Final Check-Up Gesundheitskarte

Euroforum-Konferenz - 21. / 22. Juni, Berlin

Basisspezifikationen der Gesundheitskarte

Levona Eckstein

Fraunhofer-Institut
Sichere Informations-Technologie SIT
Rheinstraße 75
64295 Darmstadt

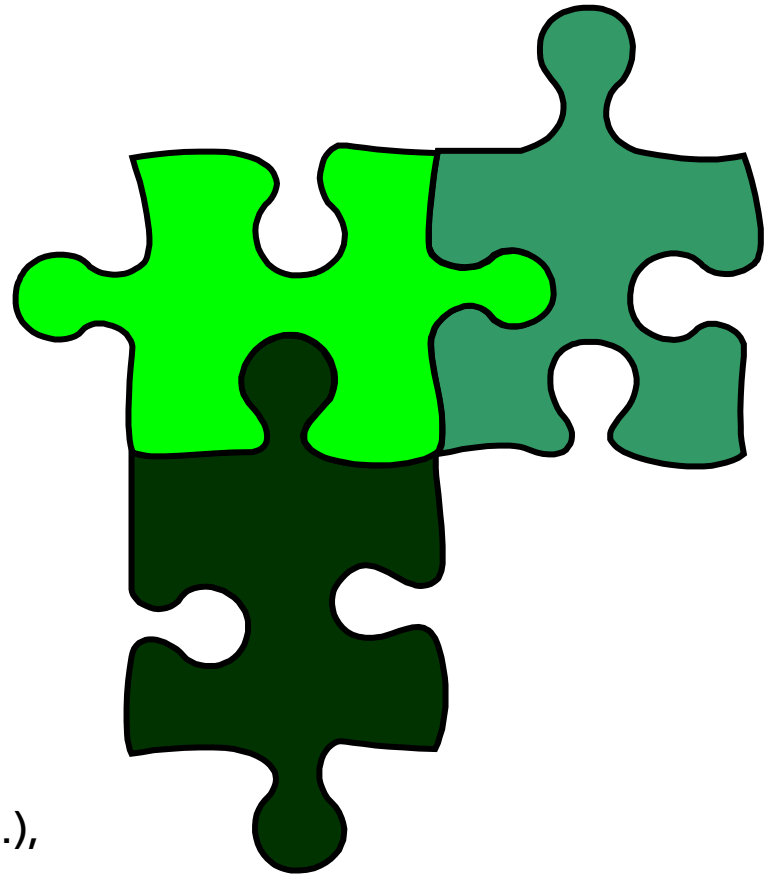
Fraunhofer SIT Institut Sichere Informations-Technologie

EUROFORUM The Conference Company

Überblick

- Aufbau und aktueller Stand
- Optische Identifikationsmerkmale (Sichtausweis / Europäische Krankenversicherungskarte)
- Plattform
- Sicherheitsarchitektur
- Authentisierungsverfahren
- Anwendungsstruktur
- Gesundheitsanwendung (HCA)
- PKI-Anwendung (ESIGN)
- Szenarien (eTicket-Verfahren / eKiosk)

Aufbau und aktueller Stand



Technische Basisspezifikationen der eGK

Teil 1: Kommandos, Algorithmen und Funktionen der Betriebssystem-Plattform; Version 1.1.0; 7.2.2006

Teil 2: Anwendungen und anwendungs-spezifische Strukturen; Version 1.1.1; 23.3.2006

Teil 3: Äußere Gestaltung; Version 1.1.0; 7.2.2006

Weitere Komponenten-Spezifikationen:

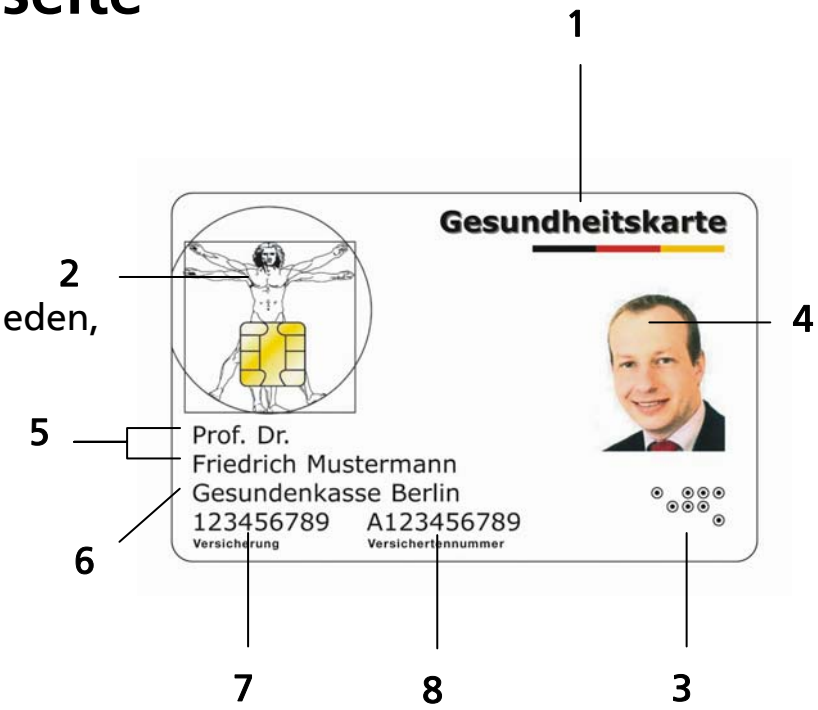
Karten-Terminal (eHealth-Terminal, SICCT-Terminal), Konnektor

Konzepte:

Fachkonzepte (Anwendungen des Versicherten, VODM, VSDM, …), PKI-Infrastrukturen für CVC, X509, Aktivierung der qualifizierten Signatur, eGK Produktion …

Link: http://www.gematik.de

Optische Identifikationsmerkmale / Vorderseite



Allgemeine Merkmale:

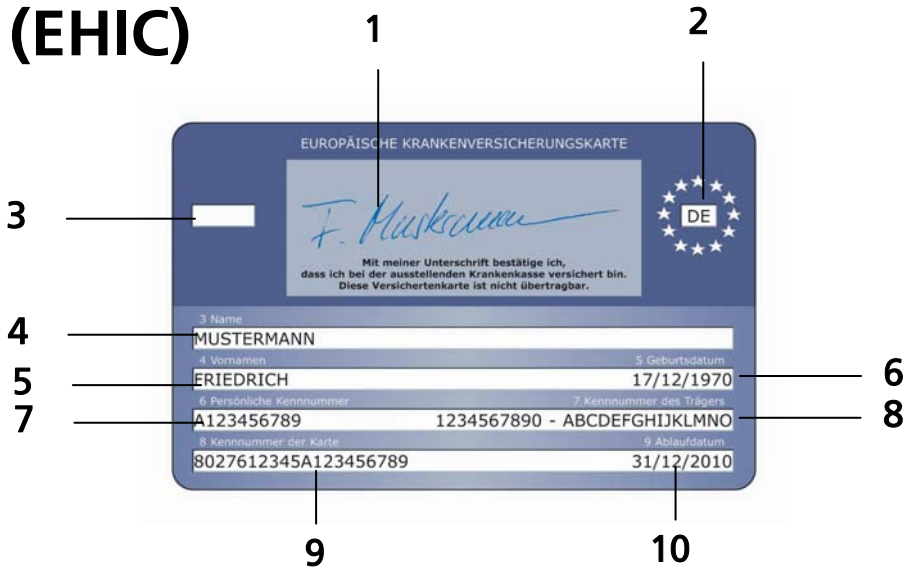
1. Einheitliche Kartenbezeichnung der eGK
2. Einheitliches Karten-Logo
3. Schriftzug „egk“ in Blindenschrift; in der Testphase wird entschieden, ob Merkmal generell verpflichtend wird

Identifikationsmerkmale
Gesetzliche Regelungen: §291 Abs. 2 und §291a Abs. 2 SGB V

4. Foto des Versicherten ab dem 16. Lebensjahres (Ausnahme: Versicherte, deren Mitwirkung bei der Erstellung des Lichtbildes nicht möglich ist) **Nicht** digital zu speichern
5. Titel, Vorname, Nachname des Karteninhabers (2 Zeilen mit max. 28 Zeichen); elektronisch überprüfbar
6. Name der herausgebenden Kasse; elektronisch überprüfbar
7. 9-stelliges bundesweit einheitliches Institutionenkennzeichen des Kostenträgers; elektronisch überprüfbar
8. unveränderlicher Teil der KVNR (die ersten 10 Stellen) nach §290 SGB V; elektronisch überprüfbar

Optische Identifikationsmerkmale / Rückseite Europäische Krankenversicherungskarte (EHIC)

- Nachweis der Gesundheitsversorgungsberechtigung im Europäischen Ausland gemäß Beschluss der EU-Kommission Nr. 190 vom 18. Juni 2003
- EHIC ersetzt E 111-Formulare
- Derzeit nur als Sichtausweis geplant; elektronischer Datensatz ab 2008
- Die verbindliche Aufnahme auf der Rückseite der eGK wird in der Testphase entschieden

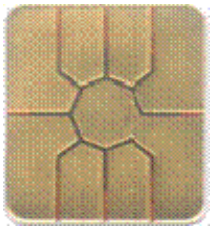


1) Nationales Feld: Unterschiftenfeld
2) Kennnummer des Ausgabestaats (DE für Deutschland)
3) Bezeichnung des Vordrucks (bei deutscher EHIC leer)
4) Name des Karteninhabers
5) Vorname(n) des Karteninhabers
6) Geburtsdatum (TT/MM/YYYY)
   (→ gemäß der in Deutschland üblichen Angaben)
7) Persönliche Kennnummer des Karteninhabers (→ die ersten 10 Stellen der KVNR)
8) Kennzeichnung des zuständigen Kostenträgers (Institutionenkennzeichen des Kostenträgers - Akronym)
9) Fortlaufende Kennnummer der Karte (= ICCSN in der Karte)
10) Ablaufdatum (TT/MM/YYYY)

Fraunhofer SIT Institut Sichere Informations-Technologie

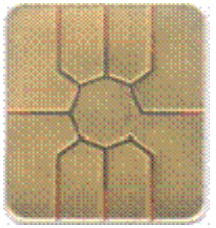
EUROFORUM The Conference Company

Chip in der eGK



- Kontaktbehaftete Mikroprozessorkarte mit Crypto-Controller (Computer im Kleinstformat) => Kartenlesegerät erforderlich
- Betriebssystem-Plattform entspricht internationalen Standards => europäische und internationale Interoperabilität sichergestellt.
- Speicherkapazität: Umfang der zu speichernden Daten ca. 34 KByte
- Sicherheitszertifizierung zum Nachweis der Sicherheitseigenschaften nach Common Criteria, da eGK zentrale Sicherheitskomponente der Telematik-Infrastruktur => Schutzprofile als Basis der Sicherheitszertifizierung im Auftrag des BMG und des BSI erstellt und veröffentlicht unter: http://www.bsi.bund.de/cc/pplist/pplist.htm

Plattform / 2



- Karten-Anwendungen und Dateien nach Kartenausgabe nachladbar und löschbar
- Dateien und Datensätze aktivierbar / deaktivierbar (wichtig für das Patienten-Rechte-Management)
- Kommandos zum Lesen / Schreiben / Hinzufügen von Daten / Suchen von Informationen in Datensätzen
- Unterstützung von sog. „Security Environments“, d.h. unterschiedliche Sätze von Zugriffsregeln können koexistent vorhanden sein, um verschiedene Anwendungsszenarien wie z.B. lokaler Zugriff auf eine Karte oder Zugriff durch eine internet-basierte Instanz zu unterstützen
- Unterstützung eines „Trusted Channels“ durch Secure Messaging (jedes Kommando und jede Antwort wird mit einer kryptografischen Prüfsumme versehen und Daten können auch verschlüsselt werden) (Sicherheit gegen Datenschutzverletzungen)
- Kryptografische Algorithmen, Authentisierungsverfahren

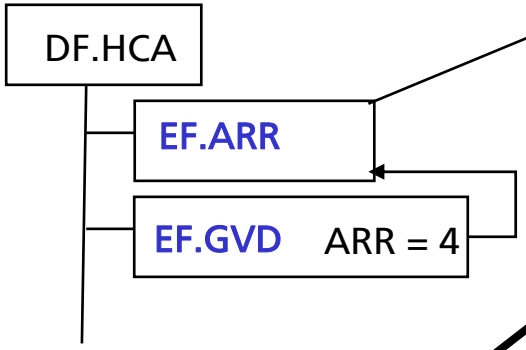
Sicherheitsarchitektur

- Sicherheitsarchitektur gemäß SmartCard-Standard ISO 7816-4
- Jedem Datenobjekt (Schlüssel, Datei) sind Sicherheitsattribute (= Zugriffsregeln) zugeordnet.
- Zugriffsregeln in der Datei EF.ARR (Access Rule References)
- Eine Zugriffsregel ist eine Kombination von Access Mode & Security Condition(s),z.B.:
  Access Mode (AM) = Lesen
  Security Condition (SC) = Benutzer-Authentisierung mit PIN
- Die Security Conditions sind statisch, aber flexibel gestaltbar; Unterstützung von UND- und ODER-Verknüpfungen mehrer Bedingungen möglich
- Jeder Zugriff wird von eGK auf Zulässigkeit geprüft, d.h. wenn Security Conditions nicht erfüllt sind, wird der Zugriff nicht ausgeführt
- Zur Prüfung der Sicherheitsbedingungen wird der Sicherheitsstatus der Karte verwendet

Sicherheitsarchitektur
Beispiel

In der eGk sind in der Datei EF.GVD schutzbedürftige Versicherungsdaten gespeichert

Die Daten dürfen nur von einem Leistungserbringer (Arzt / Zahnarzt od. Apotheker od. Psychotherapeut od. Sonstige Leistungserbringer) nach erfolgreicher CV-Authentisierung ODER vom Versicherten nach Benutzerauthentisierung mittels PIN.home gelesen werden



4. Zugriffsregel für EF.GVD

AM: READ BINARY

SC: OT Template
{AT (UQ = Ext. Auth., CHA = CHA.i, i=2-5 ||
AT (UQ = User Authentication, KeyRef =PIN.home)
}

AM: UPDATE BINARY

SC: AND Template
{ AT (UQ = Ext. Auth., KeyRef = SK.VSDD) ||
CCT (UQ = CC in SM-Kdo. und SM-Antwort) ||
CT (UQ = CG in SM-Kdo und SM-Antwort)
}

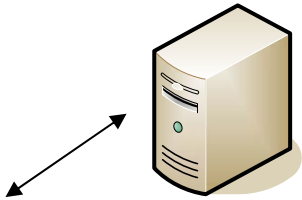
Aktualisierung der Daten nur durch den Versichertenstammdatendienst (VSDD) der Kostenträger nach erfolgreicher sym. Authentisierung mit dem Schlüssel SK.VSDD AND Secure Messaging mit Prüfsumme & Kryptogramm

Authentisierungsverfahren / 1
Authentisierung des Versicherten aus Sicht der eGK

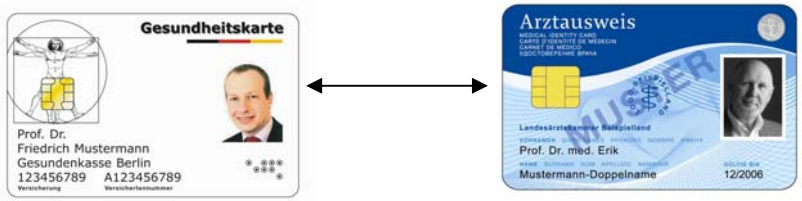
- Verfahren: PIN-Code (Besitz & Wissen)
- Drei verschiedene PINs zum Schutz bestimmter Daten und der freiwilligen Anwendungen:
  - **Cardholder-PIN (6 – 8 Ziffern)**: Erforderlich zur Nutzbarmachung freiwilliger Anwendungen bei einem Leistungserbringer (= Autorisierung des Zugriffs)
  - **PIN.home (6 – 8 Ziffern):** Erforderlich zur Wahrnehmung von Versichertenrechten an einem PC / eKiosk und zur Nutzung des privaten PKI-Schlüssels PrK.CH.AUT im Rahmen einer Client-/Server-Authentisierungsprozedur (z.B. zur Überprüfung von Zugriffsrechten auf Server,)
  - **Signatur-PIN (6 – 8 Ziffern):** Erforderlich zur Freischaltung der qualifizierten Signatur-Funktion gemäß SigG, falls vorhanden (= Identifikation des Karteninhabers)
- PINs durch Wiederholungszähler geschützt
- Versicherter kann PIN ändern => Einstellung auf denselben Wert möglich
- Bei den Pflichtanwendungen erfolgt keine Autorisierung durch den Versicherten

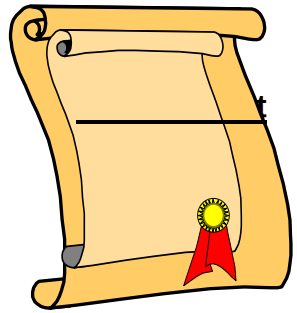
Authentisierungsverfahren / 2
Authentisierung einer zugreifenden Instanz aus Sicht der eGK

- Symmetrisches Authentifizierungsverfahren zwischen eGK und Versichertenstammdatendienst (VSDD) zum Aktualisieren, Löschen der Versichertenstammdaten



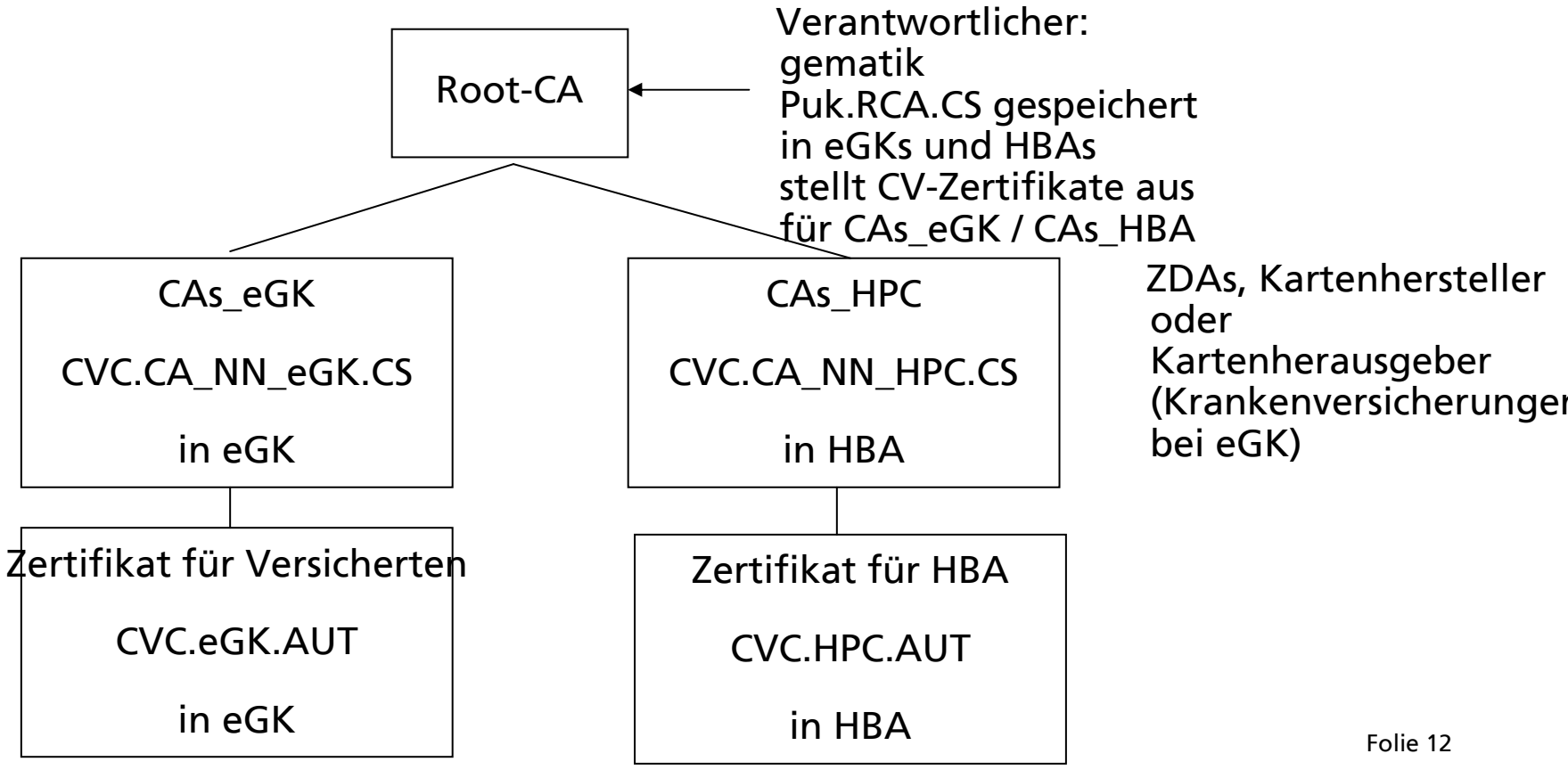
- Der Nachweis der Zugriffsberechtigung eines Heilberuflers (Arzt, Zahnarzt, Apotheker, Psychotherapeut, …) bzw. einer Institutionenkarte (SMC) gegenüber der eGK erfolgt auf Basis eines RSA-basierten Authentisierungsverfahrens mit Card Verifiable Certificates, die von der Karte interpretiert werden können; es sind **keine** X.509-Zertifikate





- Das CV-Zertifikat beinhaltet u.a.
  - den öffentlichen Authentisierungsschlüssel
  - die „Certificate Holder Authorization“ (CHA) mit Zugriffsprofil x z.B. für Arzt

Authentisierungsverfahren / 3
Hierarchie der PKI für CV-Zertifikate / vereinfachte Darstellung



Authentisierungsverfahren / 4
Aufbau eines CV-Zertifikats

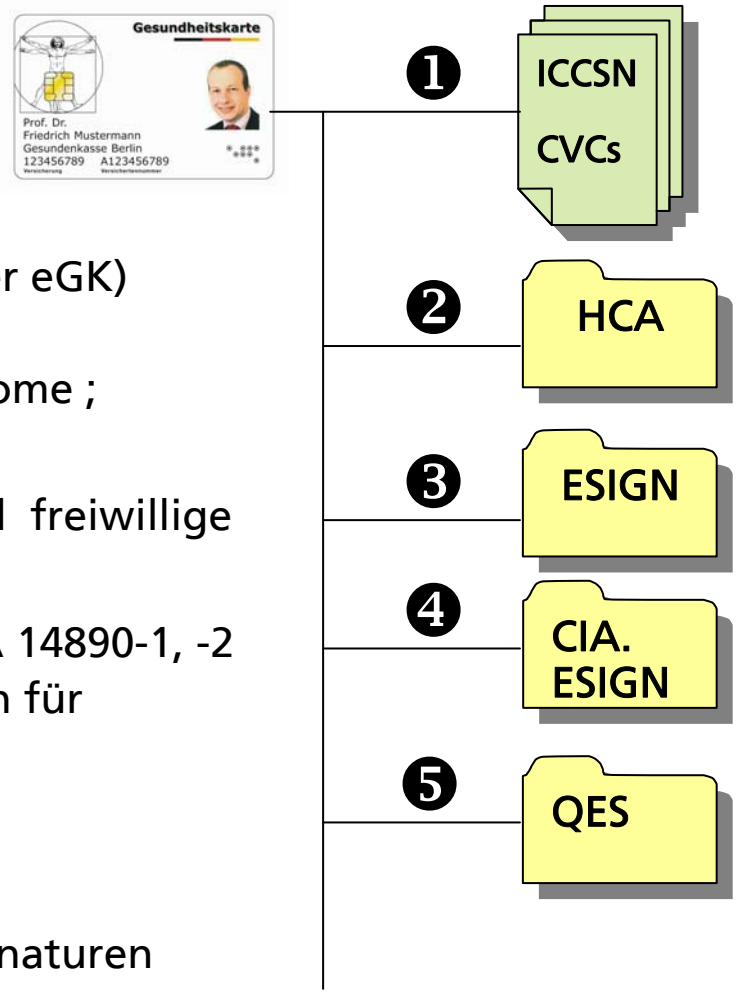
Tag	L	Value		
7F21	81CE	CV certificate (206 byte)		
		Tag	**L**	**Value**
		5F37	8180	SIG.CA (128 byte), HPC-Testlaborkarte: 8a da a0 72 4a 67 3c d2 99 a0 b0 f0 27 fb b3 53 01 f8 c1 5b b5 09 3d 20 e2 15 d0 b9 59 da e9 bb a9 d8 5b c0 33 cc 08 b4 15 5f 19 25 c2 95 c0 6c 6c 1f ef 70 29 e5 ad a8 7d 88 af 2a 39 01 3e ee 15 4f c5 2d 75 8d 74 00 8a 23 08 d8 dd 41 e3 78 3a dc bc 16 35 53 18 64 af 0d 78 9a f8 a5 0b 94 a7 2b 44 b1 61 c2 46 34 dc 43 1f 4e 26 e9 dc 4f a2 03 ad 3d 50 af b7 2b 9a 78 b2 5e 42 a5 8d cc
				Digital Signature Input for SIG.CA (6A ... BC):
				6A = Padding acccording to ISO 9796-2
				03 = CPI
				CAR (8 byte)
				CHR (12 byte)
				CHA (7 byte)
				OID (7 byte)
				PK part 1 (first part of modulus, 71 byte)
				Hash (20 byte, Hash Input: CPI | CAR | CHR | CHA | OID | PK
				BC = Trailer
		5F38	3D	PK remainder (rest of modulus followed by public exponent 00 01 00 01, 61 byte), HPC-Testlaborkarte (62 Byte!): 3d 11 74 1c e6 fe b1 99 69 b6 31 b2 8d 0a d6 1b 64 e8 28 b7 0f 54 4f f5 0d 41 e1 65 53 3c 76 a1 21 e1 58 91 83 37 a 4d 46 02 68 55 52 f3 ca 3f a2 c3 a0 c5 06 45 82 b3 bf a2 bf 00 01 00 01
		42	08	CAR (8 byte), HPC-Testlaborkarte: 30 30 30 30 31 11 00 56 (?)

Authentisierungsverfahren / 5
CV-basierte Authentisierung

- Zweistufige Zertifikatsprüfung

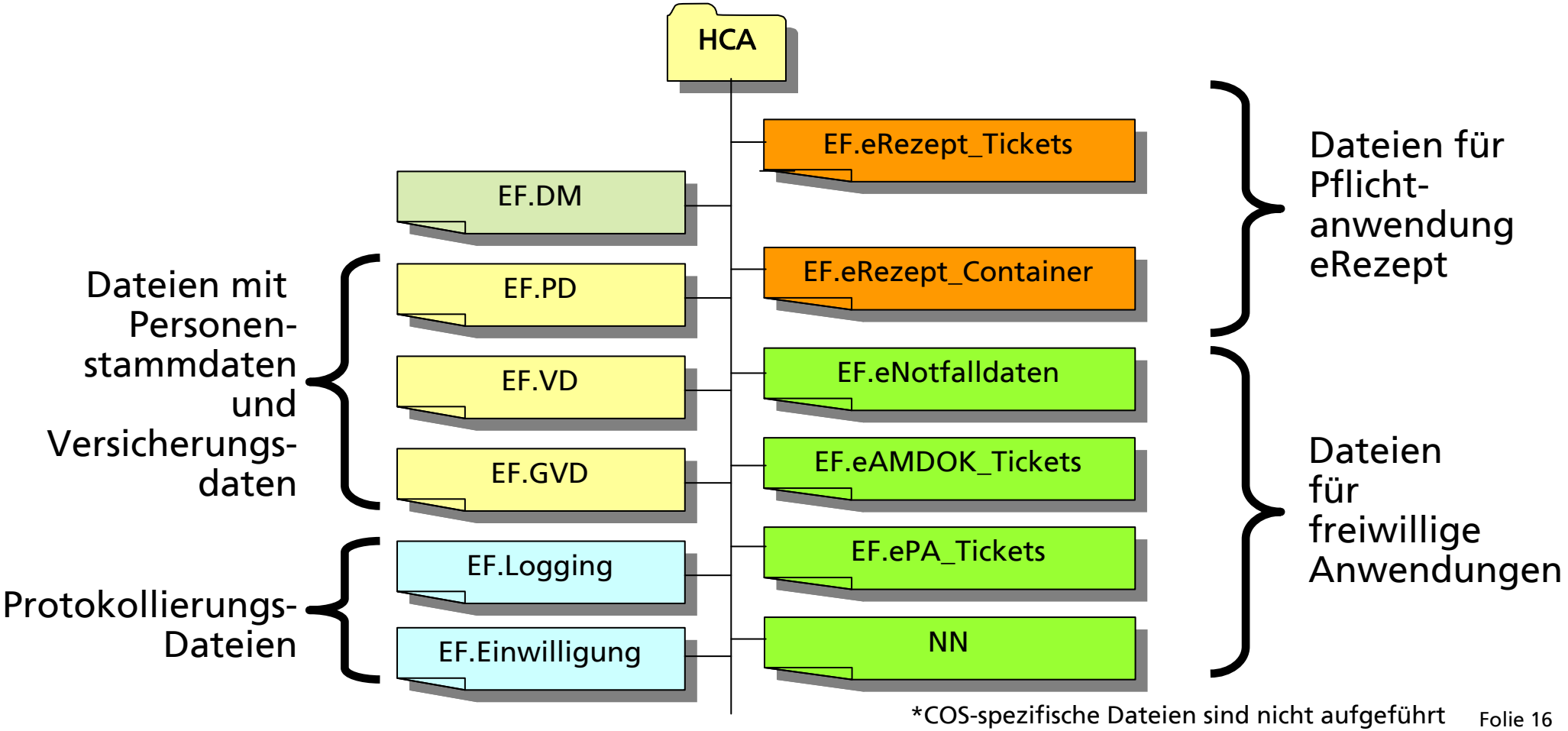
1. Import und Prüfung des CV-Zertifikats der ausstellenden Instanz für den HBA (CVC.CA_HPC.CS); in der eGK ist zur Prüfung der CVC.CA-Zertifikate von Heilberuflern der Public Key der gemeinsamen Root-CA eingetragen.
2. Nach erfolgreicher Prüfung hat die eGK den Public Key zur Verfügung, den sie benötigt, um anschließende das CV-Zertifikat des Heilberuflers (CVC.HPC.AUT) verifizieren zu können.
3. Import und Prüfung des CV-Zertifikats des Heilberuflers
4. Nach erfolgreicher Prüfung speichert die eGK den öffentlichen Authentisierungsschlüssel des HBA und das Zugriffsprofil (=CHA)
5. Ausführung des Authentisierungsverfahrens; bei erfolgreicher Ausführung wird in der eGK der Sicherheitsstatus „CHA x erfolgreich präsentiert“ (z.B. CHA = Arzt) gesetzt
6. Greift die betreffende Instanz z.B. lesend auf eine bestimmte Datei zu und ist der Zugriff an eine bestimmte Rolle (CHA) geknüpft, dann prüft die eGK, ob im Authentisierungsverfahren die entsprechende Rollenkennung (z.B. CHA=Arzt) präsentiert wurde.

Anwendungsstruktur



1. **Gobale Datenobjekte** u.a:
   - ICCSN = Identifikationsmerkmal der eGK
   - CV-Zertifikate der eGK (Root-CV-Zertifikat, CV.AUT-Cert der eGK)
   - Liste, der in der eGk vorhandenen Anwendungen
   - globale Schlüsselobjekte (Karteninhaber-PIN PIN.CH, PIN.home ; 3DES-Schlüssel für die Interaktion eGK und VSDD, …)
2. **HCA**: Gesundheits-Anwendung für Pflichtanwendungen und freiwillige Anwendungen gemäß GMG
3. **ESIGN**: PKI-Anwendung Europäischer Signaturstandard CWA 14890-1, -2 zur Bereitstellung von X509-basierten Sicherheitsfunktionen für Verschlüsselung und Client/Server-Authentisierung
4. **CIA.ESIGN**: Cryptographic Information Application (ESIGN-Ergänzungsanwendung)
5. **QES**: Anwendungsrahmen für qualifizierte elektronische Signaturen (DIN V66291-4); komplettierbar nach Kartenausgabe

HCA Gesundheitsanwendung

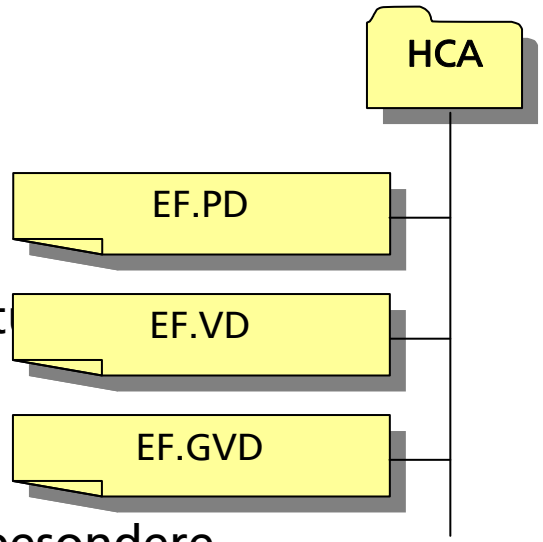


*COS-spezifische Dateien sind nicht aufgeführt

Fraunhofer SIT Institut Sichere Informations-Technologie

EUROFORUM The Conference Company

Personenstammdaten und Versicherungsdaten / 1
Umfang der gespeicherten Daten



- **EF.PD**: Personenstammdaten zur Identifikation des Versicherten (Name, Geburtsdatm, Geschlecht, KVNR, Anschrift, Aktualisierungs-/Prüfdatum)
- **EF.VD**: Versicherungsdaten (GKV/PKV) **ohne** Schutzbedürfnis (Angaben zum Kostenträger, Versicherungsart, Versichertenstat Beginn des Versicherungsschutzes, Kostenerstattung, stationäre Leistungen, Aktualisierungs-/Prüfdatum)
- **EF.GVD**: Versicherungsdaten (GKV) **mit** Schutzbedürfnis (DMP-Kennzeichen (SGB V §291 Abs. 2 Nr. 7), Kennzeichen für besondere Personengruppen (SGB V §291 Abs. 2 Nr. 7), Angaben zum Zuzahlungsstatus (SGB V §291 Abs. 2 Nr. 8), Aktualisierungs-/Prüfdatum)
- Entsprechen denen in der bisherigen Versichertenkarte, sind aber um einige Datenobjekte nach SGB V §291 ergänzt
- Struktur und Kodierung sind konform zur EHIC und ISO 21549-5 und –6 => Europa-weite Nutzung

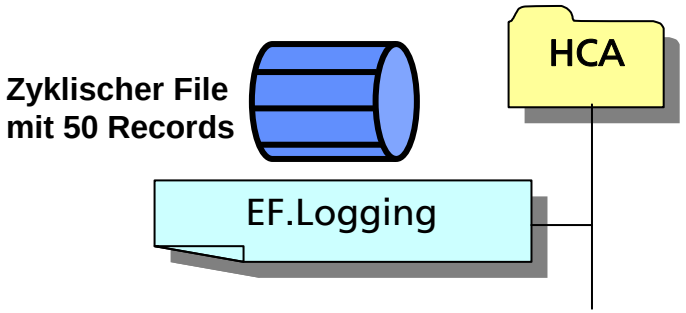
Personenstammdaten und Versicherungsdaten / 2
Zugriffsrechte & Sicherheitsbedingungen

	Zugriff	Arzt	Apo-theker	Psycho-thera-peut	Andere HPs	Versand-apo-theke	Vers. @home	Vers. @eKiosk	Kosten-träger
EF.PD	READ	always	always	always	always	always	always	always	
	Update	-	-	-	-	-	-	-	SK.VSDD
EF.VD	READ	always	always	always	always	always	always	always	
	UPDATE	-	-	-	-	-	-	-	SK.VSDD
EF.GVD	READ					-	PIN.home	PIN.home	
	Update	-	-	-	-	-	-	-	SK.VSDD

- Der Kostenträger besitzt das alleinige Schreibrecht
- Aktualisierung der Daten erfordert sym. Authentisierung & Secure Messaging mit Prüfsumme und Kryptogramm (Trusted Channel) zwischen eGK und SMC (Kostenträger)

Zugriffsprotokoll

- Die letzten 50 Zugriffe auf Patientendaten sind gemäß §291 a Abs. 6 SGB V für Zwecke der Datenschutzkontrolle zu protokollieren
- **4W: Wer** hat auf **Welche** Daten **Wann** und **Wie** zugegriffen.
- Revisionssicherheit ist nicht erforderlich (Entscheidung des Architekturboards vom 17.3.2006)
- Lesen nur durch Karteninhaber nach Eingabe von PIN.home
- Eintragung durch PVS/AVS des Heilberuflers nach C2C-Authentisierung zwischen HBA & eGK
- Änderung der Daten nicht möglich
- Logging-Daten werden der eGK übergeben



	Zugriff	HB	V
EF.Logging	READ	-	PIN.home
	Append		-

Vorschlag: Teil2 der eGK-Spezifikation

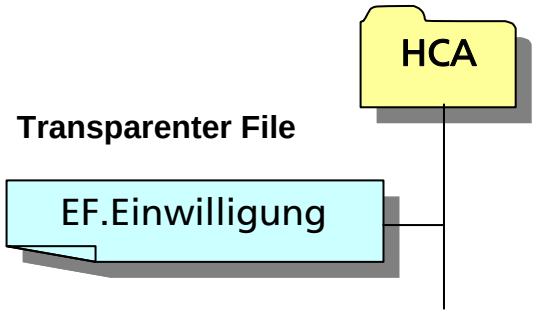
Datum (4 Byte; BCD)	HB-Be-zeichnung (23 Byte)	HBA-ICCSN (10 Byte)	Kennzeichnung der zugreifenden Person (1 Byte)	Kennzeichnung der Anwendung und Art des Zugriffs (2 Bytes)
TTMMYYYY	z.B. HNO Dr. Müller		00 = HB 0x = durch HB autorisierte Person	

Fraunhofer SIT Institut Sichere Informations-Technologie

EUROFORUM The Conference Company

Einverständniserklärung

- § 291a SGB V Abs. 3: Die Einwilligung des Versicherten zum Erheben, Verarbeiten und Nutzen von Daten der freiwilligen Anwendungen ist bei erster Verwendung der Karte vom Leistungserbringer auf der Karte zu dokumentieren.
- Lesen durch Karteninhaber nach Eingabe von PIN.home
- Lesen durch alle Heilberufler nach C2C-Authentisierung zwischen HBA & eGK
- Eintragung durch PVS/AVS des Heilberuflers (Arzt, Zahnarzt, Apotheker) nach C2C-Authentisierung zwischen HBA & eGK
- Änderung der Daten nicht möglich
- Daten müssen der eGK übergeben werden
- Auswertung der Daten erfolgt durch PVS / Konnektor



	Zugriff	HB	V
EF.Ein-willigung	READ		PIN.home
	Append		-

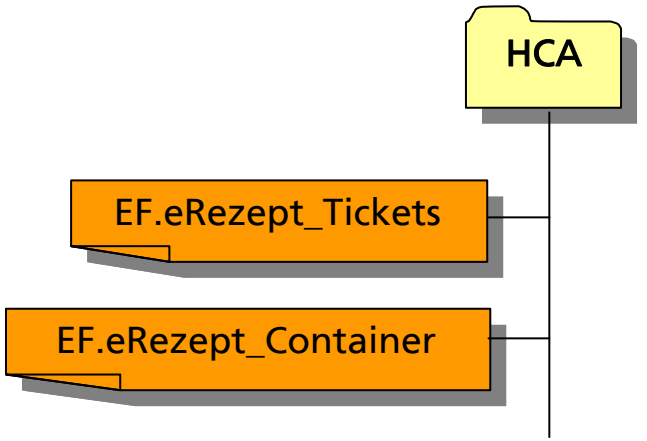
Vorschlag: Teil2 der eGK-Spezifikation

DO Flagliste für Anwendunge (1Byte)	DO Datum	DO HB-Bezeichnung und Name (10 Byte)
z.B. ‚01' = Einwilligung für eAMDOK	TTMMYYY	z.B. HNO Dr. Müller

eRezept / 1
Umfang der gespeicherten Daten

- **EF.eRezept_Ticket**
  Speicherkapazität: 5 eTickets für eRezepte auf Server
  und 5 eTickets für eRezepte

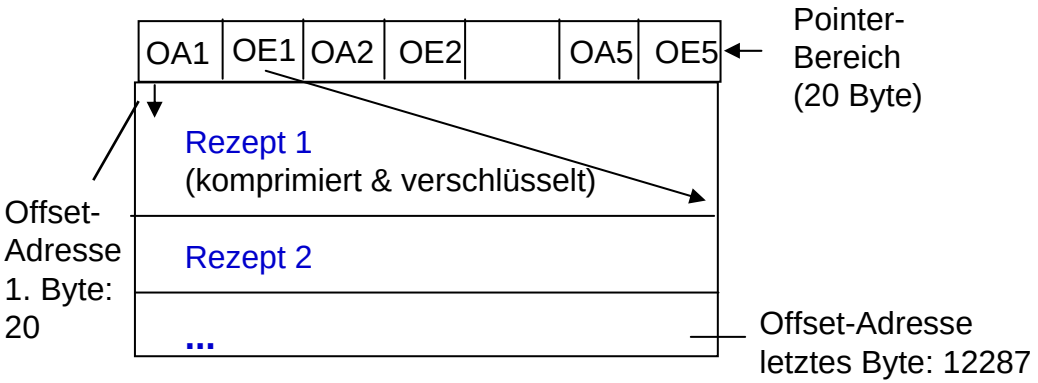
- **EF.eRezept_Container**:
  Rezepte (komprimiert XML -> ASN.1?) mit Sitzungsschlüssel verschlüsselt
  Speicherkapazität: max. 5 Rezepte



EF.eRezept-Ticket (Records max. 180 Byte)

Rec 10	eTicket für eR auf Server
	…
Rec 6	eTicket für eR auf Server
Rec 5	eTicket für eR auf eGK
	…
Rec 1	eTicket für eR auf eGK

EF.eRezept-Container
(transparente Datei von 12 KByte für max. 5 Rezepte)



OA = Offset-Anfang (2 Byte)
OE = Offset-Ende (2 Byte)

Fraunhofer SIT Institut Sichere Informations-Technologie

EUROFORUM The Conference Company

eRezept / 2
Zugriffsrechte & Sicherheitsbedingungen

- Zum Löschen eines Rezepts wird nur entsprechendes Ticket gelöscht
- Zum Ausstellen und Einlösen von Rezepten keine PIN-Eingabe nötig
- Schreibrecht haben nur die LEs, die eRezepte ausstellen dürfen
- Mit Hilfe des Kommandos DEACTIVATE RECORD können vom Versicherten eTickets verborgen werden

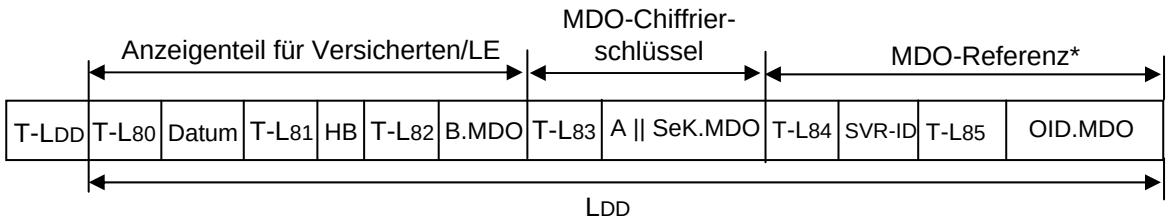
	Aktion	LE	Vers.@home	Vers.@eKiosk
EF.eRezept_Ticket	Lesen		PIN.home	
	Schreiben			
	Löschen			 & PIN.home
	Verbergen			 & PIN.home
	Sichtbarmachen			 & PIN.home
eF_eRezept_ Container	Lesen	always		
	Schreiben			
	Löschen			
	Verbergen			
	Sichtbarmachen			

- Mit Hilfe des Kommandos ACTIVATE FILE können eTickets vom Versicherten wieder sichtbar gemacht werden
- Aktive Patientenrechte (verbergen, wieder sichtbar machen und löschen) von eTickets an einem eKiosk mit Security Module Card (SMC) und Rollenkennung “eKiosk“ erlaubt (eGK / SMC-Authentisierung und PIN.home-Eingabe erforderlich)

eTicket-Konzept
Zweck und Aufbau

- eTickets = Verwaltungsobjekte für Medizinische Datenobjekte (eRezepte, freiwillige Anwendungen)
- Wichtig zur Unterstützung der Patientenrechte:
  Jedes einzelne eTicket kann durch den Versicherten individuell verwaltet werden (verbergen, wieder sicht-bar machen, löschen)

eTicket für ein medizinisches Datenobjekt



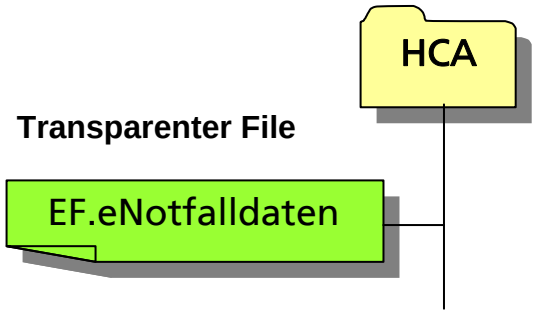
*entfällt bei Speicherung der Daten in der eGK

A = Algorithmus-Identifier (1B)
B.MDO = Bezeichnung des Med. Datenobjekts, z.B. Kurzbezeichnung Befund, Name des Medikaments
DD = Discretionary Data, Tag '73' (in diesem Fall DD = eTicket)
HB = Heilberufler, z.B. HNO Dr. Müller
LE = Leistungserbringer, z.B. Arzt
L.MDO = Länge des Med. Datenobjekts (MDO)
OID.MDO = Object Identifier des MDO auf dem Server
SeK.MDO = Session Key, mit dem das MDO verschlüsselt ist
SVR-ID = Server Identifier
T-L = Tag-Length (Tag = Identifier des Datenobjekts, z.B. '80')

LDD = max. 180 B
L80 = '04' (TTMMJJJJ, BCD-Coding)
L81 = max. 20 B (UTF8)
L82 = max. 80 (UTF8)
L83 = max. 17 B (AlgID '01'= DES-3)
L84 = max. 24 B
L85 = ma. 24 B

- eTickets werden in anwendungsspezifischen Dateien abgelegt, da unterschiedliche, anwendungsspez. Zugriffsrechte
- Ohne Ticket kein Zugriff auf die Daten möglich

eNotfalldaten

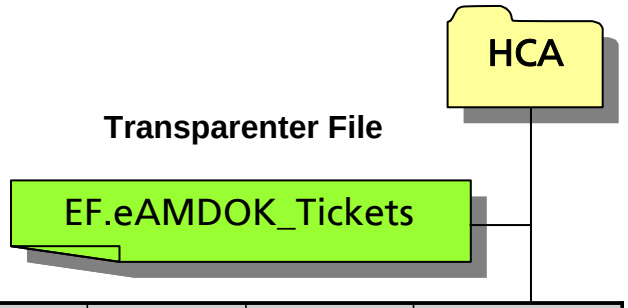


- Notfalldaten in transparenter Datei (2 KByte)
- Speicherung oder Änderung der eNotfalldaten nur mit Zustimmung des Versicherten erlaubt
  => C2C-Authentisierung (eGK / HBA) mit Rollenkennung=Arzt/Zahnarzt und PIN.CH-Eingabe erforderlich

	Aktion	LE	Vers.@home	Vers.@eKiosk
EF-eNotfalldaten	Lesen		PIN.home	
	Schreiben	& PIN.CH		
	Löschen			& PIN.home
	Verbergen			& PIN.home
	Sichtbarmachen			& PIN.home

- Lesen der eNotfalldaten durch LE erfordert C2C-Authentisierung (HBA / eGK) mit Rollenkennung=Arzt/Zahnarzt od. Psychotherapeut od. anderer Heilberufler
- Aktive Patientenrechte (verbergen, wieder sichtbar machen und löschen) der Notfalldaten an einem eKiosk mit Security Module Card (SMC) erlaubt (C2C-Authentisierung eGK/SMC mit Rollenkennung “eKiosk“ und PIN.home-Eingabe erforderlich)

eArzneimitteldokumentation



- In der eGK 2 eTickets speicherbar (Ticket für verordnete Arzneimittel und Ticket für Selbst-Medikation)
- Medizinische Daten werden über Server verwaltet/transportiert
- Speicherung der eTickets nur mit Zustimmung des Versicherten erlaubt => C2C-Auth. (eGK / HBA) mit Rollenkennung=Arzt/Zahnarzt od. Apotheker und PIN.CH-Eingabe

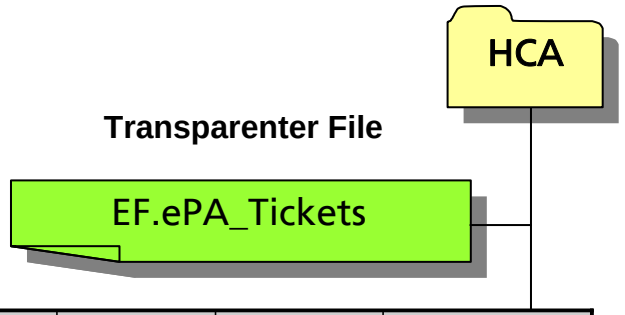
	Aktion	LE	Vers.@home	Vers.@eKiosk
EF.AMDOK_ Tickets	Lesen	& PIN.CH	PIN.home	
	Schreiben	& PIN.CH		
	Löschen			& PIN.home
	Verbergen			& PIN.home
	Sichtbarmachen			& PIN.home
	Anwendung aktivieren			& PIN.home
	Anwendung deaktivieren			& PIN.home

- Lesen der eTickets durch LE erfordert C2C-Authentisierung (HBA / eGK) mit Rollenkennung=Arzt/Zahnarzt od. Apotheker und PIN.CH-Eingabe
- Aktive Patientenrechte (verbergen, wieder sichtbar machen, löschen, Anwendung aktivieren / deaktivieren) an einem eKiosk mit SMC erlaubt (C2C-Authentisierung eGK/SMC mit Rollenkennung "eKiosk"und PIN.home-Eingabe erforderlich)

Fraunhofer SIT Institut Sichere Informations-Technologie

EUROFORUM The Conference Company

ePatientenakte

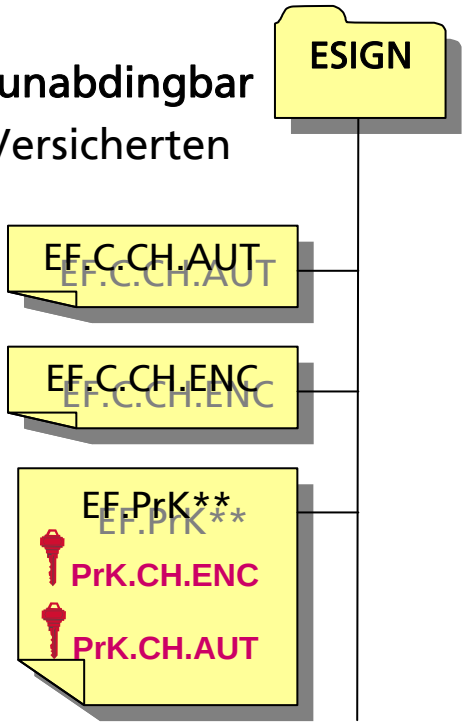


- In der eGK max. 5 eTickets speicherbar
- Medizinische Daten werden über Server verwaltet/transportiert
- Speicherung der eTickets nur mit Zustimmung des Versicherten erlaubt => C2C-Auth. (eGK / HBA) mit Rollenkennung=Arzt/Zahnarzt od. Psychotherapeut und PIN.CH-Eingabe

	Aktion	LE	Vers.@home	Vers.@eKiosk
EF.ePA_Tickets	Lesen	& PIN.CH	PIN.home	
	Schreiben	& PIN.CH		
	Löschen			& PIN.home
	Verbergen			& PIN.home
	Sichtbarmachen			& PIN.home
	Anwendung aktivieren			& PIN.home
	Anwendung deaktivieren			& PIN.home

- Lesen der eTickets durch LE erfordert C2C-Authentisierung (HBA / eGK) mit Rollenkennung=Arzt/Zahnarzt od. Psychotherapeut und PIN.CH-Eingabe
- Aktive Patientenrechte (verbergen, wieder sichtbar machen, löschen, Anwendung aktivieren / deaktivieren) an einem eKiosk mit SMC erlaubt (C2C-Authentisierung eGK/SMC mit Rollenkennung "eKiosk" und PIN.home-Eingabe erforderlich)

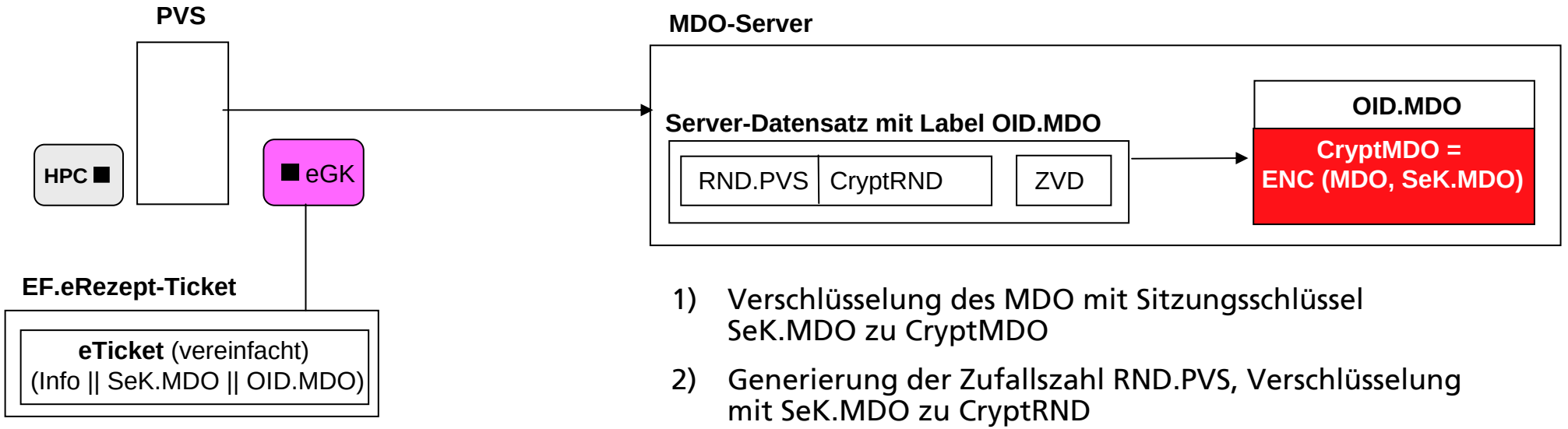
ESIGN Anwendung



- X.509-basierte Sicherheitsfunktionen für ID-Management und Datenschutz **unabdingbar**
- Die eGK enthält X.509-Authentifizierungszertifikat zur Identifizierung des Versicherten gegenüber einem System
- Kryptografische Berechnungen mit privatem Schlüssel PrK.CH.AUT (z.B. Signieren von Authentisierungstoken) erfolgen nur in der eGK
- Nutzung von PrK.CH.AUT erfordert PIN.home-Präsentation
- Die eGK enthält X.509-Verschlüsselungszertifikat
- MDOs auf Servern (ohne eTicket in eGK) werden hybrid verschlüsselt
  - Daten werden mit einem Sessionkey (SeK) verschlüsselt
  - SeK wird mit dem öffentlichen Schlüssel des Versicherten verschlüsselt (eGK nicht involviert)
  - SeK kann nur mit dem privaten Schlüssel PrK.CH.ENC des Versicherten in der eGK entschlüsselt werden

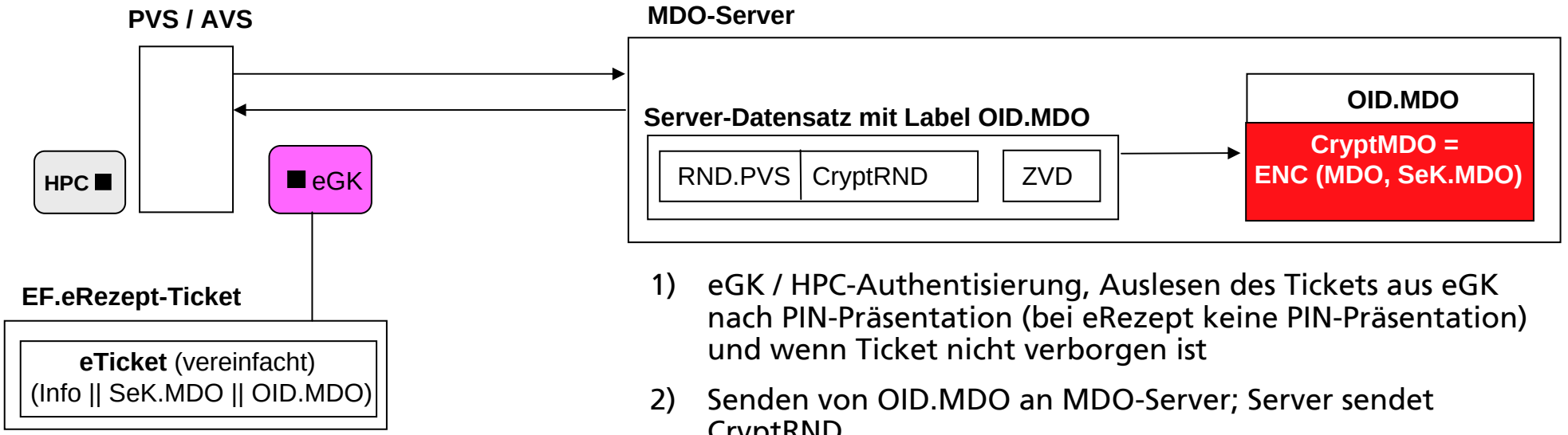
  => „Solange ich meine eGK in der Tasche habe, kann niemand unberechtigt an meine Daten."
- Nutzung von PrK.CH.ENC erfordert PIN.home-Eingabe od. C2C-Authentisierung ohne TC (Einlösung von eRezepten auf Server in Apotheke) od. C2C-Authentisierung mit TC (Einlösen von eRezepten im Versandprozess)

Szenarien / 1
Ticketverfahren (Ticket in eGK und Daten auf Server)



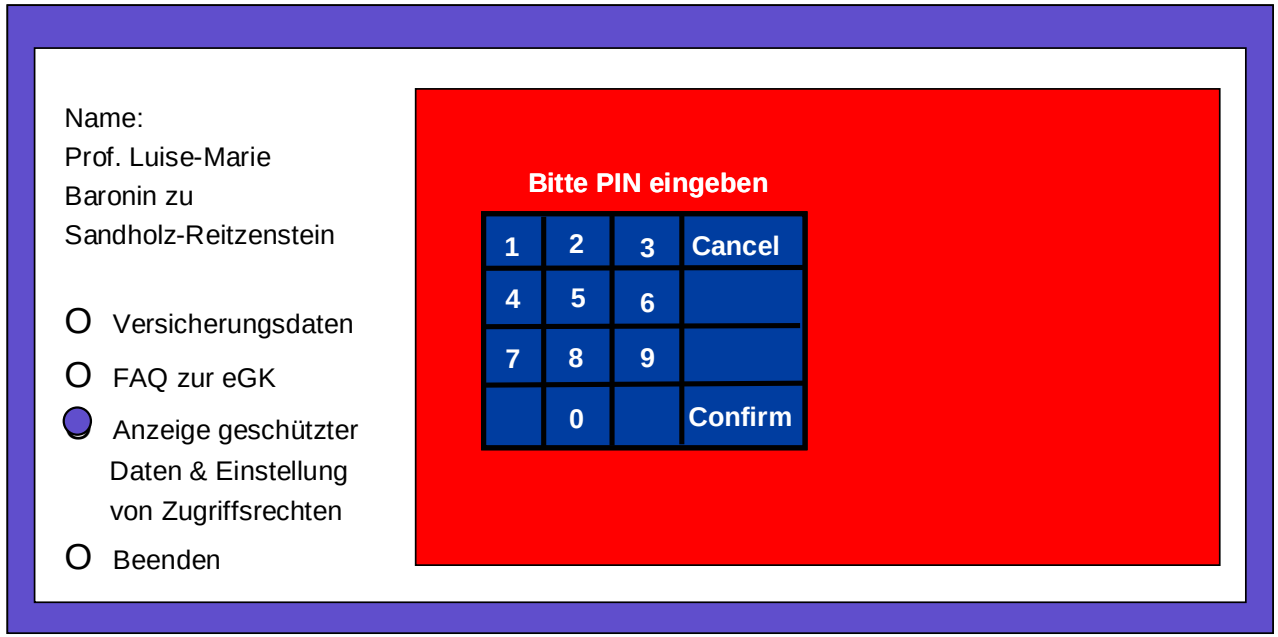
1) Verschlüsselung des MDO mit Sitzungsschlüssel SeK.MDO zu CryptMDO
2) Generierung der Zufallszahl RND.PVS, Verschlüsselung mit SeK.MDO zu CryptRND
3) Ablage von CryptMDO unter OID.MDO; Speicherung von (RND.PVS, CryptRND) unter Label OID.MDO
4) eGK / HPC-Authentisierung; Eintrag des Tickets in der eGK nach Präsentation von PIN.CH (bei Rezept keine PIN-Präsentation)
5) Schreiben des Log-Datensatzes in die eGK

Szenarien / 2
Ticketverfahren (Ticket in eGK und Daten auf Server)



1) eGK / HPC-Authentisierung, Auslesen des Tickets aus eGK nach PIN-Präsentation (bei eRezept keine PIN-Präsentation) und wenn Ticket nicht verborgen ist
2) Senden von OID.MDO an MDO-Server; Server sendet CryptRND
3) Entschlüsselung von CryptRND mit SeK.MDO; RND an Server
4) MDO-Server verifiziert RND = gespeicherte RND und sendet – falls wahr – CryptMDO
5) CryptMDO wird mit SeK.MDO entschlüsselt
6) Schreiben des Log-Datensatzes in die eGK

Szenarien / 3
Ausübung aktiver Patientenrechte an einem eKiosk

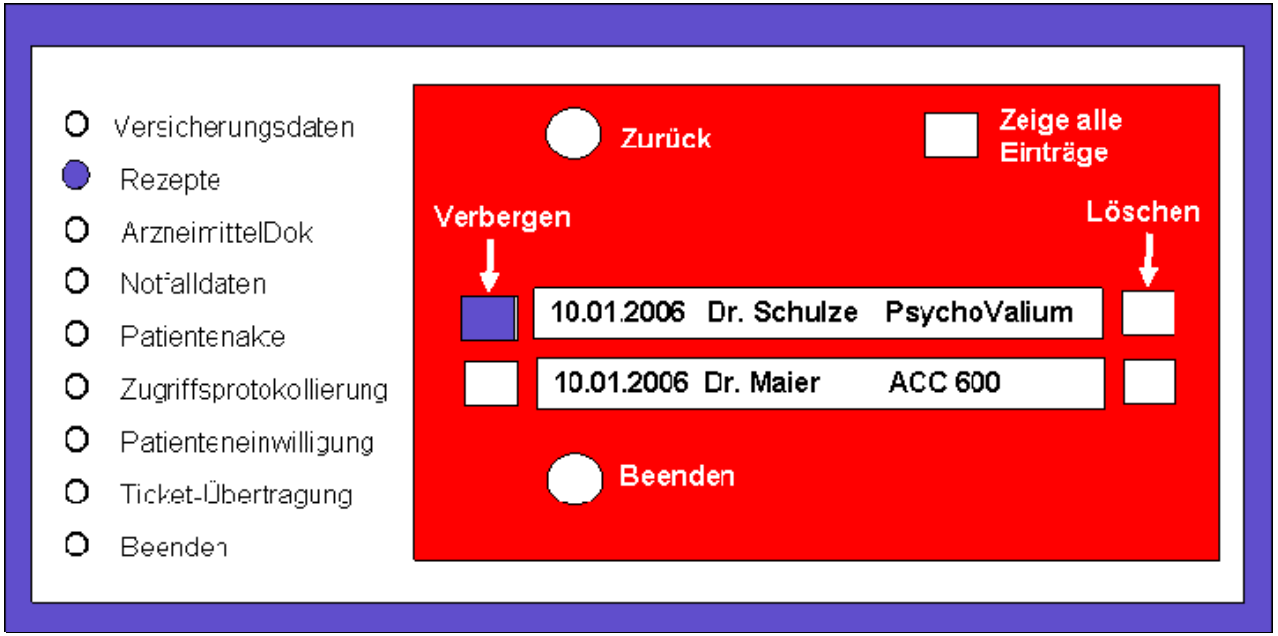


- eKiosk enthält
  Security Module Card (SMC)
  mit Zugriffsprofil "eKiosk"
- SMC muss durch einen
  Heilberufler autorisiert werden
  bevor sie eine SMC/eGK Authentifizierung ausführen kann
- Vor Ausführung aktiver Patientenrechte muss sich der Versicherte durch Eingabe seiner PIN.home identifizieren und es erfolgt eine eGK / SMC-Authentisierung

Fraunhofer SIT Institut Sichere Informations-Technologie

EUROFORUM The Conference Company

Szenarien / 4
Ausübung aktiver Patientenrechte an einem eKiosk



Beispiel: eRezept:

- eRezept verbergen
- eRezept wieder sichtbar machen
- eRezept löschen

Fraunhofer SIT Institut Sichere Informations-Technologie

EUROFORUM The Conference Company

Vielen Dank für Ihre Aufmerksamkeit

Fraunhofer SIT Institut Sichere Informations-Technologie

EUROFORUM The Conference Company