

# FMH-HPC - Technische Beschreibung

Version 1.0, 01.09.2009

## Inhaltsverzeichnis

1	Übersicht.....	1
1.1	Layout Schema der FMH-HPC.....	2
2	Technische Details.....	3
2.1	Siemens CardOS V4.3B.....	3
2.2	Chip SLE66CX322P.....	3
2.3	Card Middleware.....	3
2.4	Systemanforderungen.....	4
2.5	Kartenleser.....	4
2.6	Interoperabilität.....	4
3	eCH-0064.....	5
3.1	eCH-0064 – CVC Entwurf für FMH-HPC.....	7
	Referenzen:.....	8

## 1 Übersicht

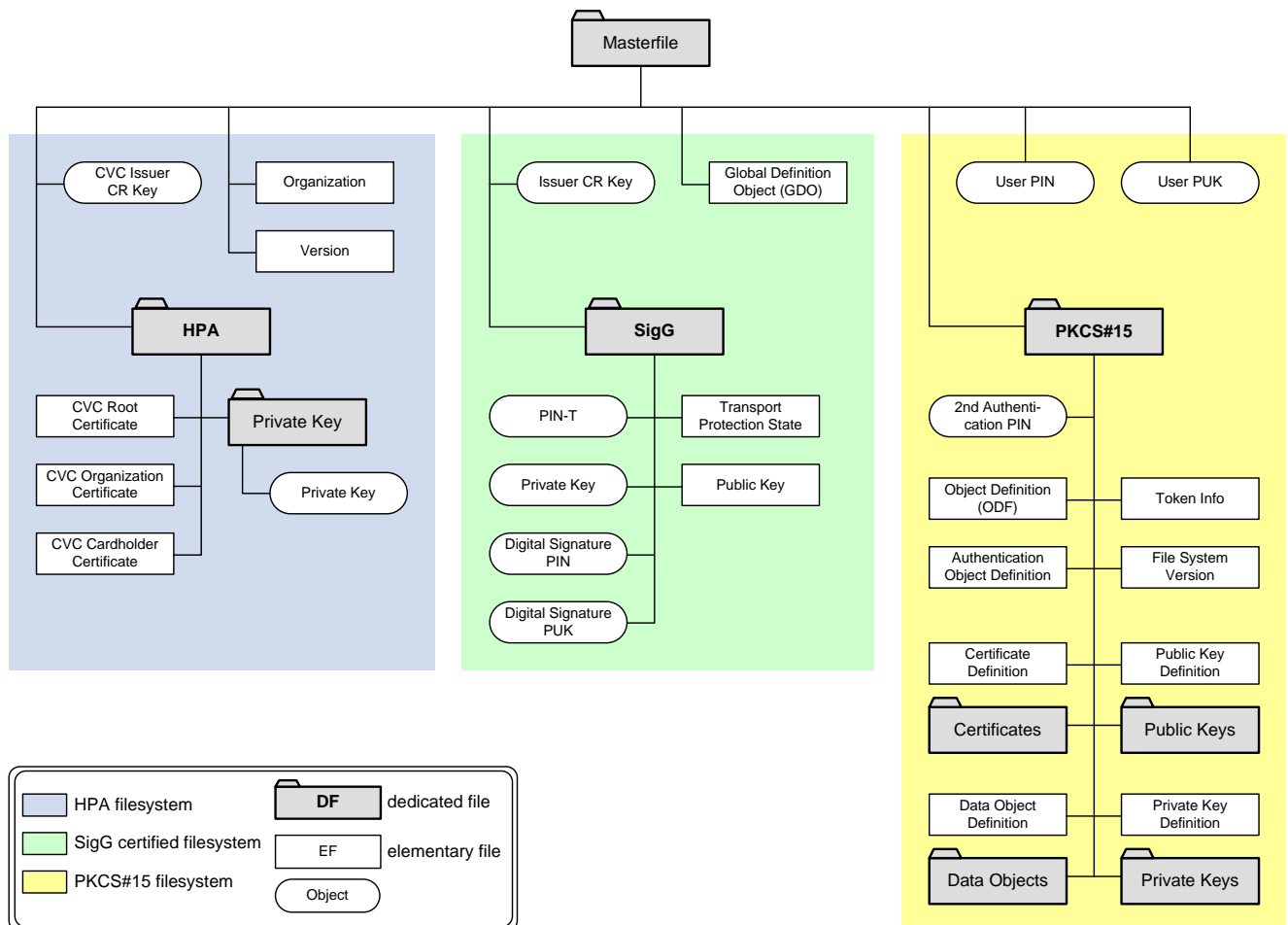
Die Health-Professional-Card der FMH (FMH-HPC) ist eine Chipkarte nach ISO 7816. Bestückt mit einem Infineonchip SLE66CX322P mit 32-Kbyte-EEPROM und dem Siemens Chipkartenbetriebssystem HiPath Security CardOS V4.3B „Re\_Cert with Application for Digital Signature“.

Dieser Chip erfüllt die Anforderung an eine sichere Signaturerstellungseinheit, SSEE (Secure Signature Creation Device - SSCD) nach dem „Bundesgesetz über die elektronische Signatur, ZertES“ (SR 943.03).

### 1.1 Layout Schema der FMH-HPC

Auf der FMH-HPC sind die folgenden 3 Umgebungen initialisiert:

- a) PKCS#15-Standardumgebung für X.509-Zertifikate nach ISO 7816-15 kompatibel mit PKCS#11-Schnittstellen.
- b) SigG-Umgebung für die qualifizierte elektronische Signatur nach ZertES<sup>1</sup>.
- c) eVK-kompatibel HPA(Health Professional Application)-Umgebung nach eCH-0064 V1.0 vom 04. Februar 2008 (Versichertenkarte).



<sup>1</sup> „Bundesgesetz über die elektronische Signatur, ZertES“ (SR 943.03).

## 2 Technische Details

### 2.1 Siemens CardOS V4.3B

HiPath Security CardOS V4.3B ist ein multifunktionales Smartcard-Betriebssystem. Es bietet sowohl aktiven als auch passiven Schutz für gespeicherte Daten, Zertifikate und kryptographische Schlüssel.

#### CardOS V4.3 B Eigenschaften

Betriebssystem:	CardOS V4.3 B
Hashes/MACs	SHA-1, MAC, Retail-MAC
asymmetrische Verfahren	RSA bis 2048 Bit (PKCS#1) auf Basis des CRT
symmetrische Verfahren	Triple-DES (ECB, CBC), DES (ECB, CBC),
Kommunikation:	T=1
Standards	ISO 7816-4,8,9
Zertifizierung	laufende CC EAL 4+
Schutz	gegen "Differential Fault Analysis", "Simple Power Analysis (SPA) und Differential Power Analysis (DPA)

### 2.2 Chip SLE66CX322P

Security	16 Bit Security Controller mit Memory Management und Protection Unit, 0,22 µm CMOS
Speicherkapazität	136-Kbytes ROM, 4Kbytes XRAM, 256 bytes internal RAM, 700 bytes Crypto RAM., 32-Kbytes EEPROM
Kryptographie	1100-Bit Advanced Crypto Engine, 112-Bit / 192-Bit DDES-EC2 Accelerator
Standards	ISO/IEC 7816 EMV 2000 GSM 11.11, 11.12,
Verbrauch und Spannung	< 10 mA @ 5.5 V < 6 mA @ 3.3 V < 4 mA @ 1.98 V

### 2.3 Card Middleware

Für die Nutzung der FMH-HPC steht eine Middleware (Card API) mit folgenden Standardschnittstellen zur Verfügung:

- Microsoft Crypto Service Provider
- PKCS#11 Cryptomodul
- Mac Key Chain
- Token Administration Utility

## **2.4 Systemanforderungen**

Um die Middleware einzusetzen zu können, muss eine PC/SC-Schnittstelle aktiv sein. Derzeit werden der folgenden Plattformen unterstützt:

- Windows XP
- Windows Vista
- Mac OS X 10.5.7 Intel

## **2.5 Kartenleser**

Die FMH-HPC ist für den Gebrauch mit Standardkartenleser konzipiert. Jeder PC/SC-kompatible Smartcard-Reader mit extended APDU wird unterstützt. Pinpad-Leser müssen PC/SC V2.01 10 unterstützen.

## **2.6 Interoperabilität**

Applikationen, die gemäss 2.3 auf die Middleware zugreifen, können die FMH-HPC verwenden.

### 3 eCH-0064

Nach eCH-0064 Version 1.0 vom 04. Februar 2008 wird ein CVC wie folgt definiert:

T	T	Beschreibung	L	Referenz
7F21		CV Certificate	81 D5	ISO/IEC 7816-6
	5F37	Signature	81 80	ISO/IEC 7816-6/8
	5F38	Remainder	44	ISO/IEC 7816-6
	42	CAR	08	ISO/IEC 7816-6

Der Inhalt des CVC wird mit folgenden Datenobjekten gebildet:

#### CVC Data Objects

CPI	Certificate Profile Identifier - 2 byte	Art des Zertifikats (Benutzer   Herausgeber)
CAR	Certification Authority Reference	Identifiziert die Herausgeber-CA
CHR	Certificate Holder Reference	Identifiziert den Zertifikatsbesitzer
CHA	Certificate Holder Authorisation	Beschreibt die Rolle des Zertifikatsbesitzers
OID	Object ID - 5 byte	Definiert den Signaturalgorithmus
CISD <sup>2</sup>	Card Issuer's Data - 5 byte	Beschreibt die Gültigkeitsdauer des Zertifikats CXD    CED Certificate Expiration Date CXD 31/12/2015 Certificate Effective Date CED 12/2009 DO CISD (TLV) = ,45051512311209'

Die Bildung der CVCs nach eCH-0064 Version 1.0 vom 04. Februar 2008 erfolgt mit:

- Message Recovery nach ISO/IEC 9799-2 Digital Signature Scheme 1
- RSA Signature 1024 bit
- Secure Hash nach SHA-1

#### RSA-1024

PK_Modulus	128 byte	Modulus
PK_Exp	4 byte Wert: 00 01 00 01	Public Exponent, fix nach eCH-0064
PR_Exp	128 byte	Privat Exponent

#### Crypto Function Input

Hash Input	CPI    CAR    CHR    CHA    OID    CISD    PK_Modulus    PK_Exp	SHA-1
DSI	6A    CPI    CAR    CHR    CHA    OID    CISD    PK_Part1    Hash    BC	Digital Signature Input

<sup>2</sup> Das Objekt CISD ist in eCH-0064 nicht spezifiziert. Es ermöglicht, auf die geforderte Länge der Signatur von 128 byte zu kommen.

**Message Recovery nach ISO/IEC 9796-2, DS1 Option 1(t=1), RSA 1024 Bit, SHA-1**

Mr	CPI    CAR    CHR    CHA    OID    CSD    PK_Part1	recoverable Part
Mn	PK_Part2    PK_Exp	non-recoverable Part, Reminder
PK_Part1	[MSB ... LSB: 1 ... 64] - 64 byte	erster Teil des Modulus des zertifizierten Public Key
PK_Part2	[MSB ... LSB: 65 ... 128]    PK_Exp - 68 byte	zweiter Teil des Modulus des zertifizierten Public Key konkateniert mit Exponent

Format und Inhalt der Datenobjekte (DO) für das CVC sind in eCH-0064 Version 1.0 vom 04. Februar 2008 spezifiziert.

Die DOs CAR (Certification Authority Reference) und CHR (Certificate Holder Reference) enthalten spezifische Angaben über die Herausgeber CA und die Person des Leistungserbringers.

Für die von den Herausgebern der eVK respektive der HPC noch abzustimmenden Werte sind in den folgenden Beispielen die Vorschläge der FMH wiedergegeben:

- CAR für HPC Herausgeberzertifikat: ("CH NNN<sup>3</sup>" '6' '1' '01' '09<sup>4</sup>')
- CAR für HPC Personenzertifikat: ("CH HPC<sup>5</sup>" '1' '1' '01' '09')
- CHR für HPC Personenzertifikat: [LE-Kennziffer<sup>6</sup>] 00 00 [ICCSN<sup>7</sup>]

<sup>3</sup> „NNN“ ist der Name der Versicher-Herausgeber-CA.

<sup>4</sup> 09: Herausgeberjahr der CA.

<sup>5</sup> „HPC“ ist in diesem Beispiel der Name der FMH-HPC-CA

<sup>6</sup> Eindeutige Identifikation des Leistungserbringers.

<sup>7</sup> ICCSN: Integrated Chip Circuit Serial Number - Chipseriennummer

### 3.1 eCH-0064 – CVC Entwurf für FMH-HPC

Es folgt ein Beispiel für die Ausprägung.

<b>Beschreibung</b>	<b>L/[byte]</b>	<b>CVC.CA_ORG_HPC</b>	
Padding bits	1	6A	nach ISO 9796-2
CPI	1	03	
CAR	8	4E 4E 4E 43 61 01 09	## ("CH NNN" '6' '1' '01' '09')
CHR	16	00 00 00 00 00 00 00 00 43 48 50 44 43 61 01 09	
CHA	7	44 46 2E 4E 6F 74 00 ## ("DF.NOT" '00')	## ("DF.NOT" '00')
OID	5	2B 0E 03 02 0F	## (1.3.14.3.2.15)
CISD	5	15 12 31 12 09	## CXD 31/12/2015 CED 12/2009
PK_Part1	64	[64 byte]	
Hash	20	[20 byte]	
Trailer	1	BC	nach ISO 9796-2
<b>Σ</b>	<b>128</b>	<b>1..2..3..4..5..6..7..8..9..10.11.12.13.14.15.16</b>	
<b>Beschreibung</b>	<b>L/[byte]</b>	<b>CVC.HPC für LE (Leistungserbringer)</b>	
Padding bits	1	6A	nach ISO 9796-2
CPI	1	04	
CAR	8	43 48 48 50 43 11 01 09	## ("CH HPC" '1' '1' '01' '09')
CHR	16	L3 L2 L1 L0 00 00 S9 S8 S7 S6 S5 S4 S3 S2 S1 S0	[LE-Kennziffer: 4 byte] 00 00 [ICCSN - 10 byte]
CHA	7	44 46 2E 4E 6F 74 01 ## ("DF.NOT" '01')	## ("DF.NOT" '01')
OID	5	2B 0E 03 02 0F	
CISD	5	15 12 31 12 09	## CXD 31/12/2015 CED 12/2009
PK_Part1	64	[64 byte]	
Hash	20	[20 byte]	
Trailer	1	BC	nach ISO 9796-2
<b>Σ</b>	<b>128</b>	<b>1..2..3..4..5..6..7..8..9..10.11.12.13.14.15.16</b>	

### **Referenzen:**

[1] Zertifizierungsbericht „Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re\_Cert with Application for Digital Signature“ T-Systems.02192.TE.08.2007 (gebührenfrei).

Quelle: [http://www.t-systems-zert.de/einzelne/ein\\_02\\_sig\\_pro\\_e.html](http://www.t-systems-zert.de/einzelne/ein_02_sig_pro_e.html)

[2] Das Dokument eCH-0064 gilt als technischer Standard für die Versichertenkarte gemäss Art. 42a KVG und der Verordnung über die Versichertenkarte (gebührenfrei).

Quelle: <http://www.ech.ch>

[3] Die mehrteilige Normreihe ISO 7816 beschreibt die physischen und elektrischen Eigenschaften von Chipkarten.

Quelle: <http://www.iso.org>

[5] Die Technischen Spezifikationen für Siemens CardOS 4.3B von Siemens sind im Rahmen eines Software Developer Kits erhältlich. Bestellung via Siemens

[6] Der PC/SC-Standard wird von der PC/SC-Workgroup definiert.

Quelle: <http://www.pcscworkgroup.com>

### **Rechtliche Information**

Die FMH behält sich ausdrücklich vor, jederzeit die technischen Spezifikationen zu ändern. Sie schliesst die Haftung aus für Schäden materieller oder immaterieller Art, die aus der Änderung der technischen Spezifikation oder der Nutzung bzw. Nichtnutzung der veröffentlichten Informationen entstanden sind.

© Copyright FMH 2009