gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Pseudonymisierungskonzepte und -services im Rahmen der Telematikinfrastruktur im Gesundheitswesen

Dr. Stefan Buschner

gematik - Gesellschaft für Telematikanwendungen
der Gesundheitskarte mbH
Friedrichstraße 136
10117 Berlin

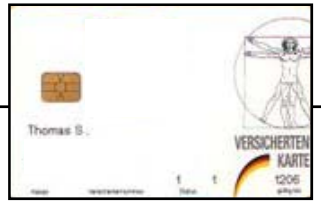
15.12.2008

Kartentypen

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Alt: Krankenversichertenkarte

- Speicherkarte (Memory Card) ohne Betriebssystem
- 256 Bytes Speicher
- Keine Sicherheitslogik

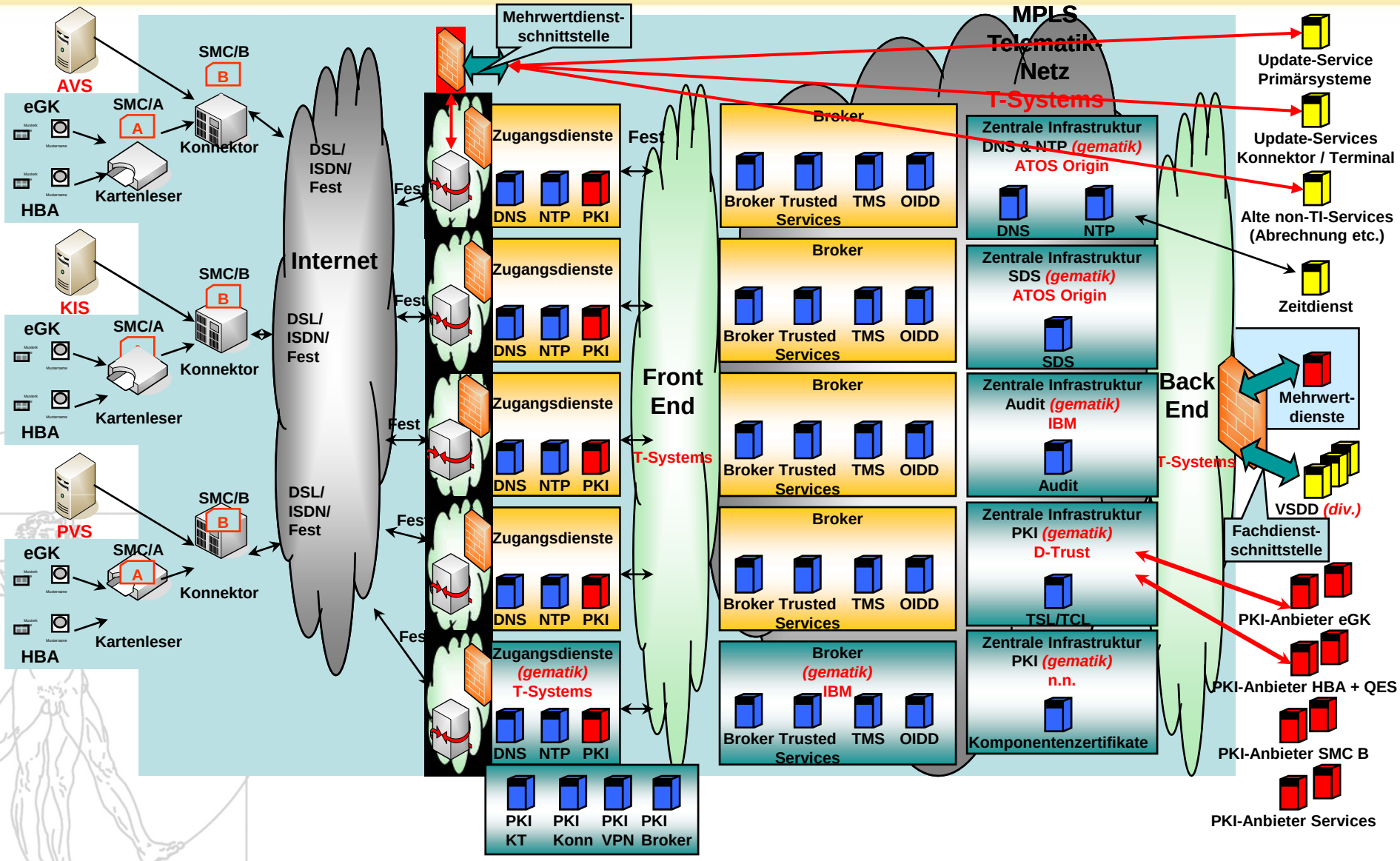


Neu: eGK

- Mikroprozessorkarte (Smart Card) mit Betriebssystem
- frei konfigurierbare Anwendungen
- 65.536 Bytes Speicher
- Konfigurierbare Sicherheitsfunktionen:
  - Authentifikation
  - Verschlüsselung
  - Signatur

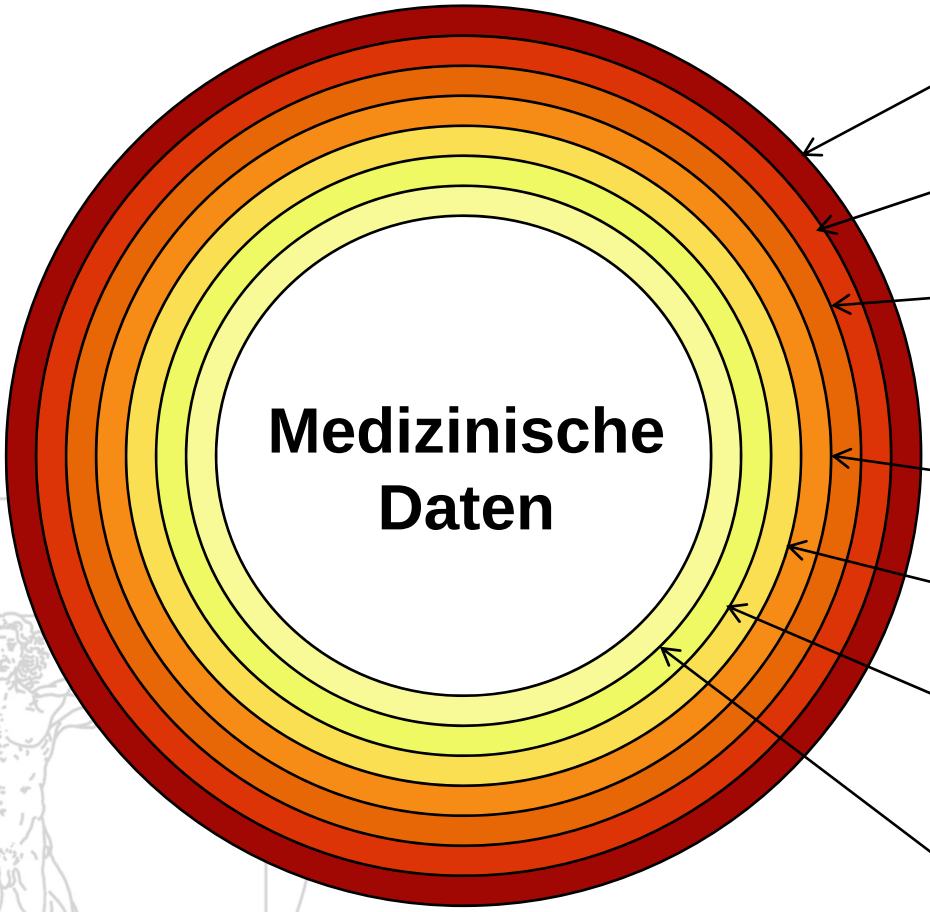
Telematikinfrastruktur

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH



Mehrschichtige Sicherheitsmechanismen in der Telematikinfrastruktur

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

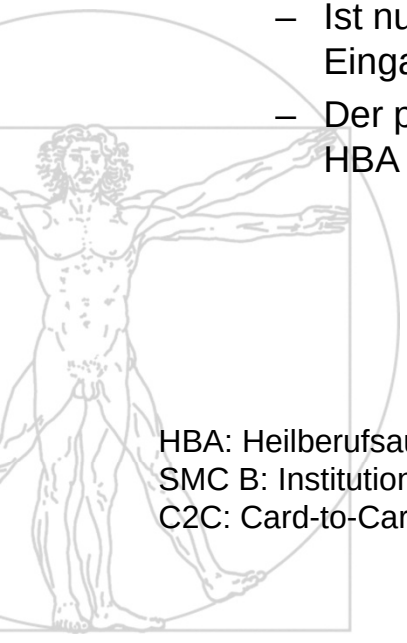


- Zertifizierte Komponenten
- Transportverschlüsselung
- **Anonymisierung und Pseudonymisierung**
- Rollenbasierte Zugriffsrechte
- Datenbasierte Zugriffsrechte
- Individuelle Ende-zu-Ende-Verschlüsselung
- Datentrennung/Zonenkonzept

Elektronische Gesundheitskarte (eGK)

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- **Die Elektronische Gesundheitskarte hat ZWEI Authentisierungszertifikate:**
  - Aut-Zertifikat
    - Enthält den Namen des Versicherten
    - Ist frei lesbar
    - Der private Schlüssel zum Zertifikat arbeitet nur nach PIN-Eingabe des Versicherten
  - AutN-Zertifikat
    - Enthält (geheimes) Pseudonym des Versicherten
    - Ist nur nach C2C-Authentifizierung mit einem HBA bzw. einer SMC B oder einer PIN-Eingabe lesbar
    - Der private Schlüssel zum Zertifikat arbeitet nur nach C2C-Authentifizierung mit einem HBA bzw. einer SMC B oder einer PIN-Eingabe des Versicherten



HBA: Heilberufsausweis von Ärzten, Zahnärzten, Apothekern …
SMC B: Institutionskarte (Praxis, Krankenhaus, Apotheke …
C2C: Card-to-Card

Elektronische Gesundheitskarte (eGK)

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- **Die Elektronische Gesundheitskarte hat ZWEI Verschlüsselungszertifikate:**
  - Enc-Zertifikat
    - Enthält den Namen des Versicherten
    - Ist frei lesbar
    - Der private Schlüssel zum Zertifikat arbeitet nur nach PIN-Eingabe des Versicherten
  - EncV-Zertifikat
    - Enthält (geheimes) Pseudonym des Versicherten
    - Ist nur nach C2C-Authentifizierung mit einem HBA bzw. einer SMC B (nicht Profil 4, 7, 8) oder einer PIN-Eingabe lesbar
    - Der private Schlüssel zum Zertifikat arbeitet nur nach C2C-Authentifizierung mit einem HBA bzw. einer SMC B (nicht Profil 4, 7, 8) oder einer PIN-Eingabe des Versicherten

- **Die Elektronische Gesundheitskarte hat eine eindeutige Identifikationsnummer (ICCSN):**
  - Ist frei Auslesbar

- **Die Verbindung von ICSSN, AutN und EncV mit dem Versicherten ist nur der ausgebenden Krankenkasse bekannt oder kann (nach Freischaltung) von der eGK gelesen werden**

Anwendungen der Pseudonyme der eGK

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- **UFS-Anfrage:**
  - Update-Flag-Service, zeigt an, ob
    - Das Versicherungsverhältnis gültig ist
    - Die Karte gültig ist
    - Die Karte aktuell ist
  - Für die Anfrage wird die ICCSN der eGK geschickt

- **VSDD-Anfrage:**
  - Versichertenstammdatendienst, dient der Aktualisierung der Stammdaten der Karte
  - Es wird das AutN-Zertifikat der Karte geschickt
  - Zertifikat von HBA/SMC B und AutN-Zertifikat werden ins Audit-Log geschrieben

- **CAMS-Anfrage:**
  - Card-Application-Management-System, dient der Aktualisierung von Applikationen und dem Sperren der Karte
  - Es wird das AutN-Zertifikat der Karte geschickt
  - Zertifikat von HBA/SMC B und AutN-Zertifikat werden ins Audit-Log geschrieben

- **VODD-Anfrage:**
  - Verordnungsdatendienst, dient dem online Transport elektronischer Rezepte
  - VOD wird mit dem EncV-Zertifikat der Karte verschlüsselt
  - Zertifikat von HBA/SMC B und EncV-Zertifikat werden ins Audit-Log geschrieben

HBA und SMC B

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- **HBA**
  - Heilberufsausweis von Ärzten, Zahnärzten, Apothekern, Psychotherapeuten, …
  - Unterscheidung der Rollen nach Profilen
  - Keine Pseudonym-Zertifikate

- **SMC B**
  - Institutionskarte von Praxen, Krankenhäusern, Apotheken, ...
  - Unterscheidung der Rollen nach Profilen
  - Keine Pseudnym-Zertifikate

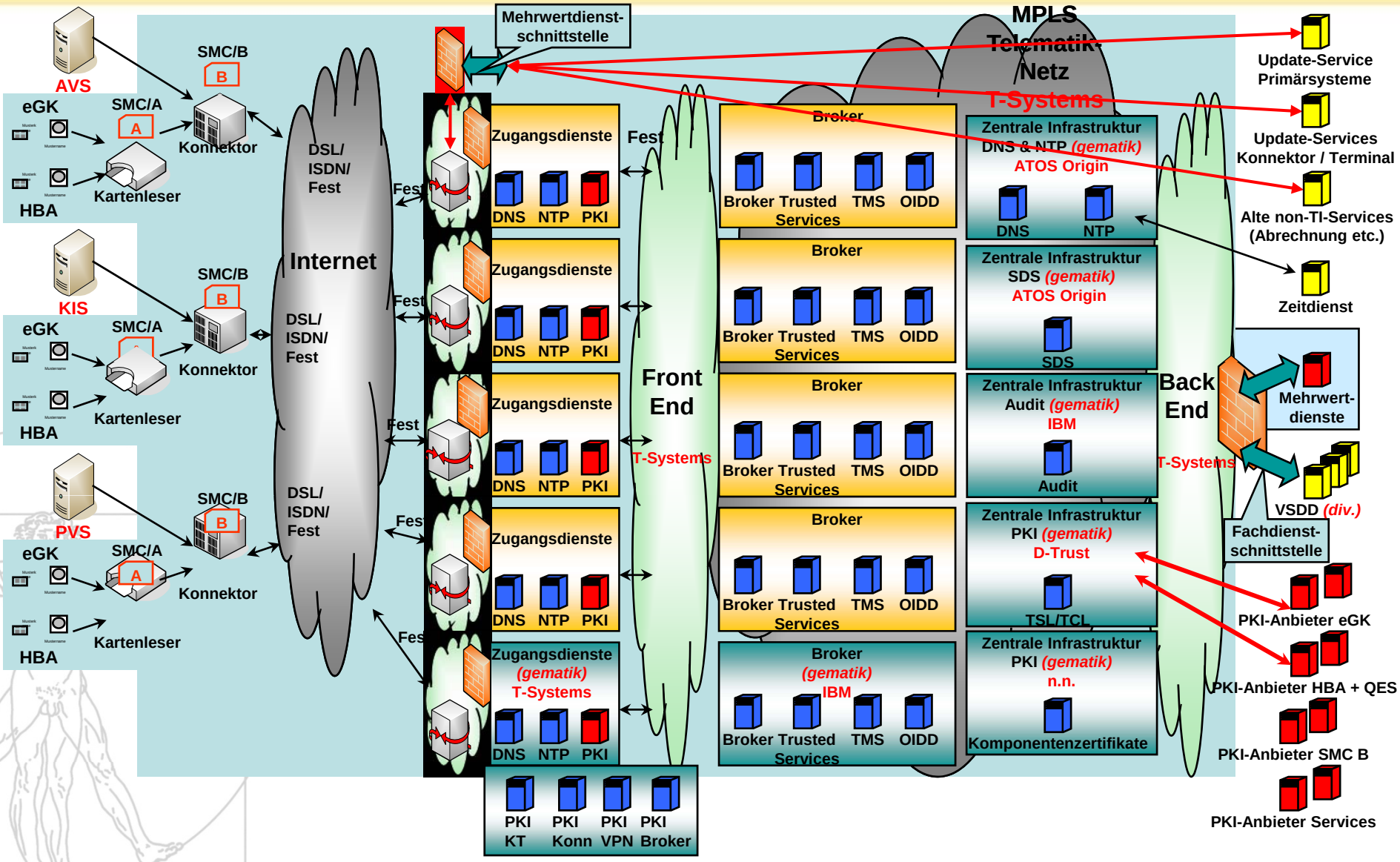
Anonymisierung von HBA- und SMC-B-Anfragen

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- **CAMS- und VSDD-Aufrufe**
  - Die Aufrufe müssen von einem HBA bzw. SMC B signiert werden
  - Broker prüft die Signatur und die Berechtigung
  - Audit-Log wird geschrieben (mit HBA- bzw. SMC-B-Zertifikat)
  - HBA/SMC-B-Signaturen werden entfernt
  - Trusted-Service des Brokers signiert die Anfrage neu und anonymisiert sie damit
  - Neusignierte Anfrage wird ans CAMS bzw. den VSDD geschickt
  - Krankenkassen können nicht nachvollziehen, wer die Kartenaktualisierung abgerufen hat

Telematikinfrastruktur

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH



Vielen Dank für Ihre Aufmerksamkeit !

gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

info@gematik.de ▪ www.gematik.de