - Authentizität durch simples „Challenge/Response“ prüfbar
- Verfälschung durch Verändern
 - Personen/Patienten-Daten werden von einer CA signiert
 - weitere Daten werden von Ärzten (oder Patient selbst?) signiert
 - Signaturen einfach prüfbar

Features der PKI: Datenschutz

- Chipkarten-Applikation kapselt Daten und Schlüssel
- Geräte und Nutzer müssen sich gegenüber der Karte authentifizieren
 - Zertifikate beinhalten Identität *und* Rechte
 - Karte nimmt Authentifizierung *und* Autorisierung vor
- Karte gibt keine Daten ohne Einwilligung des Nutzers heraus
 - Leser benötigt mechanischen Zugriff und/oder
 - Freischaltung durch PIN-Eingabe
- Spezialitäten der kontaktlosen Schnittstelle berücksichtigt

Features der PKI: Schutz vor Missbrauch

- Prinzip von Besitz *und* Wissen
 - Karte nicht nutzbar ohne PIN
 - PIN nicht nutzbar ohne Karte
- Statusprüfung
 - Zertifikate können gesperrt werden
 - Status wird veröffentlicht
 - Blacklists (CRL) oder Whitelists (TSL/TCL)
 - Online-Prüfungen (OCSP)
 - Statusinformationen werden von der CA signiert
 - annähernd jede Authentifizierung verlangt auch eine Statusprüfung
 - Alternative ist extrem kurze Laufzeit

Aufbau einer PKI

- Definition der PKI
 - Zertifikatshierarchien
 - Zahl, Bedeutung, Verwendung, Format, Algorithmen der Zertifikate
 - Art der Statusprüfungen
- Vergabe und Betrieb der CAs
 - Anforderungen und gesetzliche Vorgaben
 - Prüfung vor und nach Inbetriebnahme
- Weiterentwicklung
 - Prüfung der Aktualität der Algorithmen, ggf. Nachbesserung

Prozesse einer PKI

- Registrierung: Prüfung der Identität vor Zertifikatsausstellung
- Ausgabe
- Freischaltung: Aktivierung nach bestätigtem Empfang
- Statusprüfung: online/offline
- Sperrung: Frage der Authentifizierung
- Einzug, wenn Voraussetzungen nicht mehr erfüllt sind
- Erneuerung/Verlängerung: evtl. vereinfachte Registrierung

- Prozesse betreffen alle Hierarchien (auch Berechtigungszertifikate)
- Prozesse betreffen immer alle Hierarchiestufen und müssen für jede Hierarchiestufe separat geklärt werden!

PKI: Zusammenfassung

- PKI ist eine bewährte, ausgereifte Technologie, die folgendes ermöglicht
 - Authentifizierung und teilweise auch Autorisierung
 - Vertraulichkeit (Verschlüsselung) und Integrität (Signatur)
 - Resultat: Nicht-Abstreitbarkeit
- Einführung einer PKI erfordert
 - gründliche Vorbereitung
 - Definition der Technologien und Prozesse
- PKI kann unbemerkt im Hintergrund laufen (Bedienbarkeit/Transparenz)
- PKI erfüllt einige der Vertrauensanforderungen an die eCard-Projekte

Fazit

- PKI ist eine geeignete Kernkomponente der eCard-Projekte.
 - PKI allein deckt nicht alle Anforderungen ab.
 - Alle Aspekte müssen akribisch untersucht und spezifiziert werden.
 - Debatten, Uneinigkeiten, öffentliche Diskussionen sind ein Zeichen dafür, dass die notwendigen Anstrengungen unternommen werden, um eine vertrauenswürdige und zukunftssichere Infrastruktur aufzubauen.
- ➔ Gute Zeichen !!!

Architekturen, Definitionen, Spezifikationen sollten von einer unabhängigen Instanz öffentlich geprüft werden.

Vielen Dank für die Aufmerksamkeit!

Erik Neumann
eneumann@mtg.de
media transfer AG

Stand B15