

# eGK-Zugriffsprofile: Datensicherheit durch Card-to-Card-Authentifizierung

---

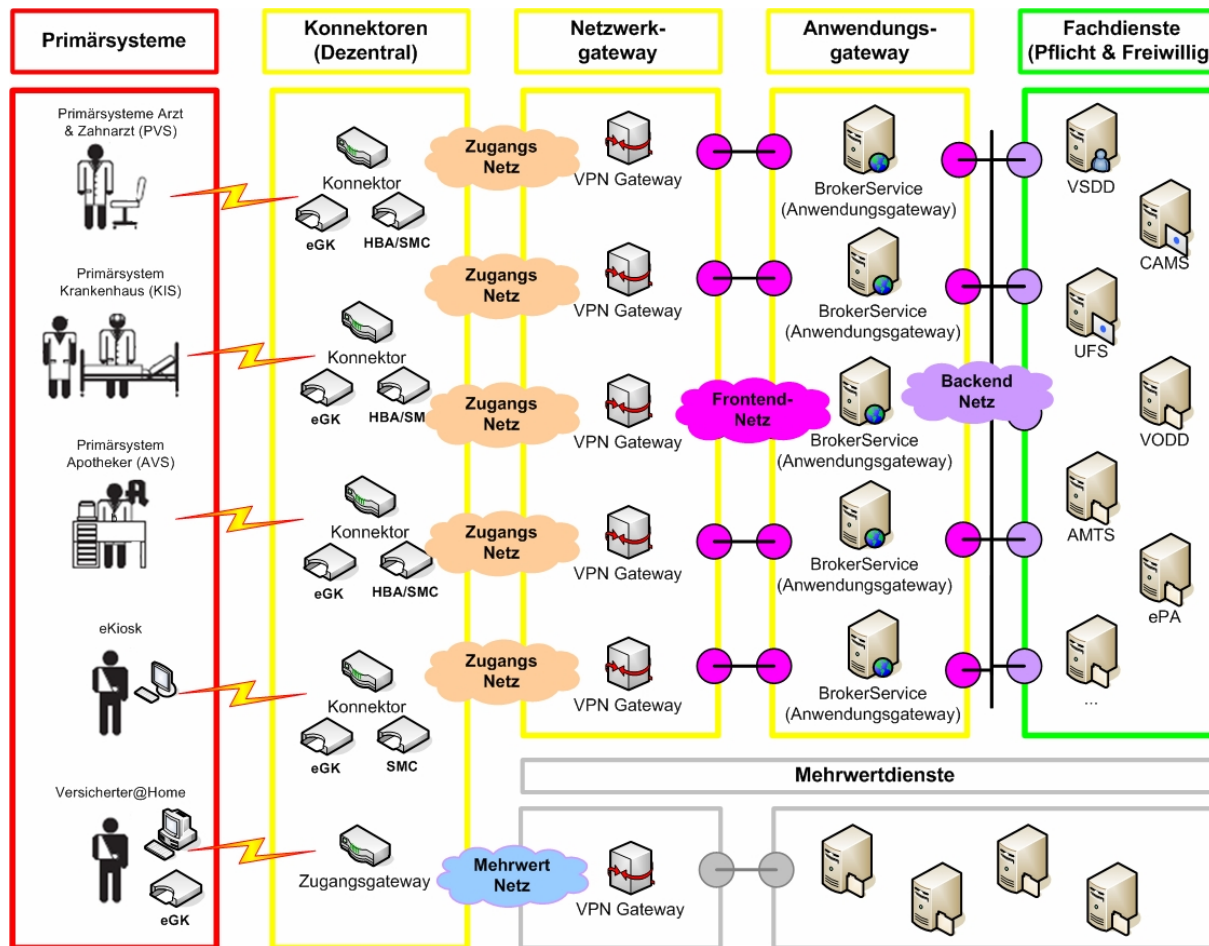
Dr. S. Buschner

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

27.09.2007

---

# Gesamtarchitektur



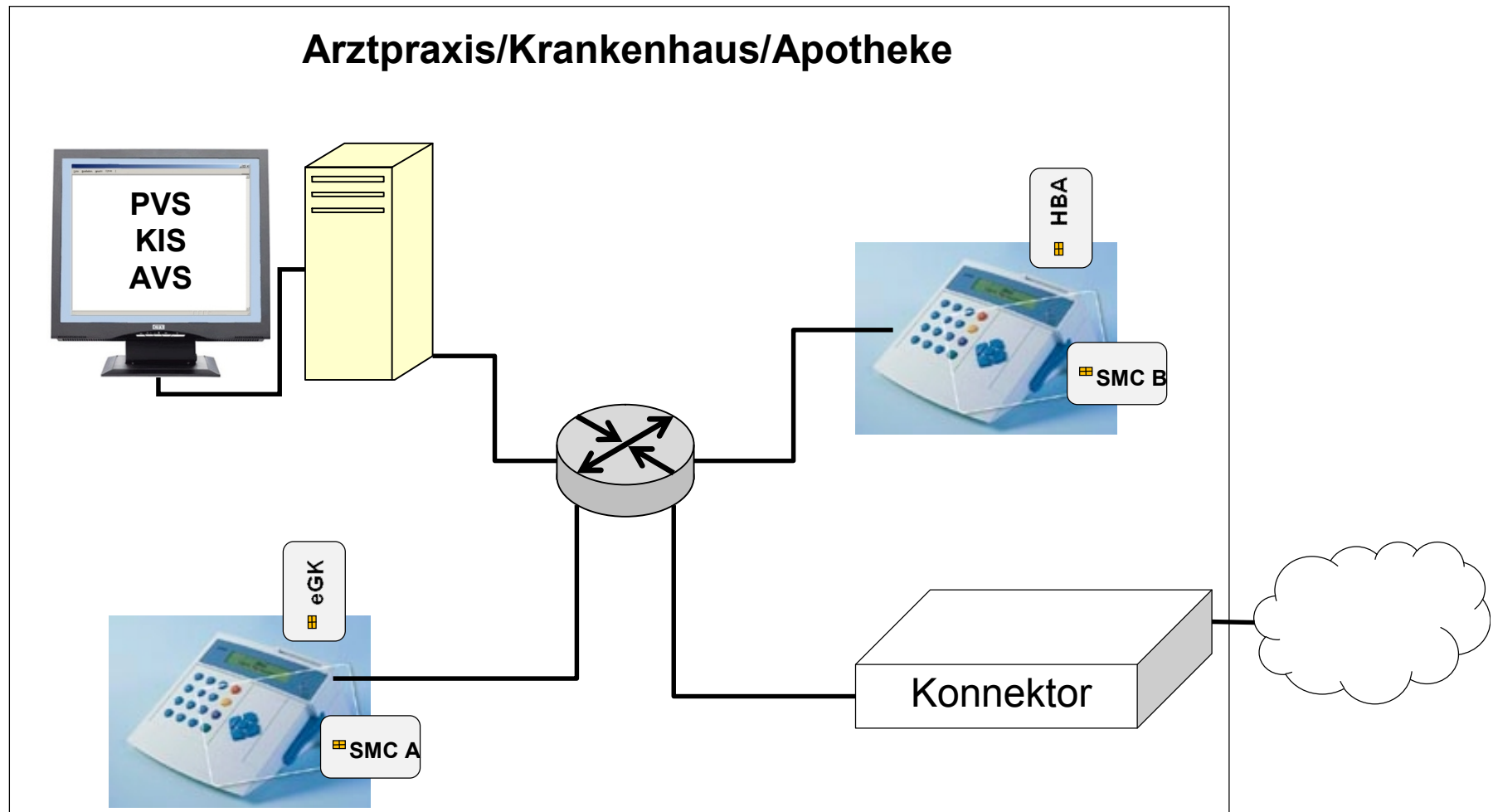
# Einführungsphasen der Telematikinfrastuktur



Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Applikation	Release				
	Rel. 1	Rel. 2		Rel. 3	
	Funktionsabschnitt				
	FA1	FA2	FA3	FA4	Nach FA4
Versicherungsstammdaten (VSDM)	Offline	Online			
eVerordnung (VODM)	Offline		Online		
Weitere Elektronische Verordnung (VODM)	N/A			Online	
Notfalldaten	Offline			Online	
Arzneimitteltherapiesicherheit (AMTS)	N/A			Online	
Anwendungen zur Wahrnehmung der Versichertenrechte (AdV)	N/A			Online	
Elektronische Patientenakte (ePA)	N/A				Online

# Dezentrales System



## Die Karten der Telematikinfrastuktur:

- **eGK**: elektronische Gesundheitskarte, Trägerin der
  - Versichertenstammdaten
  - Medizinischen Daten
  - Schlüssel und Zertifikate (X.509 und CVC)
- **HBA**: Heilberufsausweis der Leistungserbringer (Ärzte, Zahnärzte, Apotheker, ...)
  - Schlüssel und Zertifikate (X.509 und CVC)
    - Qualifizierte elektronische Signatur
    - Träger der Personenidentität (Zahn-/Arzt, Apotheker, ...)
    - Authentifizierung
    - C2C-Authentifizierung mit SMC und eGK zur Freischaltung der Karten

## Die Karten der Telematikinfrastuktur:

- **SMC A: Secure Module Card A**
  - Schlüssel und Zertifikate (CVC)
    - C2C-Authentifizierung mit eGK zur Freischaltung der eGK
    - Aufbau Trusted-Channel mit HBA
- **SMC B: Secure Module Card B**
  - Schlüssel und Zertifikate (X.509 und CVC)
    - Wie SMC A
    - Träger der Institutionsidentität (Praxis, Krankenhaus, Apotheke)
    - Authentifizierung (SSL-Tunnel zum Broker, Fachdienste)
    - Nachrichtensignatur, Entschlüsselung

## CVC: Card-Verifiable-Certificate

- ASN.1-kodiertes Zertifikat nach ISO 7816-8
- Kann von Karten mit Hilfe eines in der Karte gespeicherten öffentlichen Schlüssels geprüft werden
- Zertifikat enthält kein Ablaufdatum
- Zertifikat enthält Certificate Holder Authorisation (CHA)
  - CHA ist die Rollenkennung des Kartenbesitzers/Institution
  - 6 Byte Präfix, 1 Byte Profil-ID
  - D2 76 00 00 40 00 || xA

# Beispiel CVC



Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

tag	L	Wert		
'7F21'	'81CE'	CV-Zertifikat (206 Byte)		
		tag	L	Wert
		'5F37'	'8180'	SIG.CA (128 Byte)
				Digital Signature Input für SIG.CA ('6A' ... 'BC'):
				'6A' = Padding entsprechend [ISO 9796-2]
				'03' = CPI
				'xx.xx' = CAR (8 Byte)
				'xx.xx' = CHR (12 Byte)
				'xx.xx' = CHA (7 Byte)
				'xx.xx' = OID (7 Byte)
				'xx.xx' = PK part 1 (erster Teil des Modulus, 71 Byte)
				'xx.xx' = Hash (20 Byte, Hash Input: DEs CPI ... PK, siehe Tabelle B.8)
				'BC' = Trailer
		'5F38'	'3D'	'xx.xx' = PK-Rest (Rest des Modulus, gefolgt vom Exponenten '00010001', 61 Byte)
		'42'	'08'	'xx.xx' = CAR (8 Byte)

## Profil-IDs des CHA



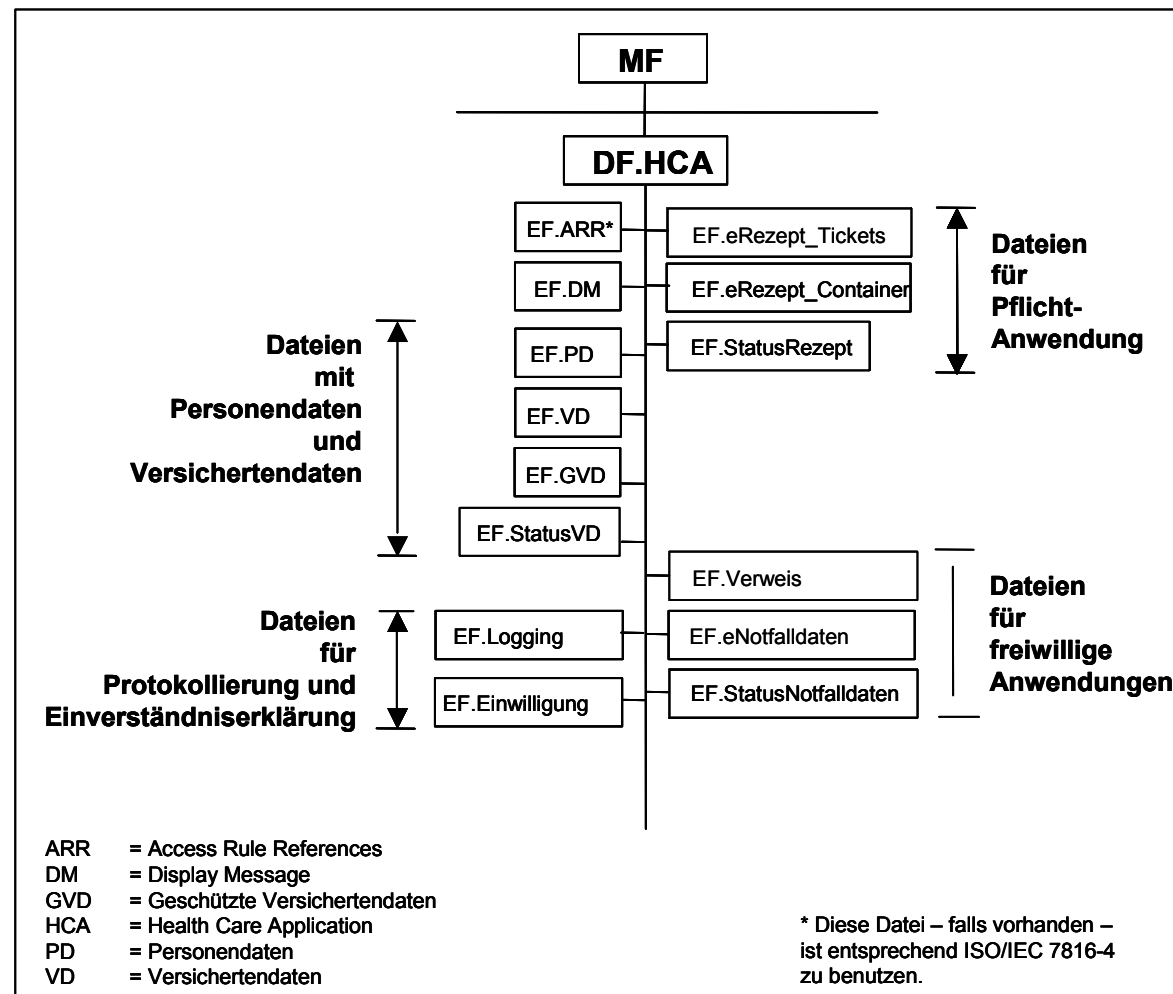
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Profil	Rolle
1	eKiosk
2	Arzt , Hilfspersonal des Arztes, SMC-B Arztpraxis
3	Apotheker, Hilfspersonal des Apothekers, SMC-B Apotheke
4	Psychotherapeut
5	HBA sonstige Leistungserbringer
6	Versand-Apotheke
7	Rettungsassistent

# Voraussichtliche Profil-IDs des CHA (gemäß eGK-Spezifikation V1.5.1 für Release 2.3.1)

Profil	Rolle
1	eKiosk
2	Arzt
3	Apotheker
4	Psychotherapeut
5	HBA sonstige Leistungserbringer
6	Versand-Apotheke
7	Rettungsassistent
8	SMC Arzt, Hilfspersonal in der Praxis
9	SMC Apotheke, Hilfspersonal in der Apotheke
A	SMC Psychotherapeut, Hilfspersonal

*(noch nicht final abgestimmt)*



# Zugriffsmöglichkeiten auf die Gesundheitsanwendungen der eGK (gemäß eGK-Spezifikation V1.5.1 für Release 2.3.1)

*(noch nicht final abgestimmt)*

ALW	Aktion kann jederzeit von jedermann ausgeführt werden
home	Aktion kann nach Eingabe von PIN.home ausgeführt werden
1	Aktion kann nach Rollenauthentisierung im Profil 1 ausgeführt werden
3 + CH	Aktion kann nach Rollenauthentisierung im Profil 3 UND Eingabe von PIN.CH ausgeführt werden
6	Damit Rolle CHA.6 im DF.HCA Aktionen ausführen kann ist es notwendig einen Trusted Channel aufzubauen. Dies ist in der folgenden Tabelle nicht extra ausgewiesen
CAMS	Rolle des CAMS repräsentiert durch den Schlüssel SK.CAMS
VSCA	Rolle des VSDD/CAMS repräsentiert durch den Schlüssel SK.VSDDCAMS
VSDD	Rolle des VSDD repräsentiert durch den Schlüssel SK.VSDD
C, Create	Recht neue Dateien, PINs oder Schlüssel anzulegen
R, Read	Recht zu lesen und in strukturierten Dateien zu suchen (SEARCH RECORD)
U, Update	Recht zu Schreiben und zu Überschreiben ( = Löschen von Information)
A, Activate	Recht ein File zu aktivieren, dabei werden auch alle Rekords sichtbar
D, Deactivate	Recht in einer Datei enthaltene Rekords zu deaktivieren (verbergen)
a, Append	Anhängen eines Rekords in einer strukturierten Datei.

# Gesundheitsanwendungen der eGK und ihre Zugriffsregeln (gemäß eGK-Spezifikation V1.5.1 für Release 2.3.1)



Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Object	ALW	home	1	1 + CH	2	2 + CH	8	8 + CH	3	3 + CH	9	9 + CH	6	6 + CH	4	4 + CH	10	10 + CH	5	5 + CH	7	7 + CH	CAMS	VSCA	VSDD
DF.HCA																							CAD	CAD	
EF.PD EF.VD EF.StatusVD	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	RU	RU
EF.GVD		R		R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R				RU	RU
EF.Einwilligung		R		R		RU		R		RU		R		R		RU									
EF.Verweis		R		R		RUAD		R		RUAD		R		R		RUAD									
EF.eRezept_Tickets		R		RUAD	RU	RU	RU	RU	RU	RU	RU	RU	RU	RU					RU	RU					
EF.StatusRezept EF.eRezept_Container				R	RU	RU	RU	RU	RU	RU	RU	RU	RU	RU					RU	RU					
EF.Notfalldaten EF.StatusNotfalldaten		AD		AD	R	RU	RU	RU	R	RU	R	RU			R	RU					R	R			
EF.Logging		R		a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a			
EF.DM		U											R	R									R	R	R

*(noch nicht final abgestimmt)*

# Einführungsphasen der Telematikinfrastuktur



Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Applikation	Release				
	Rel. 1	Rel. 2		Rel. 3	
	Funktionsabschnitt				
	FA1	FA2	FA3	FA4	Nach FA4
Versicherungsstammdaten (VSDM)	Offline	Online			
eVerordnung (VODM)	Offline		Online		
Weitere Elektronische Verordnung (VODM)	N/A			Online	
Notfalldaten	Offline			Online	
Arzneimitteltherapiesicherheit (AMTS)	N/A			Online	
Anwendungen zur Wahrnehmung der Versichertenrechte (AdV)	N/A			Online	
Elektronische Patientenakte (ePA)	N/A				Online

### Zertifikate der eGK für die Gesundheitsanwendungen:

- **EncV: Verschlüsselungszertifikat mit Pseudonym**
  - Dient der Verschlüsselung der eVerordnung für den VODD
  - Der private Schlüssel zu EncV wird nur nach einer C2C-Authentifizierung mit einer Karte mit CHA-Profil-ID 3 (neu auch 2) freigeschaltet
    - à Keine PIN-Eingabe bei der Einlösung von Rezepten
- **AutN: Authentifizierungszertifikat mit Pseudonym**
  - Dient der Nachrichtensignatur in der Praxis zur Kennzeichnung, dass die eGK anwesend ist
  - Zertifikat nur lesbar nach C2C-Authentifizierung mit Profil-ID 2, 3
    - à Keine PIN-Eingabe in der Arztpraxis für Nachrichten

# Gesamtarchitektur

