

Innovative Merkmale des HBA zur datenschutzgerechten Steuerung von Zugriffsrechten

**12. Fachtagung
„Praxis der Informationsverarbeitung
in Krankenhaus und Versorgungsnetzen“
(KIS2007)**

Ludwigshafen
22. Juni 2007



Fraunhofer Institut
Sichere Informations-
Technologie

1. Schutzbedarf der eGK
2. Der HBA: Die Identität eines Arztes
3. Basis allen Datenschutzes: C2C – Authentifizierung
4. Die SMC: Ein HBA für Geräte
 - A) SMC Typ A: Die Identität eines Gerätes
 - B) SMC Typ B: Die Identität einer Institution



Rheinstraße 75, Darmstadt

Institutsleiterin: Prof. Claudia Eckert

141 Personen
80 Wissenschaftler
Haushalt: 9,75 Mio Euro

SIT bietet

- Hersteller- und produktneutrale Beratung
- Praxisnahe Schulung und Mitarbeiter-Fortbildung
- Marktorientierte Technologiestudien
- Einbettung von Sicherheitstechnologien in bestehende Systeme
- Entwicklung prototypischer IT-Sicherheitslösungen
- Modellierung und Realisierung sicherer elektronischer Geschäftsprozesse und Dienste

SIT-Arbeiten im Bereich eHealth

- bIT4Health
- Protego
- FuE
- gematik
- Slovenien
- ...

1. Schutzbedarf der eGK

2. Der HBA: Die Identität eines Arztes

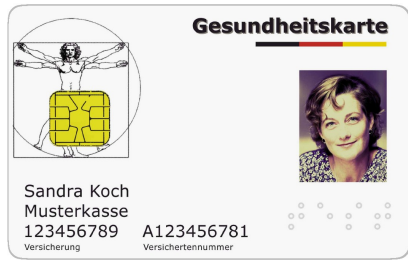
3. Basis allen Datenschutzes: C2C – Authentifizierung

4. Die SMC: Ein HBA für Geräte

A) SMC Typ A: Die Identität eines Gerätes

B) SMC Typ B: Die Identität einer Institution

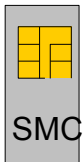
Kartenübersicht



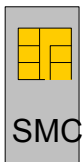
- Persönliche Daten des Versicherten
- Pseudonym des Versicherten
- Notfalldaten
- Kryptographische Schlüssel zum Authentifizieren und Entschlüsseln



- Name des Arztes
- Kryptographische Schlüssel zum Authentifizieren und Entschlüsseln und Signieren



- SMC-A: Identität eines Lesegerätes



- SMC-B: Identität des Konnektors

Schutzbedarf auf der eGK (Auswahl)

Geschützte Daten	Frei lesbare Daten
Geschützte Versichertendaten	Personenstammdaten
Protokolldaten	Versichertendaten
Einwilligung in freiwillige Anw.	
eRezept-Tickets	
Notfalldaten	
Authentifizierungszertifikat (enth. Pseudonym)	Verschlüsselungszertifikat
Privater Entschlüsselungskey (f. Rezepte)	
Privater Authentifizierungskey (f. Tickets)	

1. Schutzbedarf der eGK

2. Der HBA: Die Identität eines Arztes

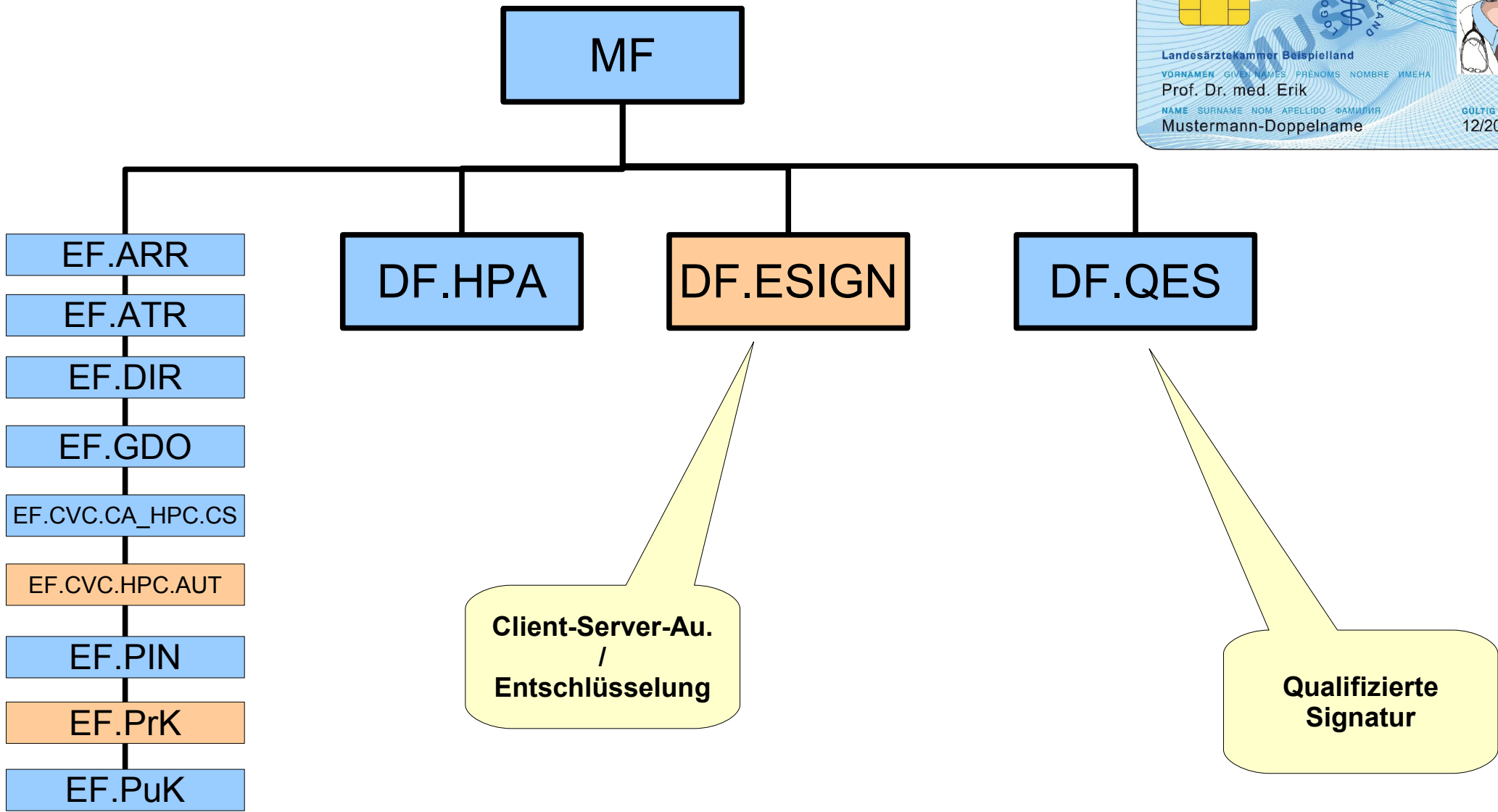
3. Basis allen Datenschutzes: C2C – Authentifizierung

4. Die SMC: Ein HBA für Geräte

A) SMC Typ A: Die Identität eines Gerätes

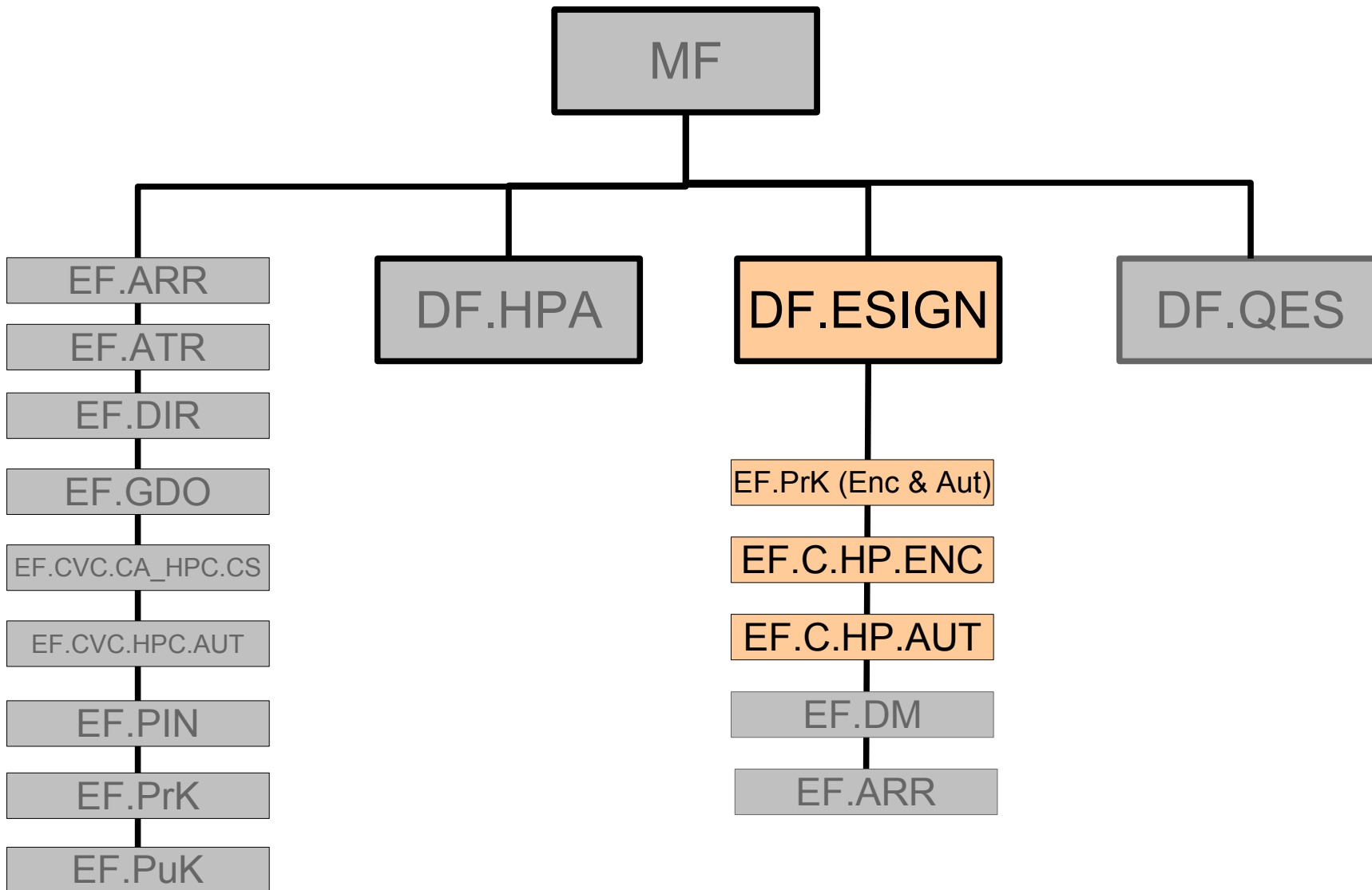
B) SMC Typ B: Die Identität einer Institution

Der HBA: Die Identität eines Arztes



1. Schutzbedarf der eGK
2. Der HBA: Die Identität eines Arztes
3. **Basis allen Datenschutzes: C2C – Authentifizierung**
4. Die SMC: Ein HBA für Geräte
 - A) SMC Typ A: Die Identität eines Gerätes
 - B) SMC Typ B: Die Identität einer Institution

Client-Server-Authentifizierung / Entschlüsselung



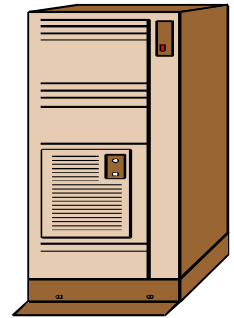
Client-Server-Authentifizierung (stark vereinfacht)

Client

Server



Software
(z.B. Browser)



Server - Credentials

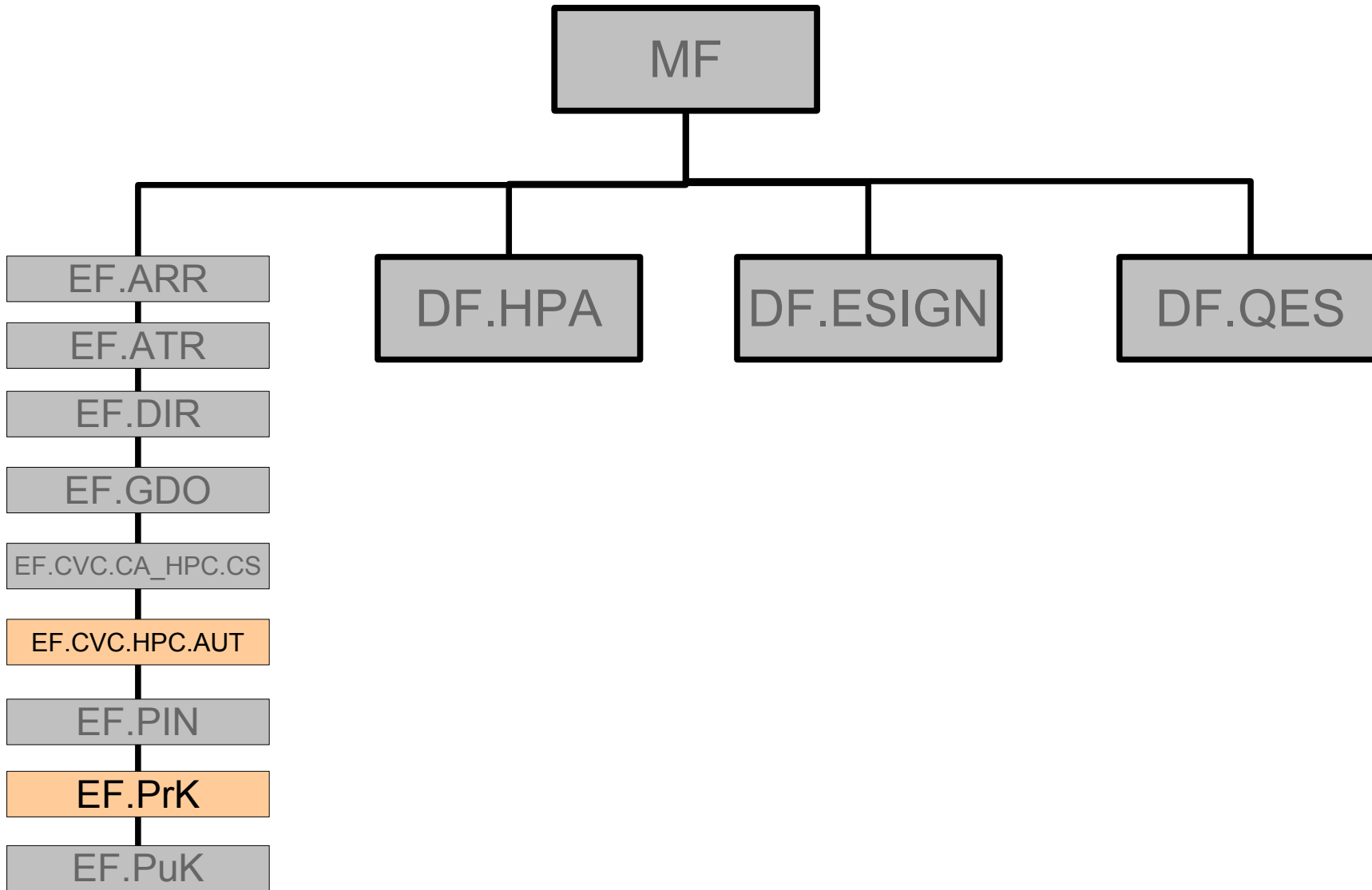


Client - Credentials

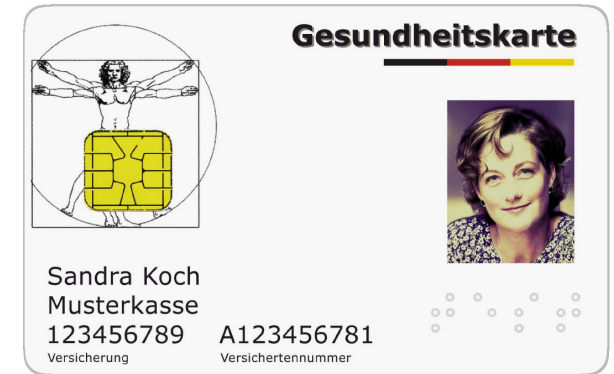
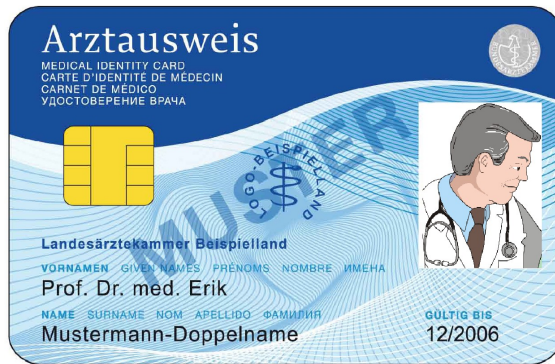


Software prüft Credentials
HBA signiert Client-Credentials

Card – to – Card – Authentifizierung (C2C)

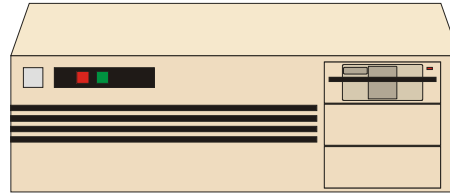
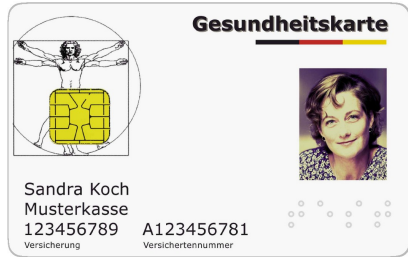


Ziele der C2C - Authentifizierung



- HBA und eGK authentifizieren sich gegenseitig
- Eine manipulierte Software kann keinen positiven Authentifizierungsstatus erzwingen
- Der Versicherte hat die Gewissheit, dass tatsächlich ein HBA auf seine eGK zugreift

C2C – Authentifizierung zwischen eGK und HBA



Internal Au.(RND.HPC)
 ← Sig(RND.HPC) **2**

Get Challenge
 ← RND.eGK **4**

External Au(Sig(RND.eGK))
 ← okay
 („ein HBA hat sich erfolgreich authentifiziert“)

1 → Get Challenge
 RND.HPC

3 → External Au (Sig(RND.HPC))
 okay
 („eine eGK hat sich erfolgreich authentifiziert“)

5 → Internal Au.(RND.eGK)
 Sig(RND.eGK)

Card Verifiable - Zertifikate

- CV – Zertifikate werden von eGK und HBA ausgewertet, nicht von der umgebenden Software
- CV – Zertifikate sind **kompakt**:
 - ◆ typ. 210 Bytes
(X.509: 1500 Bytes)
- CV – Zertifikate sind **einfach**:
 - ◆ Kodierung als Folge von Datenelementen
(X.509: ASN.1 – Kodierung)
- CV – Zertifikate „**sprechen**“ mit der Karte:
 - ◆ CHA – Attribut regelt Zugriffsrechte (z.B. „Inhaber ist Arzt“)
(X.509: Karte ignoriert Inhalt des Zertifikats)

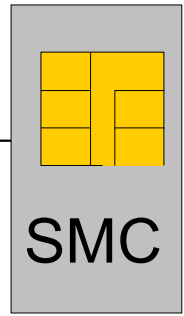
Ergebnis der C2C - Authentifizierung

- Der HBA weiß: Es liegt eine korrekte eGK vor.
- Der HBA kann dies der Software signalisieren

- Die eGK weiß: Es liegt ein korrekter HBA vor
- Die eGK kann dies der Software signalisieren
- Die eGK räumt dem HBA spezielle Rechte ein

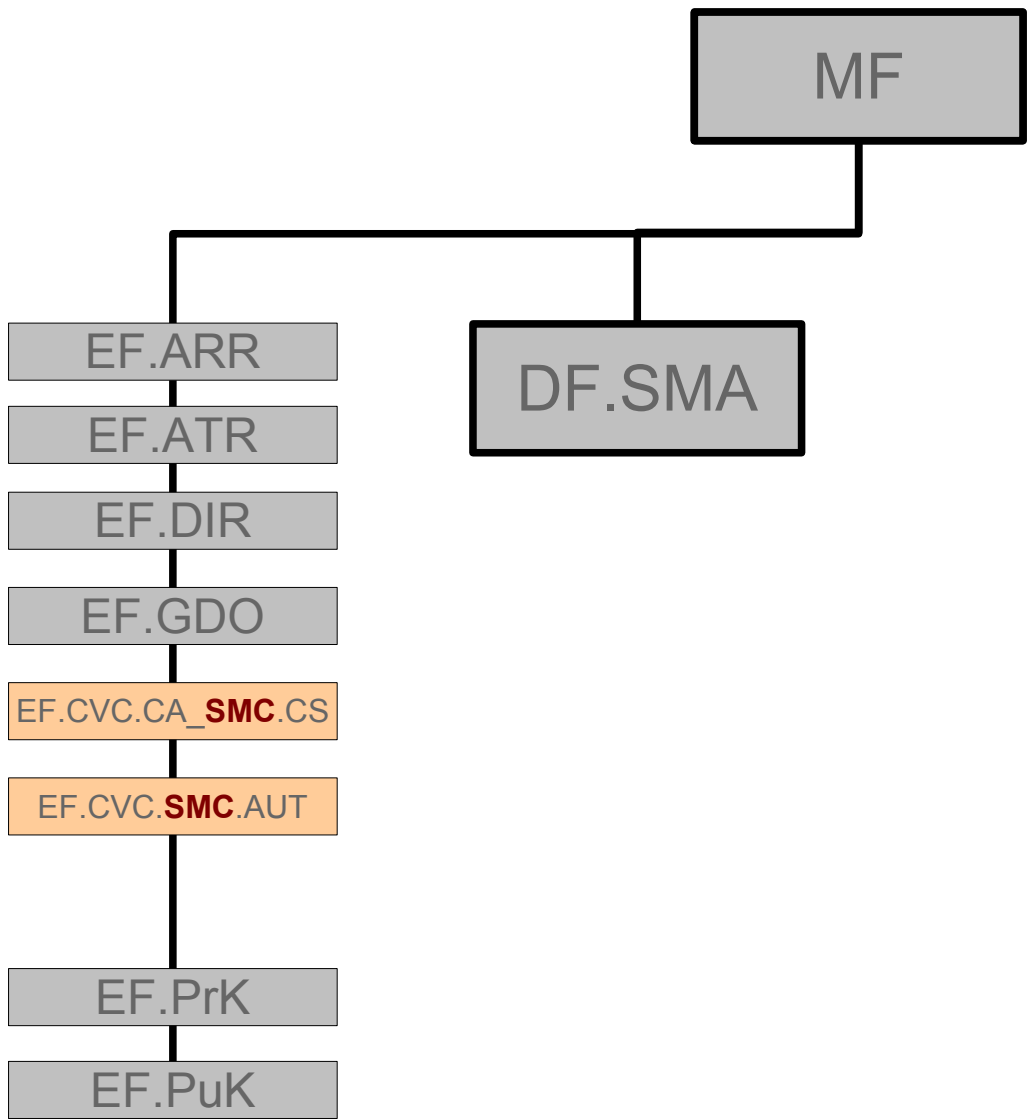
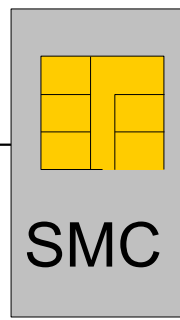
- Optional: Aufbau einer gesicherten Verbindung

1. Schutzbedarf der eGK
2. Der HBA: Die Identität eines Arztes
3. Basis allen Datenschutzes: C2C – Authentifizierung
4. **Die SMC: Ein HBA für Geräte**
 - A) SMC Typ A: Die Identität eines Gerätes
 - B) SMC Typ B: Die Identität einer Institution



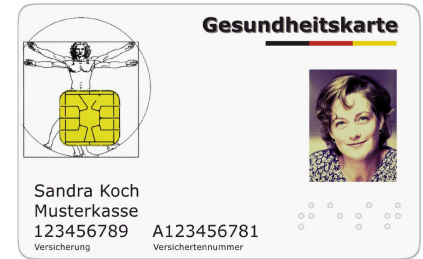
- SMC = Security Module Card
- Eine SMC **Typ-A** ist typischerweise in ein SC-Terminal eingebaut
- Eine SMC **Typ-B** ist typischerweise in einen Konnektor eingebaut
- Die SMC beruht auf der gleichen Plattform wie der HBA
- Ziele der SMC:
 - ◆ Der HBA kann eine SMC autorisieren
--> Arzthelfer können ohne HBA auf die eGK zugreifen
 - ◆ Die SMC kann verschlüsselte Verbindung zu einem HBA aufbauen (z.B. für PIN)
 - ◆ Die SMC kann eine verschlüsselte Verbindung zu einer eGK aufbauen (der HBA kann das nicht!)

SMC Typ A: Die Identität eines Gerätes



Die SMC **Typ A** ist nicht an eine Person gebunden.

SMC – Anwendung #1: Der HBA autorisiert die SMC



C2C – Au.

1

Ergebnis:
Die SMC ist
„scharf“
geschaltet

C2C – Au.

2

Ergebnis:
Die SMC
erhält HBA -
Privilegien

Anwendung: Arzt schaltet
SMC der Arzthelferin frei.

Problem #1: Arzthelferin arbeitet ohne Arzt

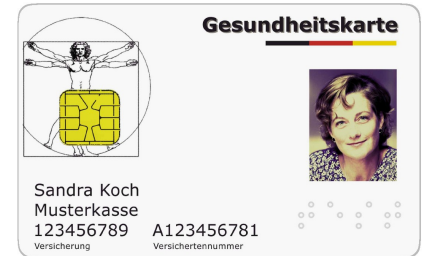
Ich möchte schon einmal die eGK des Versicherten lesen.



Ich autorisiere die SMC des Terminals mit meinem HBA.



SMC – Anwendung #1: Der HBA autorisiert die SMC



C2C – Au.

1

Ergebnis:
Die SMC ist
„scharf“
geschaltet

Anwendung: Arzt schaltet
SMC der Arzthelferin frei.

C2C – Au.

2

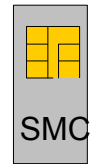
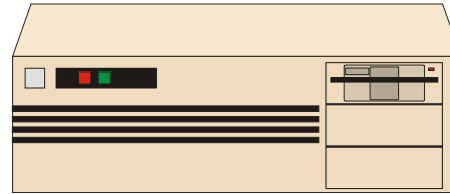
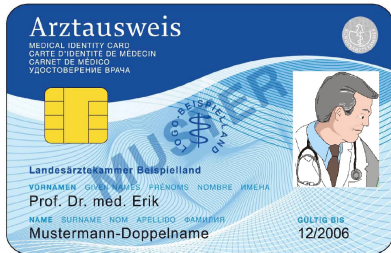
Ergebnis:
Die SMC
erhält HBA -
Privilegien

Problem #2: HBA liegt im „Safe“, Arzt will signieren

Mein HBA ist sicher verwahrt. Ich möchte aber mit meinem Terminal in jedem Raum signieren können.



SMC – Anwendung #2: Sichere Kommunikation mit HBA



Ergebnis:
Es existiert ein
sicherer Kanal
zwischen HBA
und SMC

C2C – Au.

1

2

Bitte Kommando verschlüsseln
verschlüsseltes Kommando

Verschlüsseltes Kommando

Verschlüsselte Antwort

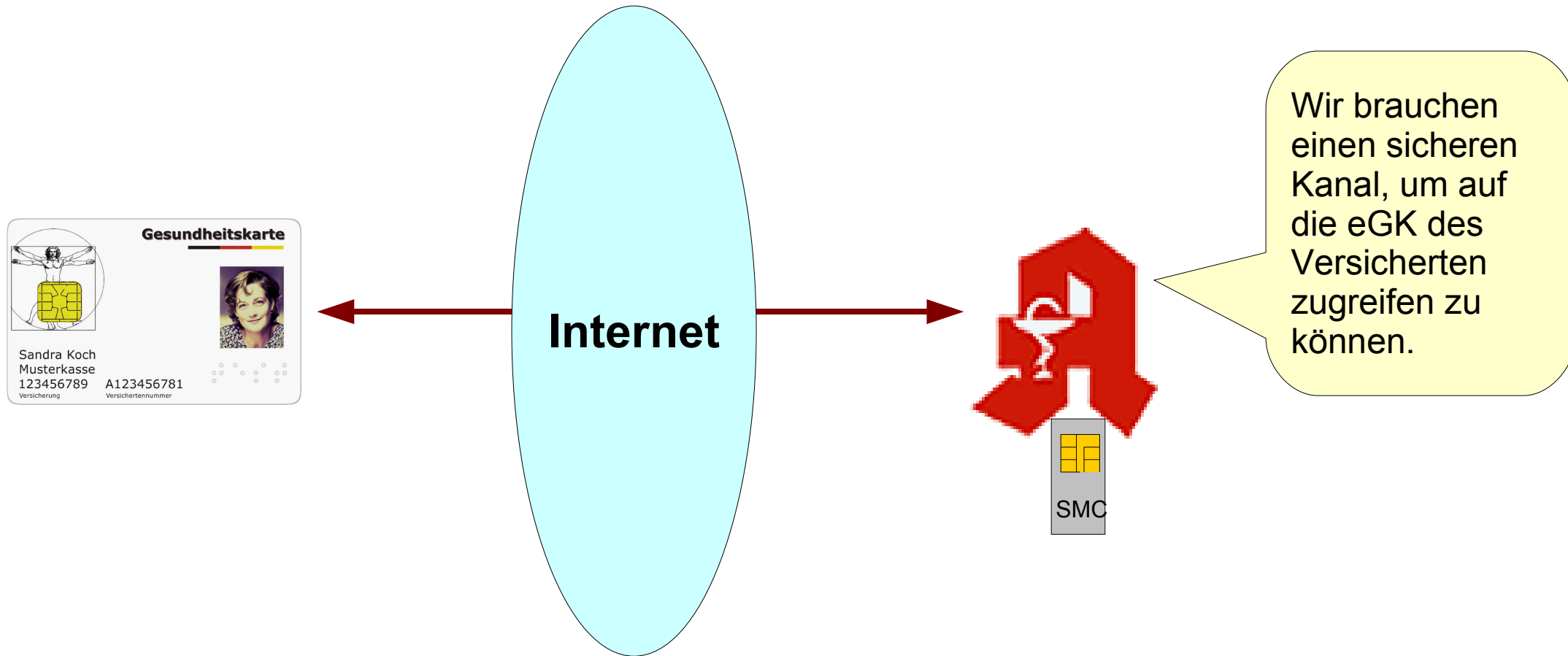
3

4

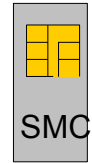
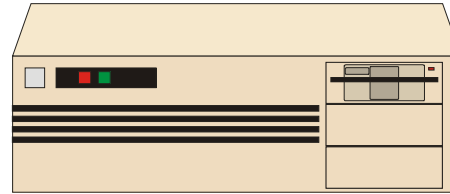
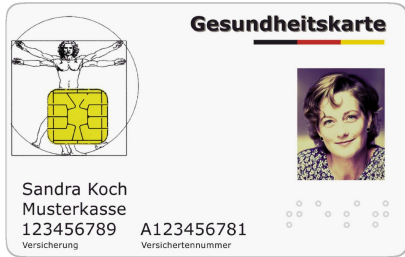
Bitte Antwort entschlüsseln
entschlüsselte Antwort

Anwendung: HBA liegt im „Safe“,
PIN wird sicher übertragen.

Problem #3: Versandapotheke dispensiert Rezept



SMC – Anwendung #3: Sichere Kommunikation mit eGK



Ergebnis:
Es existiert ein
sicherer Kanal
zwischen eGK
und SMC

C2C – Au.

1

2

Bitte Kommando verschlüsseln
verschlüsseltes Kommando

Verschlüsseltes Kommando
Verschlüsselte Antwort

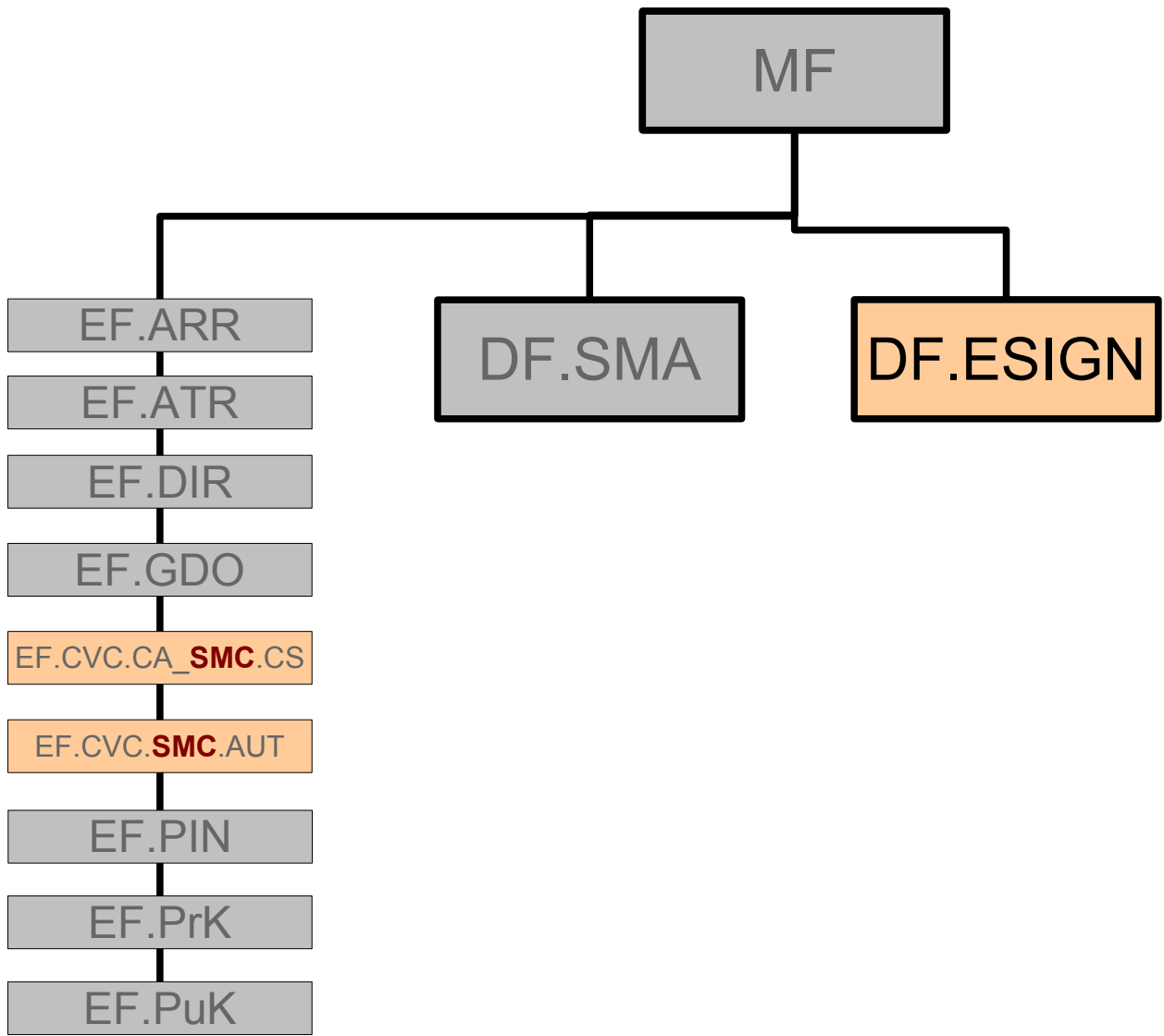
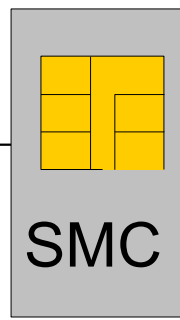
3

4

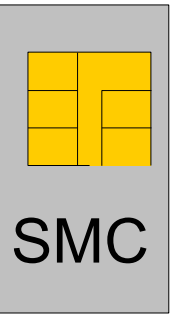
Bitte Antwort entschlüsseln
entschlüsselte Antwort

Anwendung: Versandapotheke
dispensiert ein Rezept

SMC – Typ B: Die Identität einer Institution



Die SMC **Typ B** trägt die Identität einer Institution („Praxis Bülowbogen“)



- Die SMC Typ B ist typischerweise im Konnektor
- Entschlüsselung von Dokumenten, die für die Institution bestimmt sind
- Signierung von Dokumenten, welche keine qualifizierte Signatur brauchen
- Authentifizierung der Institution
- Die SMC Typ B enthält alle Funktionen der SMC Typ A

Zusammenfassung

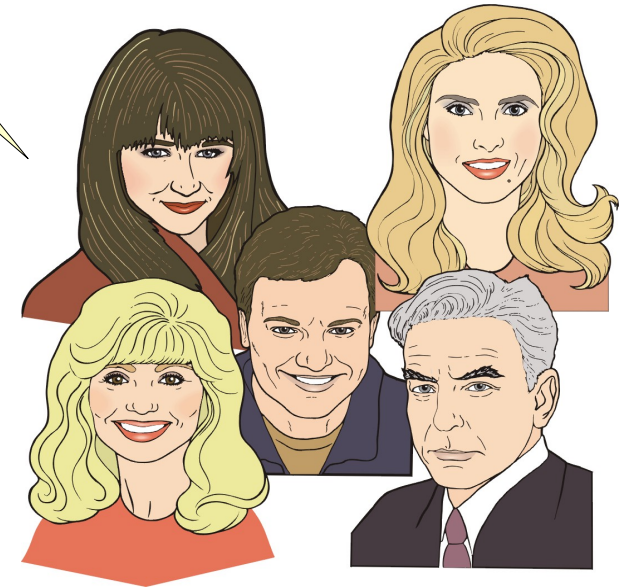
- C2C – Authentifizierung ist die Basis allen kartenbasierten **Datenschutzes**
- C2C – Authentifizierung ist **besonders sicher**, weil die Umgebungssoftware weniger Einfluss hat
- C2C – Authentifizierung räumt dem HBA Privilegien in der eGK ein
- Mit C2C – Authentifizierung kann die Kommunikation zweier Karten kryptographisch abgesichert werden
- C2C gibt dem Versicherten Sicherheit, selbst dann, wenn die Softwareumgebung nicht unter seiner Kontrolle ist
- Der HBA verfügt über weitere innovative Mechanismen (Kanal-Konzept, Nachladbarkeit, ...)

Zum Weiterlesen

Mehr
HBA!



Mehr
eGK!



Spezifikation des elektronischen **Heilberufsausweises** –
Teil I: Kommandos, Algorithmen und Funktionen der
Betriebssystemplattform

Spezifikation des elektronischen **Heilberufsausweises** –
Teil II: HBA – Anwendungen und Funktionen

Spezifikation des elektronischen **Heilberufsausweises** –
Teil III: SMC – Anwendungen und Funktionen

Spezifikation der elektronischen **Gesundheitskarte** –
Teil I: Kommandos, Algorithmen und Funktionen der
Betriebssystemplattform

Spezifikation des elektronischen **Gesundheitskarte** –
Teil II: Anwendungen und anwendungsspezifische
Strukturen