T-Systems ITC Security

Voraussetzungen zum erfolgreichen Roll-Out der Health Professional Card

Dr. Peter Alles
T-Systems GEI GmbH
Security Systems Design

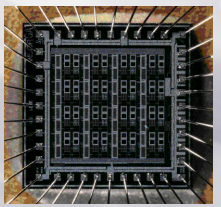
eHealth 2003 - Dresden
21.-23. Oktober 2003

Voraussetzungen zum erfolgreichen Roll-Out der HPC
Was ist zu klären, was führt zum Erfolg?

- Entwicklung Gesamtkonzeption und Beseitigung von Freiheitsgraden:
  - organisatorische Rahmenbedingungen und technische Voraussetzungen bei Leistungserbringern und Registrierungsstellen,
  - HPC-Varianten (Betriebssystem, Zusatz - oder JavaCardanwendung),
  - Einbindung der HPC in Abläufe, Systeme und Datenhaltung,
  - Anforderungen und Maßnahmen bezügl. Sicherheitstechnik, Datenschutz, Verfügbarkeit und Notfälle.
- Abwägung von Vor- und Nachteilen bezüglich
  - Implementierungsaufwand,
  - Herstellerunabhängigkeit und Portierbarkeit,
  - Qualitätssicherung,
  - Investitionssicherheit und Weiterentwicklung.
- Einbindung eines verlässlichen und leistungsstarken Partners.

Voraussetzungen zum erfolgreichen Roll-Out der HPC
Kartenproduktion und Lebenszyklus

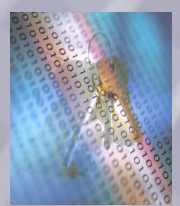
Herstellung von Betriebssystem, Mikroprozessor und Chipkarte



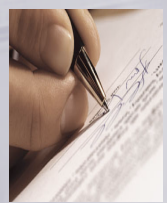
Initialisierung der Kartenanwendung

Einsatz der HPC

physikalische und logische Personalisierung der Chipkarte



Generierung von Schlüsseln und Zertifikaten



Registrierung eines Karteninhabers

Voraussetzungen zum erfolgreichen Roll-Out der HPC
Kartenpersonalisierung

- Personalisierung bedeutet die Zuordnung einer Chipkarte zu einer Person
  - durch physikalische (optische) Maßnahmen: Prägen, Aufdrucken, Lasern, Hologramm;
  - durch logische (elektrische) Maßnahmen: Einbringung von kartenindividuellen und nutzerbezogenen Daten in den Chip wie z.B. Kartennummer, Nutzername, PINs, Berechtigungsklassen, Nutzerrollen, Schlüssel, Zertifikate, Verwaltungsdaten etc.

- Voraussetzungen:
  - sichere Registrierung der Karteninhaber,
  - vertrauenswürdige Schlüssel- und Zertifikatsgenerierung in einem akkreditierten Trust Center,
  - flexible, zuverlässige und leistungsfähige Personalisierung.

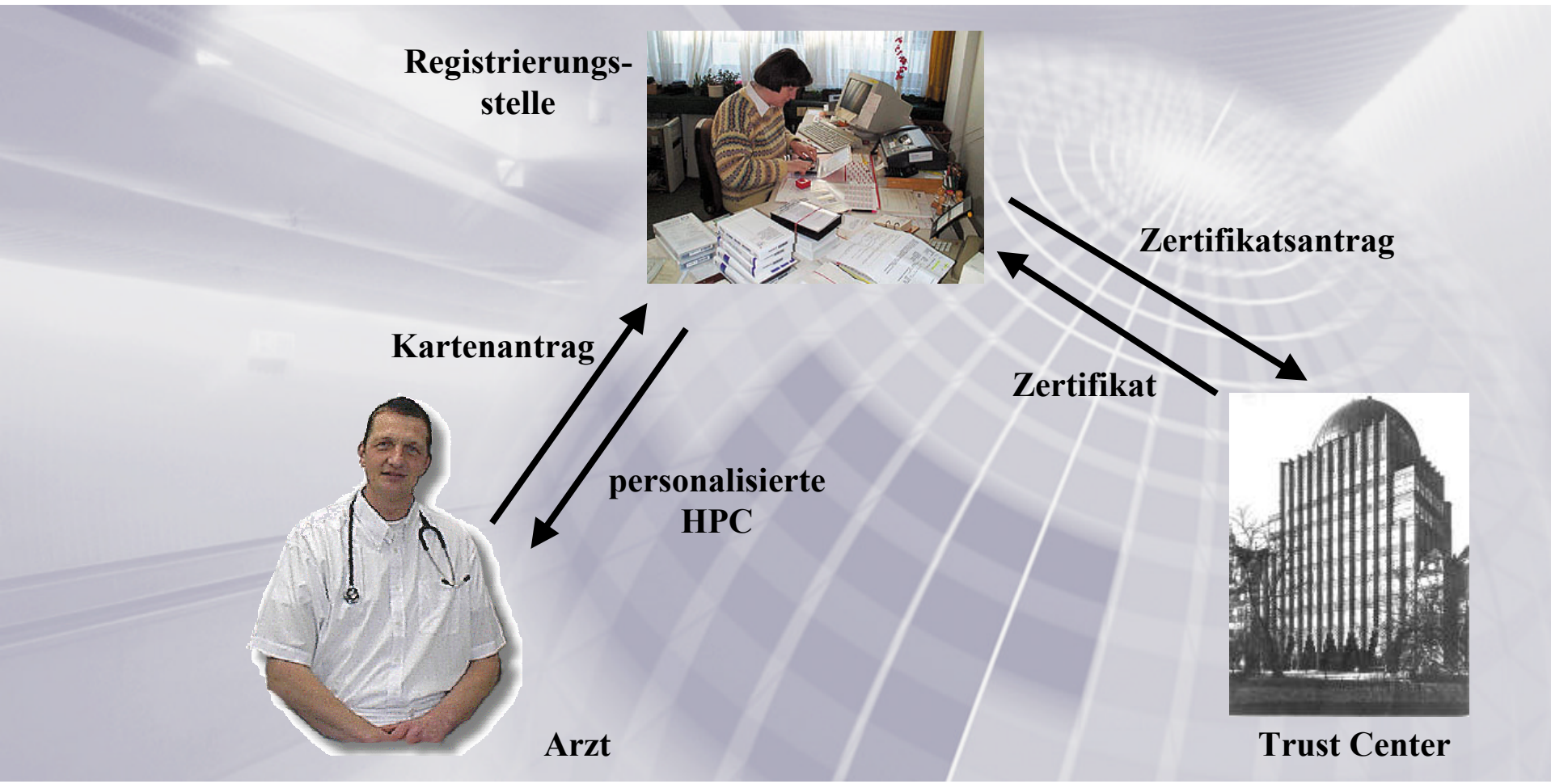
Voraussetzungen zum erfolgreichen Roll-Out der HPC
Freiheitsgrade bei der Kartenausgabe

- Erfassung der Registrierungsanträge bei
  - zentralen Registrierungsstellen (RA - Registration Authority), z.B. Landesärztekammern oder
  - dezentralen / mobilen Registrierungsagenturen z.B. Krankenhausverwaltung.

- Einsatz vorkonfigurierter Karten, die vor Ort komplettiert werden können:
  - zentrale Initialisierung und Vor-Personalisierung der Karte (z.B. PIN, Schlüssel),
  - dezentrale Ein- und Aufbringung nutzerspezifischer Daten (Name, Berechtigung, Rolle etc.) z.B. in der Krankenausverwaltung und
  - Aktivierung in der Registrierungsstelle oder beim HPC-Nutzer durch sichere Einbringung der Zertifikate.

Voraussetzungen zum erfolgreichen Roll-Out der HPC

Szenario zur Kartenausgabe



Voraussetzungen zum erfolgreichen Roll-Out der HPC
Ablauf der Kartenausgabe

- Arzt stellt Antrag bei der Registrierungsstelle für eine HPC.
- Registrierungsstelle erfasst Antragsdaten, legt weitere benutzer-spezifische Daten fest, generiert einen Zertifikatsantrag und sendet dazu die Kartennummer und den öffentlichen Kartenschlüssel an das Trust Center.
- Im Trust Center werden Zertifikate generiert und in einem online-Personalisierungsprozess über die Registrierungsstelle in die HPC eingebracht sowie in ein öffentliches Verzeichnis eingestellt.
- Registrierungsstelle bringt die weiteren Karten- und Nutzerdaten in die HPC ein und händigt die vollständig personalisierte HPC dem Arzt aus.
- Arzt legt seine PINs (persönliche Geheimzahl) fest. Die HPC ist damit einsetzbar.

- Mögliche Variante: Zertifikatseinbringung beim Arzt

Voraussetzungen zum erfolgreichen Roll-Out der HPC
Leistungen der T-Systems

- T-Systems verfügt seit 1985 umfassendes Knowhow im Beratungs- und Lösungsgeschäft der IT-Sicherheit sowie Trust Center und Chipkarten:
  - Entwicklung von kundenspezifischen Sicherheitskonzepten bezüglich Technik, Organisation und Prozessmodellierung,
  - Design, Spezifikation und Implementierung von Anwendungen für Chipkarten und Hintergrundsysteme,
  - Entwicklung, Betrieb von Trust Center, Keymanagement-Systemen,
  - Generierung von SigG-konformen Schlüsseln und Zertifikaten,
  - Evaluierung von Hardware und Software von Sicherheits-komponenten nach ITSEC, Common Criteria, ZKA.
- Eigenes plattformunabhängiges Chipkartenbetriebssystem TCOS.
- T-TeleSec-Chipkarte Netkey E4 ist nach ITSEC / E4 hoch evaluiert.
- Im gesetzlich akkreditierten Trust Center der T-Systems werden seit 1997 signaturgesetzkonforme Schlüssel und Zertifikate erzeugt.

Voraussetzungen zum erfolgreichen Roll-Out der HPC

Referenzauswahl der T-Systems im Bereich Chipkarten und Trust Center-Dienstleistungen