

CPS FMH: description technique

Version 1.0, 01.09.2009

Sommaire

Sommaire	1
1. Aperçu	1
2. Détails techniques.....	2
2.1. Siemens CardOS V4.3B.....	2
2.2. Carte à puce SLE66CX322P.....	3
2.3. Carte middleware	3
2.4. Système requis	4
2.5. Lecteur de carte.....	4
2.6. Interopérabilité.....	4
3. eCH-0064.....	5
3.1. eCH-0064 – projet de CVC pour la CPS FMH.....	7
Références:	8

1. Aperçu

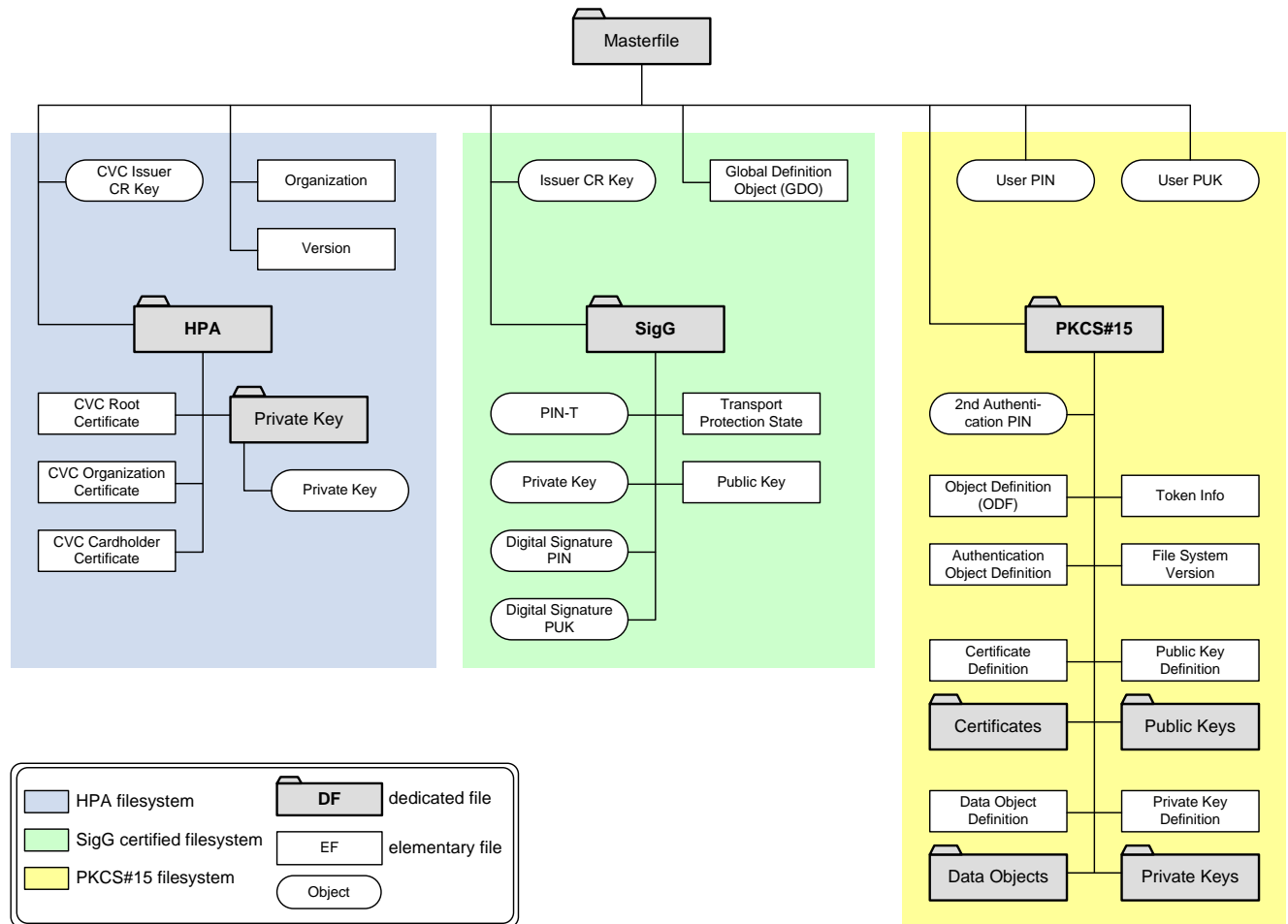
La carte professionnelle de santé de la FMH (CPS FMH) est une carte à puce répondant à la norme ISO 7816. Elle est dotée d'une puce Infineon SLE66CX322P avec 32 Ko d'EEPROM et du système d'exploitation pour carte à puce de Siemens HiPath Security CardOS V4.3B «Re_Cert with Application for Digital Signature».

Cette carte à puce satisfait aux exigences d'un dispositif sécurisé de création de signature électronique, SSEE (Secure Signature Creation Device - SSCD) au «sens de la loi fédérale sur la signature électronique SCSE» (RS 943.03).

1.1 Schema de mise en page de la CPS FMH

Sur la CPS FMH, les trois environnements suivants sont initialisés:

- a) environnement standard PKCS#15 pour certificats X.509 selon la norme ISO 7816-15 compatible avec les interfaces PKCS#11.
- b) environnement SigG pour une signature électronique qualifiée au sens de la SCSE¹.
- c) environnement HPA (Health Professional Application) compatible avec la carte d'assuré électronique selon la norme eCH-0064 V1.0 du 4 février 2008 (carte d'assuré).



2. Détails techniques

2.1. Siemens CardOS V4.3B

HiPath Scurity CardOS V4.3B est une carte à puce multifonctionnelle de système d'exploitation. Elle offre une protection active et passive aux données sauvegardées, certificats et clés cryptographiques.

Caractéristiques de la CardOS V4.3 B

Système d'exploitation:	CardOS V4.3 B
Hashes/MACs	SHA-1, MAC, Retail-MAC
Procédure asymétrique	RSA jusqu'à 2048 bit (PKCS#1) sur la base du CRT

¹ „Loi fédérale sur la signature électronique (SCSE)“ (RS 943.03).

Procédure symétrique	Triple DES (ECB, CBC), DES (ECB, CBC),
Communication:	T=1
Normes	ISO 7816-4,8,9
Certification	CC EAL 4+ en vigueur
Protection	Contre «Differential Fault Analysis», «Simple Power Analysis» (SPA) et «Differential Power Analysis» (DPA)

2.2. Carte à puce SLE66CX322P

Sécurité	16 Bit Security Controller avec Memory Management et Protection Unit, 0,22 µm CMOS
Espace mémoire	136 Ko de ROM, 4Ko de XRAM, 256 octets de RAM interne, 700 octets de Crypto RAM., 32 Ko d'EEPROM
Cryptographie	Advanced Crypto Engine de 1100 bits, DDES-EC2 Accelerator de 112 bits /192 bits
Normes	ISO/IEC 7816 EMV 2000 GSM 11.11, 11.12,
Consommation et tension	< 10 mA @ 5.5 V < 6 mA @ 3.3 V < 4 mA @ 1.98 V

2.3. Carte middleware

Pour l'utilisation de la CPS FMH, un middleware (Card API) avec les interfaces standard suivantes est disponible:

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

2.4. Système requis

Afin de pouvoir utiliser un middleware, une interface PC/SC (carte à puce) doit être activée. Actuellement, les plates-formes suivantes sont prises en charge:

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

2.5 Lecteur de carte

La CPS FMH est conçue pour une utilisation avec des lecteurs de cartes standard. Tous les lecteurs de cartes à puce compatible à une interface PC/SC avec un extended APDU sont pris en charge. Les lecteurs Pinpad doivent prendre en charge l'interface PC/SC V2.01 10.

2.6. Interopérabilité

Les applications qui conformément au point 2.3 ont accès au middleware peuvent utiliser les CPS FMH

3. eCH-0064

D'après la norme eCH-0064 Version 1.0 du 4 février 2008, un CVC est défini de la manière suivante:

T	T	Description	L	Référence
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

Le contenu du CVC est constitué des objets de données suivants:

CVC Data Objects

CPI	Certificate Profile Identifier - 2 byte	type du certificat (utilisateur éditeur)
CAR	Certification Authority Reference	identifie l'autorité de certification de l'éditeur
CHR	Certificate Holder Reference	identifie le titulaire du certificat
CHA	Certificate Holder Authorisation	décrit le rôle du titulaire du certificat
OID	Object ID - 5 byte	définit l'algorithme de signature
CISD ²	Card Issuer's Data - 5 byte	décrit la durée de validité du certificat CXD CED Certificate Expiration Date CXD 31/12/2015 Certificate Effective Date CED 12/2009 DO CISD (TLV) = ,45051512311209'

La composition du CVC d'après eCH-0064 Version 1.0 du 4 février 2008 est réalisée avec:

- Message Recovery selon ISO/IEC 9769-2 Digital Signature Scheme 1
- RSA Signature 1024 bit
- Secure Hash nach SHA-1

RSA-1024

PK_Modulus	128 octets	Module
PK_Exp	Valeur de 4 octets: 00 01 00 01	Public Exponent, fixe selon eCH-0064
PR_Exp	128 octets	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

² L'objet CISD n'est pas spécifié par eCH-0064. Cela permet d'arriver à la longueur de 128 octets exigée pour la signature.

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

Mr	CPI CAR CHR CHA OID CISD PK_Part1	recoverable part
Mn	PK_Part2 PK_Exp	non-recoverable part, reminder
PK_Part1	[MSB ... LSB: 1 ... 64] - 64 byte	première partie du module de la clé publique certifiée
PK_Part2	[MSB ... LSB: 65 ... 128] PK_Exp - 68 byte	seconde partie du module de la clé publique certifiée en concaténation avec exposant

Le format et le contenu des objets de données (OD) pour le CVC sont spécifiés dans eCH-0064 Version 1.0 du 4 février 2008.

Les OD CAR (Certification Authority Reference) et CHR (Certificate Holder Reference) contiennent des données spécifiques de l'éditeur de l'autorité de certification et de la personne du prestataire de service.

Pour les valeurs encore à harmoniser avec l'éditeur de la carte de patient électronique et respectivement de la CPS, les exemples suivants illustrent les propositions faites par la FMH:

- CAR du certificat de l'éditeur de la CPS: ("CH NNN³" '6' '1' '01' '09⁴')
- CAR du certificat personnel de la CPS: ("CH HPC⁵" '1' '1' '01' '09')
- CHR du certificat personnel de la CPS: [indice prest. serv.⁶] 00 00 [ICCSN⁷]

³ „NNN“ est le nom de l'assureur éditeur de l'autorité de certification (CA).

⁴ 09: année d'édition de la CA.

⁵ „HPC“ est dans cet exemple le nom de la CA de la CPS FMH

⁶ Identification univoque du prestataire de service.

⁷ ICCSN: Integrated Chip Circuit Serial Number – numéro de série de la carte à puce



Verbindung der Schweizer Ärztinnen und Ärzte
 Fédération des médecins suisses
 Federazione dei medici svizzeri
 Swiss Medical Association

3.1. eCH-0064 – projet de CVC pour la CPS FMH

Voici un exemple à titre explicatif.

Description	L/[octet]	CVC.CA_ORG_HPC	
Padding bits	1	6A	Selon 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 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	selon ISO 9796-2
Σ	128	1..2..3..4..5..6..7..8..9..10.11.12.13.14.15.16	
Description	L/[octet]	CVC.HPC pour le prestataire de service	
Padding bits	1	6A	selon 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	[indice prest. serv.: 4 octets] 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	Selon ISO 9796-2

Elfenstrasse 18, Postfach 170, CH-3000 Bern 15
 Telefon +41 31 359 11 11, Fax +41 31 359 11 12
 info@fmh.ch, www.fmh.ch

Σ 128 1..2..3..4..5..6..7..8..9..10.11.12.13.14.15.16

Références:

[1] Rapport de certification «Carte à puce avec processeur SLE66CX322P (ou SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature»

T-Systems.02192.TE.08.2007 (gratuit).

Source: http://www.t-systems-zert.de/einzelne/ein_02_sig_pro_e.html

[2] Le document eCH-0064 fait foi de standard technique pour la carte d'assuré en vertu de l'art. 42a LAMal et de l'ordonnance sur la carte d'assuré (gratuit).

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

[3] ISO 7816 est une famille de normes qui décrit les caractéristiques physiques et électriques des cartes à puce.

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

[5] Les spécifications techniques pour la carte Siemens CardOS 4.3B de Siemens sont disponibles avec un kit de développement logiciel. A commander auprès de Siemens.

[6] La norme de l'interface PC/SC est définie par le Workgroup PC/SC.

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

[7] Safari utilise une authentification basée sur des certificats uniquement si le serveur web le requiert explicitement. Dans le cas contraire, l'authentification basée sur des certificats doit être provoquée au niveau local.

Source: <http://support.apple.com/kb/HT1679>

Informations juridiques

La FMH se réserve expressément le droit de modifier à tout moment les spécifications techniques. Elle ne saurait être tenue responsable des dommages matériels ou immatériels qui pourraient être causés par toute modification de la spécification technique ou par l'utilisation ou la non-utilisation des informations publiées.

© Copyright FMH 2009