

eCH-0064 – Spécifications du système de la carte d'assuré

Titre	Spécifications du système de la carte d'assuré
Code	eCH-0064
Type	Norme de procédure
Stade	Définie
Version	1.0
Statut	Approuvée
Validation	2008-02-04
Date de publication	2008-02-04
Remplace	
Langues	Allemand, français La version allemande fait foi.
Mandant	Office fédéral de la santé publique (OFSP)
Auteurs	Groupe spécialisé Carte d'assuré eCH Adrian Schmid, OFSP, adrian.schmid@bag.admin.ch Jürg Burri, OFSP, juerg.burri@bag.admin.ch Willy Müller, USIC, willy.mueller@isb.admin.ch Peter Stadlin, Arpage SA, stadlin@arpage.ch Martin Stingelin, Stingelin Informatik Sàrl, info@stingelin-informatik.com
Edition / Distributeur	Association eCH, Mainaustrasse 30, Postfach, 8034 Zurich Tél. 044 388 74 64, télécopie 044 388 71 80 www.ech.ch / info@ech.ch

Résumé

Le présent document a valeur de norme technique pour la carte d'assuré au sens de l'art. 42a LAMal et de l'ordonnance sur la carte d'assuré. Il contient des exigences de base techniques pour le système de la carte d'assuré, compte tenu des normes valables au plan international.

Table des matières

1	Statut du document.....	6
2	Introduction	7
2.1	Aperçu	7
2.2	Champ d'application	7
2.3	Protection et sécurité des données.....	8
2.4	Délimitation.....	10
2.5	Schéma de composants	10
2.6	Notation	12
3	Spécifications du système de la carte d'assuré défini aux art. 2 et 6 [OCA]	13
3.1	Exigences générales	13
3.1.1	Spécifications techniques	13
3.1.2	Exigences physiques.....	13
3.1.3	Exigences en matière de communication	13
3.1.4	Attestation électronique du fournisseur de prestations	14
3.2	Carte à puce et système d'exploitation	14
3.2.1	Série de commandes	14
3.2.2	Opérations de codage	15
3.2.3	Mémoire EEPROM.....	15
3.2.4	Initialisation et personnalisation de la carte à puce.....	16
3.3	Authentification	17
3.3.1	Certificats vérifiables à partir de la carte [CVC]	17
3.3.2	Authentification.....	17
3.4	Système de fichiers	18
3.4.1	Gestion des fichiers selon la norme ISO/IEC 7816-4.....	18
3.4.2	Structure des fichiers de la carte d'assuré.....	18
3.5	Gestion du PIN	29
3.5.1	Série de commandes	29
3.5.2	Activation du PIN / Désactivation et saisie.....	29
3.5.3	Etats de protection du PIN.....	30
3.5.3.1	Carte d'assuré après remise par l'assureur.....	30
3.5.3.2	Activation du dispositif PIN.....	30

3.5.3.3	Modification du blocage par PIN pour des catégories de données d'urgence	30
3.5.3.4	Modification du code PIN (dispositif PIN activé)	30
3.5.3.5	Désactivation du dispositif PIN	30
3.5.3.6	Dispositifs de blocage du code PIN	31
3.6	Authentification carte à carte et autorisation	31
3.6.1	Principe	31
3.6.2	Clés et certificats dans des entités	32
3.6.3	Termes et abréviations	35
3.6.4	Procédure	36
3.6.4.1	Authentification et autorisation carte à carte hors ligne	36
3.6.4.2	Vérification de certificat en ligne / hors ligne (facultative)	39
3.6.4.3	PKI hors ligne des organisations émettrices pour l'établissement de CVC	40
4	Procédure de consultation en ligne au sens de l'art. 15 [OCA]	42
4.1	Principe	42
4.2	Exigences en matière de communication	42
4.3	Accès direct en ligne au moyen de HTTP via SSL/TLS	42
4.3.1	Navigateur Internet sur l'ordinateur du fournisseur de prestations	42
4.3.2	Contrôle d'accès	43
4.4	Accès en ligne direct au moyen de SOAP/HTTP via SSL/TLS	43
4.4.1	Procédure de consultation en ligne depuis des applications chez le fournisseur de prestations	43
4.4.1.1	Protocoles d'accès	43
4.4.1.2	Contrôle de l'accès	43
4.4.2	Procédure de consultation directe en ligne passant par le serveur pour des services chez les fournisseurs de prestations ou des tiers qu'ils ont mandatés	44
4.4.2.1	Protocole d'accès	44
4.4.2.2	Contrôle de l'accès	44
4.4.2.3	Connexion client - serveur	45
4.4.2.4	Service de certification des assureurs pour les certificats selon X.509 (RFC 3280)	45
4.5	Accès authentifié par l'intermédiaire d'un fournisseur de services réseau (service d'authentification)	45
4.5.1	Gestion de l'identité et des accès	45

4.5.2	Procédure d'accès.....	46
5	Essais pilotes cantonaux au sens de l'art. 16 [OCA].....	48
6	Définition des certificats.....	49
6.1	Spécification des CVC selon ISO/IEC 7816-8 avec recouvrement des messages selon ISO/IEC 9796-2	49
6.1.1	CVC ['7F21']	50
6.1.2	Signature ['5F37']	50
6.1.3	CPI - Identificateur de profil du certificat ['5F29']	50
6.1.4	CAR - Référence de l'autorité de certification (Authority Key Identifier)	51
6.1.5	CHR - Référence du détenteur du certificat (Subject Key Identifier)	52
6.1.6	CHA - Autorisation du détenteur du certificat.....	53
6.1.7	Codage OID	53
6.2	Certificats de serveur conformes à X.509 (RFC 3280) pour le service en ligne	54
6.2.1	Définition des certificats.....	54
6.2.2	DESCRIPTION (2.3.4.13) : carpukcvc.....	55
6.3	Certificats d'émetteur conformes à X.509 (RFC 3280) [X509.CA_Pub _x]	55
7	Exclusion de responsabilité – Droits de tiers	56
8	Droits d'auteur.....	57
	Annexe A – Glossaire et abréviations.....	58
	Annexe B – Références et bibliographie	59
	Annexe C – Collaboration et rédaction.....	61

1 Statut du document

Le présent document est la version définitive que le Comité d'experts a approuvée le 4 février 2008.

2 Introduction

2.1 Aperçu

Le Parlement a créé la base légale pour l'introduction d'une carte d'assuré maladie le 8 octobre 2004. C'est l'**art. 42a** de la **loi fédérale sur l'assurance-maladie (LAMal)**. En vigueur depuis le 1^{er} janvier 2005, il a la teneur suivante :

¹ *Le Conseil fédéral peut décider qu'une carte d'assuré portant un numéro d'identification attribué par la Confédération soit remise à chaque assuré pour la durée de son assujettissement à l'assurance obligatoire des soins. La carte contient le nom de l'assuré et un numéro d'assurance sociale attribué par la Confédération.*

² *Cette carte comporte une interface utilisateur ; elle est utilisée pour la facturation des prestations selon la présente loi.*

³ *Le Conseil fédéral règle, après consultation des milieux intéressés, les modalités d'introduction de la carte par les assureurs, ainsi que les standards techniques qui doivent être appliqués.*

⁴ *Moyennant le consentement de l'assuré, la carte contient des données personnelles auxquelles peuvent avoir accès les personnes qui y sont autorisées. Le Conseil fédéral définit, après avoir consulté les milieux intéressés, l'étendue des données pouvant être enregistrées sur la carte. Il règle l'accès aux données et leur gestion.*

Les dispositions d'exécution de la loi se trouvent dans l'ordonnance sur la carte d'assuré pour l'assurance obligatoire des soins [OCA]. Celle-ci prévoit notamment, à son art. 17, que les normes internationales doivent être prises en compte lors de la fixation des standards techniques et que ces derniers, prévus par l'art. 42a, al. 3, LAMal, sont réglés dans une ordonnance du DFI [ODFI]. Cette ordonnance départementale exige en particulier que la norme ici concrétisée soit utilisée pour mettre en œuvre le système de la carte d'assuré.

La présente norme définit un minimum de normes technologiques en vue de permettre au plus grand nombre possible de fournisseurs du marché de les respecter.

2.2 Champ d'application

La norme définit les exigences techniques auxquelles la carte doit satisfaire en vertu de l'art. 2 [OCA], ainsi que la mise en œuvre des exigences de sécurité fixées à l'art. 7 [OCA] pour les données figurant sur la carte et à l'art. 15 [OCA] pour les services d'information en ligne que les assureurs devront offrir.

La présente norme n'est pas destinée à la mise en place du projet, mais à sa conception, sa structure et sa procédure. D'autres spécifications détaillées sont donc nécessaires pour le système de la carte d'assuré. La norme est conçue en premier lieu pour les spécialistes auxquels sera confiée la mise en œuvre technique des services de la carte ainsi que de la procédure de consultation en ligne.

2.3 Protection et sécurité des données

L'utilisation de la carte d'assuré implique le traitement de données personnelles, parmi lesquelles les informations médicales sont particulièrement dignes d'être protégées au sens de la loi sur la protection des données (LPD). Tous les services qui travaillent avec ces données doivent se conformer aux principes de la LPD (légalité, proportionnalité, transparence, affectation au but fixé). Dans le système de la carte d'assuré, le droit fondamental de tout individu à l'autodétermination en matière d'information doit être garanti. De plus, des mesures techniques et organisationnelles appropriées doivent protéger les données contre toute utilisation non autorisée. Lors de l'application judicieuse des prescriptions légales ([OCA], [ODFI], [LPD], [OLPD]), la protection et la sécurité des données sont garanties par

- l'obligation d'informer les assurés des données qui figurent sur leur carte, de leur droit à être renseignés et à faire rectifier les données, qui permet de clarifier la différence entre les fonctions obligatoires de la carte et celles qui sont facultatives ;
- l'identification sûre des personnes ayant le droit d'accès ;
- l'accès sélectif aux données par des droits d'accès et de traitement échelonnés et l'autorisation de l'assuré pour les fonctions facultatives;
- la transmission des données suffisamment sûre en ce qui concerne l'interrogation en ligne.

La présente norme réglemente les mesures d'ordre technique. L'exploitant des données est responsable des mesures organisationnelles.

Protection et sécurité des données	Mesures pour les données administratives au sens des art. 3 et 4 OCA		Mesures pour les données personnelles au sens de l'art. 6 OCA (fonction facultative de la carte)	
	Dans la norme	Hors norme	Dans la norme	Hors norme
Autodétermination de l'assuré	- Pas de mesure technique (l'utilisation de la carte est une obligation pour l'assuré LAMal qui veut se faire rembourser une prestation par l'assurance-maladie)	- Accord de l'assuré pour la consultation en ligne (art. 15, al. 3, OCA) - Droit à l'information et possibilité de faire traiter les données conformément à l'art. 9 OCA - Exposé des droits et des obligations selon les art. 12 et 13 OCA	- Possibilité pour les assurés de protéger à l'aide d'un code PIN toutes les catégories de données médicales (chap. 3.5)	- Accord de l'assuré pour la saisie et le traitement des données (art. 7, al. 3, OCA) - Droit à l'information et possibilité de faire traiter les données selon l'art. 9 OCA - Exposé des droits et des obligations selon les art. 12 et 13 OCA

Protection et sécurité des données	Mesures pour les données administratives au sens des art. 3 et 4 OCA		Mesures pour les données personnelles au sens de l'art. 6 OCA (fonction facultative de la carte)	
Définition claire des droits d'accès	<ul style="list-style-type: none"> - Report sécurisé des données et contrôle d'accès pour la consultation en ligne par les assureurs au moins par le biais de l'ID et du mot de passe (chap. 4); 	<ul style="list-style-type: none"> - Droits d'accès généralement pour les fournisseurs de prestations procédant à la consultation en ligne selon l'art. 5 OCA - Contrôle des droits d'accès dans le cas particulier par l'assuré 	<ul style="list-style-type: none"> - Authentification carte à carte entre carte d'assuré (CA) et attestation de fournisseur de prestations (art. 6 OCA) - Sous (art. 6 OCA) fichiers avec accès réglementé aux fichiers contenant des données médicales (ch. 3.4.2); 	<ul style="list-style-type: none"> - Définition des droits d'accès généraux selon l'art. 7 OCA - Droits d'accès dans le cas particulier uniquement avec l'accord de l'assuré (par transmission de la carte, déverrouillage du code PIN) - Authentification du fournisseur de prestations par l'attestation électronique justifiant de sa qualité selon l'art. 8 OCA
Sécurité lors du traitement de données	<ul style="list-style-type: none"> - Processus d'accès définis pour la consultation en ligne (ch. 4.3 à 4.5). - Exigences en matière de communication pour la consultation en ligne (ch. 4.2); 	<ul style="list-style-type: none"> - Loi et ordonnance sur la protection des données 	<ul style="list-style-type: none"> - Traitement local des données 	<ul style="list-style-type: none"> - Loi et ordonnance sur la protection des données

2.4 Délimitation

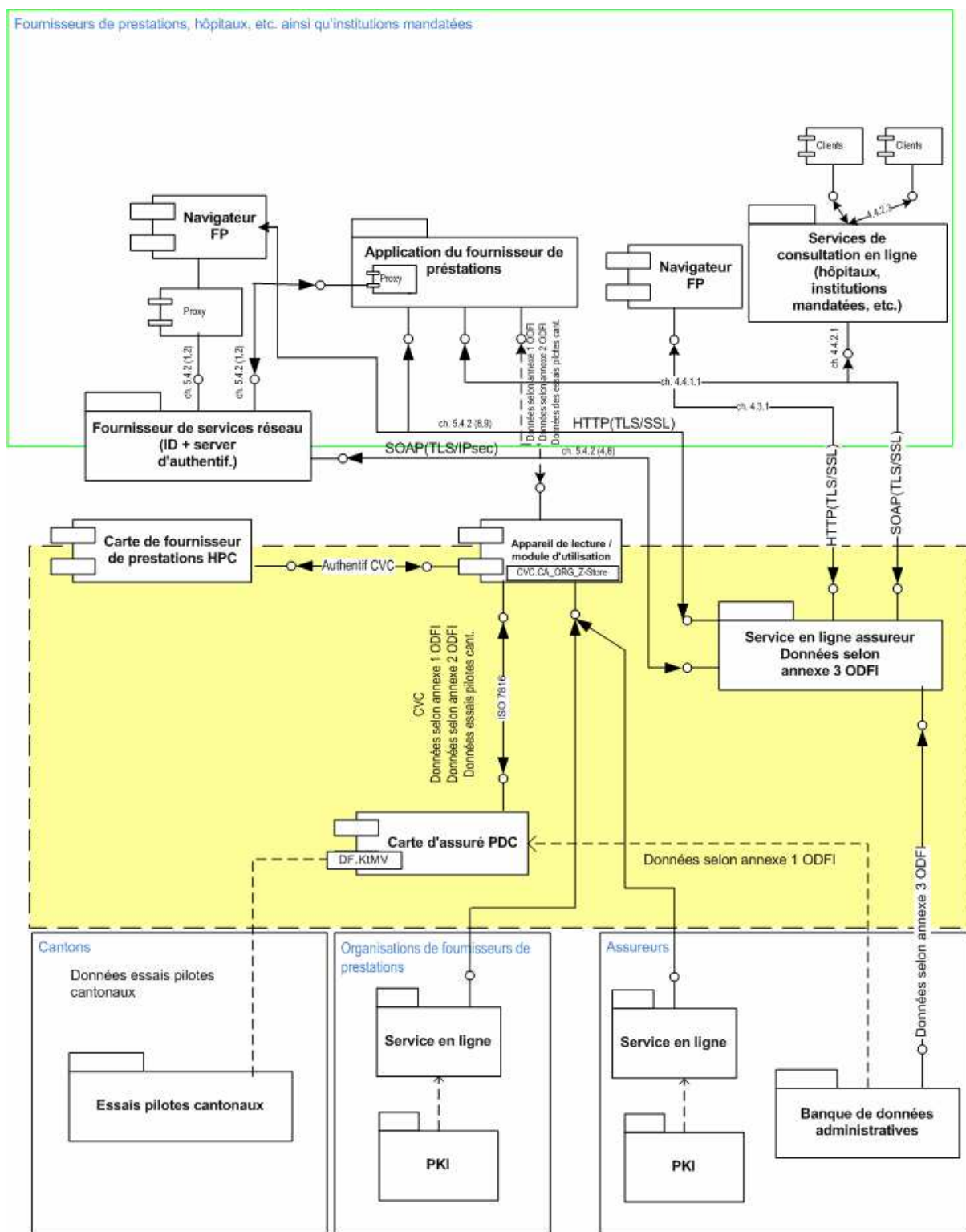
Les éléments déjà décrits dans d'autres normes ne sont cités ici que sous forme de référence. Les dérogations aux normes référencées sont explicitement signalées comme telles dans la présente norme.

Les éléments suivants ne sont pas compris dans la présente norme et doivent être réglés séparément :

- aspects organisationnels en lien avec l'établissement et l'utilisation de la carte d'assuré ;
- aspects organisationnels en lien avec la procédure de consultation en ligne.

2.5 Schéma de composants

Le schéma ci-après indique les composants du système de la carte d'assuré et les connexions les plus importantes entre eux. La zone marquée en jaune contient les composants qui sont définis par la présente norme. Pour certains composants, tels que la carte électronique de fournisseur de prestations (*Health professional Card*, HPC) et l'appareil de lecture / module d'utilisation, la norme contient des spécifications partielles, nécessaires pour le système de la carte d'assuré. La norme ne régleme spécifiquement qu'une partie des composant en-dehors de la zone marquée en jaune. Les jeux de données pour les données administratives et médicales sont définis dans l'ODFI.



2.6 Notation

Les directives du présent document sont données suivant la terminologie de [RFC2119], au moyen des expressions ci-dessous, écrites en CAPITALES, qui ont la signification suivante :

- EXIGÉ :** Le responsable est tenu d'appliquer strictement la directive.
- RECOMMANDÉ :** Le responsable peut, pour des motifs importants, décider de ne pas appliquer la directive.
- FACULTATIF :** Le responsable est libre d'appliquer la directive ou non.

3 Spécifications du système de la carte d'assuré défini aux art. 2 et 6 [OCA]

3.1 Exigences générales

3.1.1 Spécifications techniques

Motivation : Les exigences prennent en compte les normes internationales comme le veut l'art. 17 [OCA] et sont remplies par le plus grand nombre de fournisseurs de cartes possible.

EXIGÉ : Les spécifications techniques de la carte d'assuré suivent la norme ISO/IEC 7816. Les termes techniques utilisés dans le présent chapitre sont définis dans ladite norme.

3.1.2 Exigences physiques

Motivation : Les exigences sont remplies par le plus grand nombre de fournisseurs de cartes possible.

EXIGÉ : La carte d'assuré doit satisfaire aux exigences des normes suivantes :

- ISO/IEC 7816-1 (Cartes à circuit(s) intégré(s) à contacts – Caractéristiques physiques)
- ISO/IEC 7816-2 (Dimensions et emplacement des contacts)

3.1.3 Exigences en matière de communication

Motivation : Les exigences minimales qui suivent, basées sur la norme ISO/IEC 7816, sont conçues de manière à pouvoir être remplies par le plus grand nombre de fournisseurs de cartes possible.

EXIGÉ : La procédure de transmission entre la carte d'assuré et l'appareil de lecture / module d'utilisation est implémentée conformément à la norme ISO/IEC 7816-3 et comprend les fonctions suivantes :

- **EXIGÉ** : protocole de transmission T = 1, la faculté d'enchaînement (chaining) étant également exigée.
- **EXIGÉ** : lorsqu'un bloc de transmission est envoyé à la carte, l'octet NAD doit avoir la valeur '00' ; autrement dit, pas d'adresse nœud.
- **RECOMMANDÉ** : ne pas utiliser la commande de suspension ABORT [PCB], qui peut cependant être déclenchée facultativement par la carte pour interrompre une chaîne trop longue si la taille de la mémoire tampon I/O n'est pas respectée.
- **EXIGÉ** : taille des champs d'information : IFSC = 128 octets (au moins), IFSD = 254 octets.
- **EXIGÉ** : sélection des paramètres de protocole (PPS) au moyen du mode négociable, sinon diviseur (CRFC) réglé sur 372 ou 512, afin de garantir une vitesse de transfert d'au moins 38 kbps.
- **EXIGÉ** : codage ATR conforme à la norme ISO/IEC 7816-3.

3.1.4 Attestation électronique du fournisseur de prestations

Motivation : L'attestation électronique du fournisseur de prestations doit être un jeton universel comprenant des fonctions, des commandes et des interfaces physiques conformes aux règles internationales, afin de permettre une intégration simple et optimale de nombreuses applications utilisées par les fournisseurs de prestations, notamment en rapport avec la carte d'assuré et pour l'utilisation de cette dernière.

EXIGÉ : L'attestation électronique du fournisseur de prestations répond en tant que carte à puce HPC aux spécifications des normes ISO/IEC 7816-1, 2, 3, 4, 5, 6, 8 et 9 et doit être donnée au format ID-1 conformément à la norme ISO 7810. Elle peut au besoin être transférée par le fournisseur de prestations par transposition du format ID-1 au format ID-000. Toutes les fonctions et les structures de données sont définies publiquement.

3.2 Carte à puce et système d'exploitation

3.2.1 Série de commandes

Motivation : La série de commandes minimale ci-dessous, conforme aux normes ISO/IEC 7816, permet la mise en œuvre des fonctionnalités exigées au ch. 3.6 et elle concerne le plus grand nombre possible de fournisseurs et de systèmes d'exploitation de cartes.

EXIGÉ : Le système d'exploitation de la carte d'assuré doit comprendre au moins le jeu de commandes ci-dessous conformément à la norme ISO/IEC 7816-4. Le nombre de commandes du jeu peut être réduit si, lors de la substitution d'une commande de base par l'utilisation spécifique des commandes contenues dans cette liste, la fonctionnalité requise, la performance et l'interopérabilité de la carte d'assuré ne sont pas restreintes.

- APPEND RECORD
- CHANGE REFERENCE DATA
- DISABLE VERIFICATION REQUIREMENT
- ENABLE VERIFICATION REQUIREMENT
- ENVELOPE
- ERASE BINARY
- ERASE RECORD (S)
- EXTERNAL AUTHENTICATE
- GET CHALLENGE
- GET DATA
- GET RESPONSE
- INTERNAL AUTHENTICATE
- MANAGE CHANNEL
- MANAGE SECURITY ENVIRONMENT
- PUT DATA
- READ BINARY
- READ RECORD (S)
- RESET RETRY COUNTER
- SEARCH BINARY
- SEARCH RECORD
- SELECT
- UPDATE BINARY

- UPDATE RECORD
- VERIFY
- WRITE BINARY
- WRITE RECORD

3.2.2 Opérations de codage

Motivation : La série de commandes minimale ci-dessous, basée sur les normes ISO/IEC 7816, permet de remplir les exigences relatives aux opérations de codage effectuées sur des cartes à puce peu coûteuses.

EXIGÉ : Pour les opérations de codage, le système d'exploitation de la carte à puce (carte d'assuré) doit comprendre au moins la série de commandes ci-dessous, conformément à la norme ISO/IEC 7816-8 :

GENERATE ASYMMETRIC KEY PAIR

- '7F49' INTERINDUSTRY TEMPLATE
 - '06' identificateur d'objet de l'algorithme
 - '80' référence algorithmique utilisée dans les objets de données de référence de commande pour un échange sécurisé de messages (év. pour des essais pilotes cantonaux)
 - série d'objets de données-clés publique pour RSA
 - '81' module
 - '82' exposant public

PERFORM SECURITY OPERATION

- traitement d'une signature numérique ;
- calcul d'un adressage dispersé ;
- vérification d'une signature numérique ;
- vérification d'un certificat ;
- chiffrement ;
- déchiffrement.

3.2.3 Mémoire EEPROM

Motivation : Cette exigence est nécessaire pour l'enregistrement des données définies dans l'[ODFI] et elle est remplie par les cartes standard à court délai de livraison.

EXIGÉ : La zone de mémoire EEPROM de la carte à puce doit disposer d'au moins 32 Ko.

Remarque : Les annexes 1 à 3 de l'[ODFI] spécifient le catalogue pour les données médicales, administratives et personnelles disposant de 2 à 70 Ko. Les données effectivement enregistrées sur la carte d'assuré n'en comprennent que la partie jugée pertinente et souhaitable par la personne assurée.

3.2.4 Initialisation et personnalisation de la carte à puce

Motivation : La série de commandes ci-dessous est nécessaire pour la spécification touchant la personnalisation et l'initialisation de la carte.

EXIGÉ : La carte à puce comprend au moins la série de commandes ci-dessous, conforme à la norme ISO/IEC 7816-9 :

- CREATE FILE
- DELETE FILE
- DEACTIVATE FILE
- ACTIVATE FILE
- TERMINATE DF
- TERMINATE EF
- TERMINATE CARD USAGE

EXIGÉ : Les états et les changements d'état d'un cycle de vie complet des fichiers sont réglés conformément à la norme ISO/IEC 7816-9.

EXIGÉ : L'initialisation et la personnalisation doivent être effectuées de telle sorte qu'après la clôture de ces processus et l'activation finale de la carte d'assuré, l'éditeur de la carte n'ait plus la possibilité d'intervenir sur les fichiers des données d'urgence sans une attestation de fournisseur de prestations autorisé.

3.3 Authentification

3.3.1 Certificats vérifiables à partir de la carte [CVC]

Motivation : Les cartes conformes aux normes ISO/IEC 7816 ont besoin de CVC pour que l'authentification carte à carte (C2C) soit sûre.

EXIGÉ : Des certificats vérifiables à partir de la carte tels que définis ci-dessous sont utilisés pour l'authentification et l'autorisation.

Exigences interindustrie pour les CVC		
Balise	Élément de donnée	Défini dans
'7F21'	CVC	ISO/IEC 7816-6
'5F4E'	Contenu du certificat	ISO/IEC 7816-8
'5F29'	Descripteur du profil d'échange, p. ex. identificateur de profil du certificat (CPI)	ISO/IEC 7816-6
'42'	Autorité de certification de référence (CAR), attribut de référence du service de certification (SC) qui délivre le certificat (analogue à l'identificateur de clé d'autorité (AKI), RFC 3280)	ISO/IEC 7816-6/8
'5F20'	Référence du détenteur du certificat (CHR), p. ex. nom du titulaire de la carte ou numéro de série ICCSN	ISO/IEC 7816-6/8
'5F49'	Clé publique du détenteur du certificat (objet de donnée simple)	ISO/IEC 7816-6/8
'7F49'	Clé publique du détenteur du certificat (objet de donnée calculé, de préférence)	ISO/IEC 7816-8
'06'	Identificateur d'objet (OID) pour l'algorithme de signature ou le détenteur du certificat	ISO/IEC 7816-6
'5F4A'	Clé publique du SC ou sa référence	ISO/IEC 7816-6
'5F4C'	Autorisation du détenteur du certificat (CHA), où les rôles d'accès sont définis	ISO/IEC 7816-8/9
'5F37'	Signature du certificat, signature du SC qui délivre le certificat	ISO/IEC 7816-6/8
'5F38'	Reste de la clé publique (reste du module, suivi d'un exposant)	ISO/IEC 7816-6

3.3.2 Authentification

Motivation : Le RSA représente la procédure asymétrique la plus courante.

EXIGÉ : L'authentification repose sur une procédure asymétrique selon la norme ISO/IEC 9798-3, qui prévoit l'utilisation de clés publiques et de clés privées.

EXIGÉ : L'algorithme utilisé est RSA, la longueur de la clé devant être d'au moins 1024 bits.

EXIGÉ : SHA 1 doit être utilisé comme fonction de hachage avec une valeur de 160 bits.

3.4 Système de fichiers

3.4.1 Gestion des fichiers selon la norme ISO/IEC 7816-4

Motivation : Les exigences minimales qui suivent, basées sur les normes ISO/IEC 7816, sont conçues de manière à pouvoir être remplies par le plus grand nombre de fournisseurs de cartes possible.

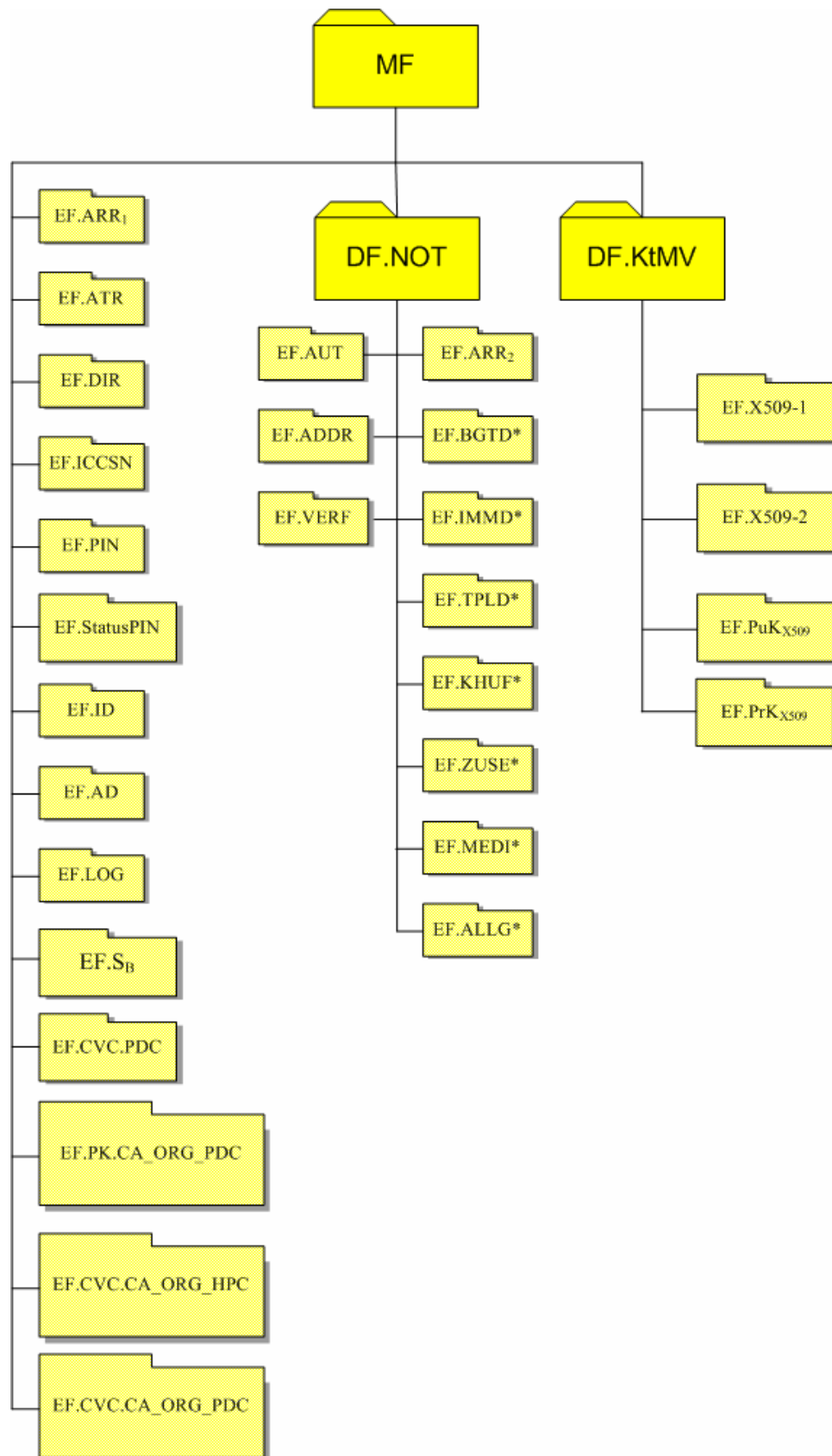
EXIGÉ : La gestion des fichiers doit satisfaire à la norme ISO/IEC 7816-4 et comprendre les fonctionnalités suivantes :

- Niveau d'imbrication : au moins aux niveaux fichier maître (MF) et fichier dédié (DF)
- Fichiers élémentaires (EF) avec structures transparentes
- EF avec structure linéaire et enregistrements de longueur fixe
- EF avec structure linéaire et enregistrements de longueur variable
- EF avec structure cyclique
- Enregistrements d'une longueur maximale de 511 octets
- Nombre d'enregistrements dans un fichier : 254 au maximum
- EF avec un identificateur court (utilisable uniquement dans le DF et l'application correspondants)
- DF avec identificateur d'application

3.4.2 Structure des fichiers de la carte d'assuré

Motivation : Les exigences ci-après, relatives à la structure des fichiers conformément aux normes ISO/IEC 7816, sont nécessaires à la mise en œuvre des dispositions de l'[ODFI].

EXIGÉ : Les fichiers de la carte d'assuré sont organisés conformément à la norme ISO/IEC 7816-4. La structure des fichiers est illustrée dans la figure suivante. Chacun des fichiers est décrit dans les paragraphes qui suivent.



Les fichiers marqués d'un (*) contiennent des données médicales conformément à l'annexe 2 de l'[ODFI].

EXIGÉ : Des mesures techniques doivent empêcher l'éditeur de la carte d'accéder aux données médicales.

EXIGÉ : L'accès aux fichiers marqués d'un (*) n'est possible que moyennant authentification préalable et autorisation du groupe de fournisseurs de prestations correspondant.

EXIGÉ : Les fichiers marqués d'un (*) peuvent en outre être protégés contre tout accès au moyen d'un code PIN personnel.

EXIGÉ : Les prescriptions suivantes concernant les EF au niveau du MF sont impératives.

MF	Fichier maître	Actif
Répertoire racine, sélectionné implicitement après une réinitialisation de la carte à puce, où se trouvent tous les autres répertoires et dossiers. Toute carte à puce doit en avoir un.		

DF.NOT	Fichier dédié	Actif
Fonctionne comme fichier répertoire et rassemble tous les fichiers contenant des données utiles appartenant à une application. Les cartes à puce ayant plusieurs applications peuvent contenir plusieurs DF correspondants, chacun avec ses propres EF (p. ex. pour les essais pilotes cantonaux). Le fichier répertoire DF.NOT contient toutes les données nécessaires pour accéder aux données médicales de la carte d'assuré et les sauvegarder.		

EF.ARR ₁	Fichier de référence de règle d'accès			Interne
Structure : linéaire variable	Type : enregistrement	AM : R	SC :	
Est utilisé pour enregistrer une règle d'accès au niveau du MF.				
Fichier	Nom du fichier	Lecture	Ecriture / suppression	
Fichier de vérification du titulaire de la carte	EF.PIN	Octet d'activation + octet de statut + PIN	Octet d'activation + octet de statut + PIN	
Données accessibles en cas d'urgence	DF.NOT	Authentification ok	Authentification ok	
Facultatif : essai pilote cantonal	n.n.	n.n.	n.n.	
Autres règles d'accès	n.n.	n.n.	n.n.	

EF.ATR	Fichier de réponse à la réinitialisation			Actif
Structure : transparente	Type : BER-TLV	AM : R	SC :	
Après l'enclenchement de l'alimentation de tension, de l'horloge et du signal de réinitialisation, la carte à puce envoie à la broche (<i>pin</i>) I/O une réponse à la réinitialisation (Answer To Reset, ATR). Conformément à la norme ISO/IEC 7816-3, cette chaîne de caractères longue de 33 octets au maximum est toujours envoyée avec le diviseur 372 et contient des objets de données servant à identifier les caractéristiques d'exploitation de la carte (paramétrage du mode de transmission, identification, etc.). Ces objets de données sont conservés dans le fichier EF.ATR en mode lecture seule et ne peuvent être modifiés.				

EF.DIR	Fichier répertoire			Actif
Structure : linéaire variable	Type : enregistrement	AM : R	SC :	
EF.DIR contient les modèles d'application suivant la norme ISO/IEC 7816-4 pour les applications présentes sur la carte d'assuré. Ce fichier est particulièrement approprié pour sélectionner les applications des essais pilotes cantonaux. EF.DIR présente une structure d'enregistrement qui doit être affichée dans les octets d'historique.				

EF.ICCSN	Fichier d'identificateur de carte à puce [ICCSNF]			Actif
Structure : linéaire variable	Type : enregistrement	AM : R	SC :	
EF.ICCSN est le fichier où est enregistré le DO ICCSN (identificateur [balise] '5A'). L'ICCSN correspond au numéro d'identification de la carte d'assuré.				
Enregistrement 1 : SIMPLE-TLV: DO ICCSN (identificateur [balise] '5A')				
Enregistrement 2 : nombre de référence (binaire 8 octets)				
Enregistrement 3 : temps universel (GeneralizedTime[15 BCD] := YYYYMMDDHHMMSSZ)				

EF.PIN		Fichier de vérification du titulaire de la carte			Interne
Structure : ou bien/ou bien		Type : ou bien/ou bien		AM : R/UP	SC :
- transparente - linéaire variable		- chaîne binaire - enregistrement			
Lors de l'établissement de la carte, l'octet d'activation est réglé sur 0, autrement dit il est possible d'accéder aux données d'urgence sans code PIN. Quand l'assuré veut protéger au moyen d'un code PIN un fichier désigné par un (*) (voir structure des données), l'octet d'activation est réglé sur 1.					
Octet d'activation	Identificateur du PIN	Valeur du PIN	Présélection du nombre de tentatives	Valeur de déblocage du PIN	Nombre de tentatives de déblocage
0/1 ; non/oui	Référence ←	6-8 chiffres	5 tentatives	8 chiffres	10 tentatives

EF.StatusPIN		Statut de la saisie du PIN pour l'accès aux données d'urgence			Interne
Structure : linéaire fixe		Type : enregistrement		AM : R/UP	SC :
<ul style="list-style-type: none"> - Ce fichier contient le statut relatif à l'activation d'une saisie du PIN. - Il contient aussi le statut du PIN concernant le blocage ou la libération de chaque fichier (EF) de données d'urgence (voir EF.PIN). - Les règles d'accès sont contenues dans les fichiers respectifs EF.ARR₂ et EF.ARR₁. 					

EF.ID		Données d'identification			Actif
Structure : transparente		Type : BER-TLV		AM : R	SC :
Données d'identification conformément à l'annexe 1 de l'[ODFI]					

EF.AD		Données administratives			Actif
Structure : transparente		Type : BER-TLV		AM : R	SC :
Données administratives du titulaire de la carte conformément à l'annexe 1 de l'[ODFI]					

EF.LOG		Fichier journal		Actif
Structure : linéaire cyclique		Type : enregistrement (p. ex. 50 enregistrements)		AM : R/UP
				SC :
Fichier journal spécifique à l'application. Il contient des informations techniques sur le statut tout au long de la session. Cela rend possible une fonction de débogage (error recovery) et une fonction de récupération d'état (roll back).				

EF.S _B	Clé privée pour authentification asymétrique			Interne
Structure :		Type :		AM : R
- linéaire variable - transparente		- enregistrement - chaîne binaire		SC :
La procédure d'authentification carte à carte basée sur des CVC nécessite une clé privée globale S _B , sauvegardée dans un fichier de clé au-dessous du fichier maître MF. La clé publique correspondante est intégrée dans le certificat CVC.PDC qui se trouve dans le fichier conteneur EF.CVC.PDC.				

EF.CVC.PDC		Fichier pour CVC		Actif
Structure : transparente		Type : binaire		AM : R
				SC :
Le fichier EF.CVC.PDC contient le CVC de la carte d'assuré.				

EF.PK.CA_ORG_PDC		Clé publique racine pour authentification asymétrique		Interne
Structure :		Type :		AM : R
- linéaire variable - transparente		- enregistrement - chaîne binaire		SC :
Pour la procédure d'authentification C2C sur la base des CVC, une clé publique racine globale PK.CA_ORG_PDC est nécessaire. Elle est générée sur CVC-PKI hors ligne et enregistrée sous le fichier MF dans un fichier clé. La clé publique correspondante est intégrée au certificat CVC.CA_ORG_PDC qui est lisible dans le fichier conteneur EF.CVC.CA_ORG_PDC et ne peut être modifié. Cette clé racine est nécessaire pour l'examen dynamique du certificat délivré par les organisations de fournisseurs de prestations. Ces certificats sont chargés par l'appareil de lecture / module d'utilisation dans le fichier conteneur EF.CVC.CA_ORG_HPC et la signature correcte est vérifiée avec la clé publique racine.				

EF.CVC.CA_ORG_PDC		Fichier pour CVC		Actif
Structure: transparente	Type: binaire	AM: R	SC:	
Pour compléter, le certificat racine des assureurs CVC.CA_ORG_PDC est enregistré dans ce fichier conteneur. Un CVC occupe env. 220 octets.				

EF.CVC.CA_ORG_HPC		fichier pour CVC		Actif
Structure: transparente	Type: binaire	AM: R/W	SC:	
Ce fichier conteneur permet un examen dynamique des certificats provenant des fournisseurs de prestations ou de leurs organisations. Les certificats émanant des organisations qui sont enregistrés sur l'appareil de lecture / module d'utilisation sont en conséquence enregistrés sélectivement dans ce fichier conteneur. La hiérarchie de confiance est garantie par une vérification des certificats hiérarchisée à deux niveaux. Ce certificat est utilisé dans le cadre de la procédure d'authentification carte à carte pour la vérification des certificats. Un CVC occupe env. 220 octets				

EXIGÉ : Les prescriptions suivantes concernant les EF au niveau DF.NOT sont impératives.

EF.ARR₂		Fichier de référence de règle d'accès		Interne
Structure : linéaire variable	Type : enregistrement	AM : R	SC :	
Est utilisé pour sauvegarder des règles d'accès à l'intérieur du répertoire DF.NOT.				
Fichier	Nom	Lecture	Ecriture/suppression	
Données relatives au groupe sanguin et à la transfusion	EF.BGTD	Clé_1 + PIN	Clé_2 + PIN	
Données relatives aux vaccins	EF.IMMD	Clé_1 + PIN	Clé_2 + PIN	
Données relatives aux transplantations	EF.TPLD	Clé_1 + PIN	Clé_2 + PIN	
Allergies	EF.ALLG	Clé_1 + PIN	Clé_2 + PIN	
Maladies et séquelles d'accidents	EF.KHUF	Clé_1 + PIN	Clé_2 + PIN	
Inscriptions supplémentaires	EF.ZUSE	Clé_1 + PIN	Clé_2 + PIN	
Médication	EF.MEDI	Clé_1 + PIN	Clé_2 + PIN ou Clé_3 + PIN	
Adresses de contact	EF.ADDR	Clé_1	Clé_1	
Existence de directives anticipées	EF.VERF	Clé_1	Clé_1	

EF.AUT		Fichier de référence de l'autorisation			Interne
Structure : linéaire fixe		Type : enregistrement	AM : R	SC :	
Est utilisé pour l'attribution des règles d'accès à l'aide du code d'autorisation.					
Fournisseurs de prestations		Code d'autorisation	Clé_1	Clé_2	Clé_3
Médecins		CHA ₁	x	x	
Pharmaciens		CHA ₂	x		x
Dentistes		CHA ₃	x	x	
Chiropraticiens		CHA ₄	x	x	
Sages-femmes		CHA ₅	x		
Physiothérapeutes		CHA ₆	x		
Ergothérapeutes		CHA ₇	x		
Infirmiers		CHA ₈	x		
Logopédistes/orthophonistes		CHA ₉	x		
Diététiciens		CHA ₁₀	x		

EF.BGTD		Données relatives au groupe sanguin et à la transfusion		Actif
Structure : transparente		Type : BER-TLV	AM : R/UP/W	SC : EF.ARR ₂
Le contenu de l'objet de données structuré est défini dans l'annexe 2 de l'[ODFI].				

EF.IMMD		Données relatives aux vaccins		Actif
Structure : linéaire variable		Type : enregistrement (SIMPLE-TLV)	AM : R/UP/W	SC : EF.ARR ₂
Ce fichier doit être pris comme structure d'enregistrement. Chaque enregistrement contient un objet de données, codé en SIMPLE-TLV. Le contenu de chaque enregistrement et les objets structurés correspondants sont définis dans l'annexe 2 de l'[ODFI].				
Inscriptions :				
Enregistrements [1 .. 50]		Vaccinations		

EF.TPLD		Données relatives aux transplantations		Actif
Structure : linéaire variable		Type : enregistrement (SIMPLE-TLV)	AM : R/UP/W	SC : EF.ARR ₂
Ce fichier doit être pris comme structure d'enregistrement. Chaque enregistrement contient un objet de données, codé en SIMPLE-TLV. Le contenu de chaque enregistrement et les objets structurés correspondants sont définis dans l'annexe 2 de l'[ODFI].				
Inscriptions :				
Enregistrements [1 .. 10]		En attente de transplantation		
Enregistrements [11 .. 20]		Transplantations déjà effectuées		

EF.KHUF		Maladies et séquelles d'accidents		Actif
Structure : linéaire variable		Type : enregistrement (SIMPLE-TLV)	AM : R/UP/W	SC : EF.ARR ₂
Ce fichier doit être pris comme structure d'enregistrement. Chaque enregistrement contient un objet de données, codé en SIMPLE-TLV. Le contenu de chaque enregistrement et les objets structurés correspondants sont définis dans l'annexe 2 de l'[ODFI].				
Inscriptions :				
Enregistrements [1 .. 50]		Maladies et séquelles d'accidents		

EF.ZUSE		Inscriptions supplémentaires		Actif
Structure : linéaire variable		Type : enregistrement (SIMPLE-TLV)	AM : R/UP/W	SC : EF.ARR ₂
Ce fichier doit être pris comme structure d'enregistrement. Chaque enregistrement contient un objet de données, codé en SIMPLE-TLV. Le contenu de chaque enregistrement et les objets structurés correspondants sont définis dans l'annexe 2 de l'[ODFI].				
Inscriptions :				
Enregistrements [1 .. 10]		Mention de dossiers médicaux et pharmaceutiques disponibles		
Enregistrements [11 .. 35]		Autres inscriptions médicales et pharmaceutiques		

EF.MEDI Médication			Actif
Structure : linéaire variable	Type : enregistrement (SIMPLE-TLV)	AM : R/UP/W	SC : EF.ARR ₂
Ce fichier doit être pris comme structure d'enregistrement. Chaque enregistrement contient un objet de données, codé en SIMPLE-TLV. Le contenu de chaque enregistrement et les objets structurés correspondants sont définis dans l'annexe 2 de l'[ODFI].			
Inscriptions :			
Enregistrements [1 .. 50]		Médicaments pris en permanence	

EF.ALLG Allergies			Actif
Structure : linéaire variable	Type : enregistrement (SIMPLE-TLV)	AM : R/UP/W	SC : EF.ARR ₂
Ce fichier doit être pris comme structure d'enregistrement. Chaque enregistrement contient un objet de données, codé en SIMPLE-TLV. Le contenu de chaque enregistrement et les objets structurés correspondants sont définis dans l'annexe 2 de l'[ODFI].			
Inscriptions :			
Enregistrements [1 .. 25]		Réactions allergiques immédiates	
Enregistrements [26 .. 50]		Réactions allergiques retardées	

EF.ADDR Adresses de contact			Actif
Structure : linéaire variable	Type : enregistrement (SIMPLE-TLV)	AM : R/UP/W	SC : EF.ARR ₂
Ce fichier doit être pris comme structure d'enregistrement. Chaque enregistrement contient un objet de données, codé en SIMPLE-TLV. Le contenu de chaque enregistrement et les objets structurés correspondants sont définis dans l'annexe 2 de l'[ODFI].			
Inscriptions :			
Enregistrements [1 .. 10]		Adresses de contact en cas d'urgence	

EF.VERF	Existence de directives anticipées et de carte de donneur		Interne
Structure : linéaire variable	Type : enregistrement (SIMPLE-TLV)	AM : R/UP/W	SC : EF.ARR ₂
Ce fichier doit être pris comme structure d'enregistrement. Chaque enregistrement contient un objet de données, codé en SIMPLE-TLV. Le contenu de chaque enregistrement et les objets structurés correspondants sont définis dans l'annexe 2 de l'[ODFI].			
Inscriptions :			
Enregistrements [1 .. 10]		Mention de l'existence de directives anticipées et d'une carte de donneur	

DF.KtMV	Fichier dédié	Actif
Fonctionne comme fichier répertoire et rassemble tous les fichiers contenant des données utiles appartenant à une application. Les cartes à puce ayant plusieurs applications peuvent contenir plusieurs DF correspondants, chacun avec ses propres EF. Le fichier répertoire DF.KtMV contient toutes les données nécessaires pour accéder aux essais pilotes cantonaux.		

EF.X509-1	Fichier conteneur pour certificat X.509		Actif
Structure : transparente	Type : binaire	AM : One-time write	SC :
Fichier conteneur vide pour un fichier éventuel qui contiendrait un certificat X.509 dans le cadre d'un essai pilote cantonal. Le fichier de certificat en codage DER ne peut être sauvegardé qu'une seule fois et peut toujours être lu.			

EF.X509-2	Fichier conteneur pour certificat X 509		Actif
Structure : transparente	Type : binaire	AM : R/W	SC :
Fichier conteneur vide pour un fichier éventuel qui contiendrait un certificat X.509 dans le cadre d'un essai pilote cantonal. Le fichier de certificat en codage DER peut être sauvegardé, réécrit plusieurs fois et toujours être lu.			

EF.PuK _{x509}	Clé publique pour authentification asymétrique			Actif
Structure: - linéaire variable - transparente	Type: - enregistrement - chaîne binaire	AM: R	SC:	
Clé publique générée dans le cadre de l'initialisation et de la personnalisation par l'organisation émettrice de la carte d'assuré et enregistrée dans ce conteneur. Cette clé publique peut être utilisée pour un test d'exploitation dans le cadre d'un essai pilote cantonal et toujours lue. La clé privée correspondante est enregistrée dans le conteneur EF.PrK _{x509} et n'est pas lisible.				

EF.PrK _{x509}	Clé privée pour procédure asymétrique			Actif
Structure : - linéaire variable - transparente	Type : - enregistrement - chaîne binaire	AM : R	SC :	
Clé privée générée dans le cadre de l'initialisation et la personnalisation par l'organisation émettrice de la carte d'assuré et enregistrée dans ce fichier conteneur. Cette clé privée peut être utilisée pour un test d'exploitation dans le cadre d'un projet pilote cantonal et n'est pas lisible. La clé publique correspondante, enregistrée dans le conteneur EF.PrK _{x509} , est lisible.				

3.5 Gestion du PIN

Motivation : Les exigences de gestion du PIN conformes aux normes ISO/IEC 7816 sont nécessaires à la mise en œuvre des dispositions de l'[OCA].

3.5.1 Série de commandes

EXIGÉ : La série de commandes suivante est utilisée, conformément à la norme ISO/IEC 7816-4, pour la gestion du PIN :

- VERIFY
- CHANGE REFERENCE DATA
- RESET RETRY COUNTER
- ENABLE VERIFICATION REQUIREMENT
- DISABLE VERIFICATION REQUIREMENT
- TERMINATE CARD USAGE

3.5.2 Activation du PIN / Désactivation et saisie

La gestion du PIN ne nécessite pas d'authentification ni d'autorisation carte à carte. Le PIN peut être activé sur un appareil de lecture / module d'utilisation à clavier chez un fournisseur de prestations ou sur un appareil de lecture dédié à clavier chez l'assuré lui-même ou chez un autre fournisseur de prestations.

L'activation, la désactivation ou la saisie du PIN ne donne pas à elle seule accès aux données d'urgence.

3.5.3 Etats de protection du PIN

EXIGÉ : Tous les processus de détermination de l'état de protection du PIN sont effectués individuellement, de façon séquentielle, et ne peuvent être combinés.

3.5.3.1 Carte d'assuré après remise par l'assureur

EXIGÉ : Le dispositif PIN est désactivé. De la sorte, un libre accès réglementé à toutes les données d'urgence est possible, à condition que l'authentification carte à carte ait fonctionné et que l'autorisation ait été donnée.

3.5.3.2 Activation du dispositif PIN

EXIGÉ : Les opérations suivantes sont effectuées :

1. Activation du dispositif PIN.
2. Sélection des catégories de données d'urgence (fichiers EF) qui doivent être verrouillées ou déverrouillées au moyen d'un code PIN saisi sur un clavier par
3. Saisie du nouveau code PIN sur un clavier par l'assuré.

3.5.3.3 Modification du blocage par PIN pour des catégories de données d'urgence

EXIGÉ : Les opérations suivantes sont effectuées :

1. Saisie du code PIN sur un clavier par l'assuré.
2. Sélection des catégories de données d'urgence (fichiers EF) qui doivent être verrouillées ou déverrouillées au moyen d'un code PIN saisi sur un clavier par
3. Saisie du code PIN sur un clavier par l'assuré.

3.5.3.4 Modification du code PIN (dispositif PIN activé)

EXIGÉ : Les opérations suivantes sont effectuées :

1. Saisie du code PIN sur un clavier par l'assuré.
2. Saisie de la requête de modification sur un clavier par l'assuré.
3. Saisie du code PIN modifié sur un clavier par l'assuré.
4. Répétition de la saisie du code PIN sur un clavier par l'assuré.

3.5.3.5 Désactivation du dispositif PIN

EXIGÉ : Les opérations suivantes sont effectuées :

1. Saisie du code PIN sur un clavier par l'assuré.
2. Saisie de la requête de désactivation sur un clavier par l'assuré.

En cas de réactivation, les derniers blocages par PIN sont à nouveau actifs.

3.5.3.6 Dispositifs de blocage du code PIN

EXIGÉ : La saisie du PIN est bloquée après cinq tentatives erronées. Elle peut être débloquée au moyen d'un code PUK de 8 chiffres admettant un maximum de dix tentatives erronées. Après dix erreurs de saisie du code PUK, la carte d'assuré reste bloquée et ne peut plus être réactivée. Le code PUK aléatoire, initialisé par l'assureur lors de l'établissement de la carte, se trouve sur cette dernière.

3.6 Authentification carte à carte et autorisation

Motivation : Ces exigences sont nécessaires à la mise en œuvre des règles d'autorisation carte à carte de l'[OCA] ; voir aussi la motivation du ch. 3.3.1.

3.6.1 Principe

Le processus d'autorisation entre la CA (carte d'assuré) et la HPC (*Health Professional Card*) est basé sur une procédure asymétrique conforme à la norme ISO/IEC 9798-3. Pour cela, la CA et la HPC contiennent des CVC répondant aux exigences du ch. 3.6.2. Les certificats des fournisseurs de prestations contiennent en particulier la valeur d'autorisation CHA qui atteste l'appartenance à un groupe de fournisseurs de prestations (voir ch. 3.3.1). Comme les deux organisations (fournisseurs de prestations et assureurs) n'ont pas de secrets centraux communs et que l'authentification et l'autorisation reposent uniquement sur une procédure asymétrique avec un secret individuel des deux côtés, des vérifications sont nécessaires pour les certificats. Pour cela, la CA se fie à la clé racine publique non modifiable du CVC d'organisation(s) d'assureurs enregistrés sur cette carte. Tous les certificats délivrés par les organisations de fournisseurs de prestations ont été signés numériquement au moyen de la clé racine privée d'organisation(s) d'assureurs. Il est ainsi possible de vérifier avec certitude l'attestation de fournisseur de prestations par une vérification des certificats à deux niveaux, même dans le cas d'une attestation de fournisseur de prestations, chargée après coup et enregistrée entre-temps. En effet, la hiérarchie de certificats vérifiée se fonde sans lacune sur la clé racine publique non modifiée et enregistrée du CVC d'organisation(s) d'assureurs. Il est possible de vérifier en ligne ou hors ligne les certificats des assurés ainsi que ceux des organisations concernées à l'aide d'un appareil de lecture / module d'utilisation.

Pour l'authentification, la carte de l'assuré génère d'abord un nombre aléatoire R_B qu'elle envoie ensuite à la carte du fournisseur de prestations. Cette dernière signe ce nombre aléatoire au moyen de sa clé privée individuelle et renvoie le paquet de données signé à la carte de l'assuré. Celle-ci peut alors vérifier la signature propre au nombre aléatoire au moyen de la clé publique, qui est contenue dans le CVC de la carte du fournisseur de prestations. De cette façon, la carte du fournisseur de prestations s'est authentifiée pour la carte de l'assuré. Une authentification réciproque n'est pas nécessaire, car la carte d'assuré ne libère pas l'accès à la carte de fournisseur de prestations. Si ce processus d'authentification réussit, la carte d'assuré libère l'accès conformément à la valeur d'autorisation spécifique CHA (rôle, soit droit d'accès du FP) non modifiable, incluse dans le CVC de la carte du fournisseur de prestations. L'ensemble du processus d'authentification et

d'autorisation ne nécessite donc en principe que deux secrets individuels (les clés privées S_A et S_B). Ces secrets sont répartis entre des titulaires différents. L'authentification et l'autorisation ne posent aucune exigence de confidentialité quant à l'appareil de lecture / module d'utilisation.

3.6.2 Clés et certificats dans des entités

Pour une authentification et autorisation carte à carte efficace au moyen d'une procédure asymétrique, les certificats qui contiennent la clé publique et les clés privées qui s'y rapportent doivent être stockés dans les environnements mémoire correspondants. Pour cela, les fichiers et paramètres sur la partie privée d'une carte à puce ne sont pas lisibles de l'extérieur et ne peuvent être utilisés que par le système d'exploitation de la carte pour des procédures déterminées. Afin de rendre sûre la procédure d'authentification et autorisation carte à carte, qui exige des certificats vérifiables à partir de la carte (*Card verifiable certificates*, CVC), ces certificats doivent être lisibles et stockés de manière non modifiable dans la partie publique de la carte à puce en question. L'appareil de lecture / module d'utilisation ne joue dans cette procédure qu'un rôle de « présentateur » et produit, le cas échéant, une liaison en ligne avec les entités émettrices. Comme il peut aussi être utilisé hors ligne, les certificats nécessaires actuels peuvent être téléchargés au préalable depuis Internet et mémorisés dans la partie dite publique de l'appareil de lecture / module d'utilisation. Aucune protection particulière de l'appareil de lecture / module d'utilisation n'est nécessaire pour garantir la protection des données personnelles médicales de l'assuré.

EXIGÉ : Les clés et certificats suivants sont appliqués sur la carte HPC, l'appareil de lecture / module d'utilisation et la CA.

A: Carte HPC

Partie publique	Partie privéé
- CVC.HPC[P _A]	- S _A

T: Appareil de lecture / module d'utilisation

Partie publique	Partie privéé
- X509.CA_Pub _{x1} - X509.CA_Pub _{x2} - X509.CA_ORG_PDC _m - X509.CA_ORG_HPC _m - CVC.CA_ORG_PDC _m [PK.CA_ORG_PDC _m] - CVC.CA_ORG_HPC _m [PK.CA_ORG_HPC _m]	

B: Carte d'assuré

Partie publique	Partie privéé
- CVC.CA_ORG_HPC _m [PK.CA_ORG_HPC _m] - CVC.CA_ORG_PDC _m [PK.CA_ORG_PDC _m] - CVC.PDC[P _B]	- PK.CA_ORG_PDC _m - S _B

Indications sur la carte d'assuré [B]	
S_B	Clé privée assignée à la clé publique P_B dans le certificat de personne
$CVC.PDC[P_B]$	Certificat de personne, avec la clé publique P_B qu'il contient
$PK.CA_ORG_PDC_m$	Clé racine publique du CVC d'organisation(s) d'assureurs
$CVC.CA_ORG_PDC_m[PK.CA_ORG_PDC_m]$	CVC d'organisation(s) de fournisseurs de prestations, avec $m:= 1 \dots n$; p. ex. 10 certificats d'organisation de fournisseurs de prestations.
$CVC.CA_ORG_HPC_m[PK.CA_ORG_HPC_m]$	CVC d'organisation(s) d'assureurs

Indications sur la carte de fournisseur de prestations [A]	
$CVC.HPC[P_A]$	CVC du fournisseur de prestations, avec la clé publique P_A qu'il contient
S_A	Clé privée assignée à la clé publique P_A dans le certificat du fournisseur de prestations
Autres certificats possibles	Ne font pas l'objet des réglementations relatives à la carte d'assuré

Indications sur l'appareil de lecture / module d'utilisation [T]	
$CVC.CA_ORG_PDC_m[PK.CA_ORG_PDC_m]$	CVC d'organisation(s) d'assureurs
$CVC.CA_ORG_HPC_m[PK.CA_ORG_HPC_m]$	CVC d'organisation(s) de fournisseurs de prestations, avec $m:= 1 \dots n$; p. ex. 10 certificats d'organisations de fournisseurs de prestations
$X509.CA_ORG_PDC_m$	Certificat du serveur conforme à X.509 (RFC 3280) d'organisation(s) d'assureurs
$X509.CA_ORG_HPC_m$	Certificat du serveur conforme à X.509 (RFC 3280) d'organisation(s) de fournisseurs de prestations, avec $m:= 1 \dots n$; p. ex. 10 certificats du serveur d'organisation(s) de fournisseurs de prestations
$X509.CA_Pub_x$	Certificat d'émetteur conforme à X.509 (RFC 3280) du fournisseur de service de certification reconnu, avec possibilité que $x:= 1 \dots n$

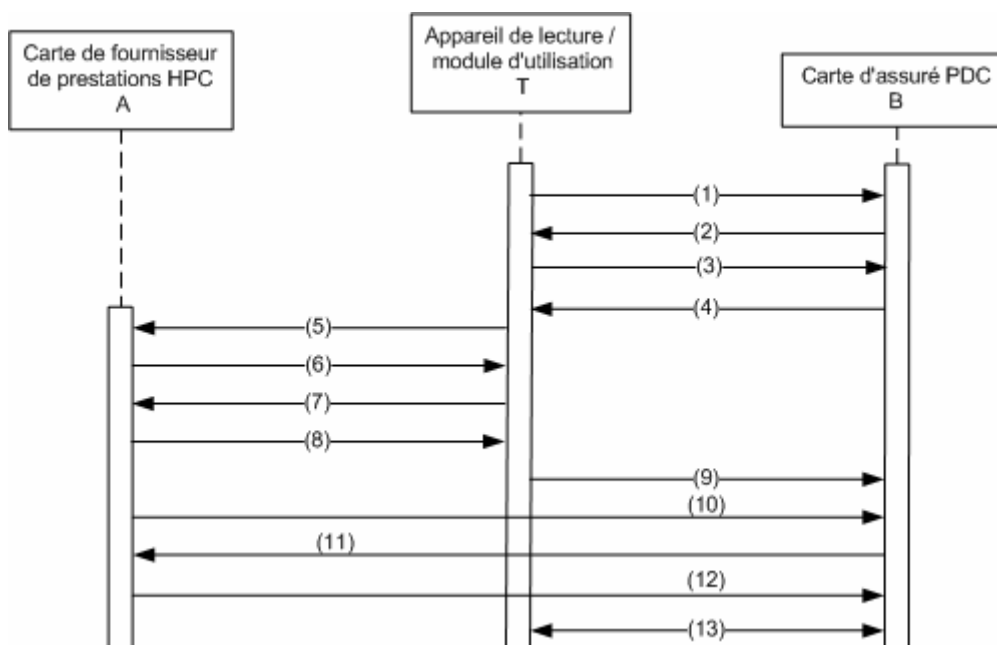
3.6.3 Termes et abréviations

	Signification
CHA ₁	Médecins
CHA ₂	Pharmaciens
CHA ₃	Dentistes
CHA ₄	Chiropraticiens
CHA ₅	Sages-femmes
CHA ₆	Physiothérapeutes
CHA ₇	Ergothérapeutes
CHA ₈	Infirmiers
CHA ₉	Logopédistes/orthophonistes
CHA ₁₀	Diététiciens
CHA _m	Autorisation du titulaire de carte, intégrée dans le CVC codé
R _x	Nombre aléatoire généré par l'entité X
sS _x	Codage au moyen de la clé privée secrète de l'entité X
sP _x	Vérification de la signature au moyen de la clé publique de l'entité X
CVC	Certificat vérifiable à partir de la carte
X509	Certificat basé sur la norme RFC 3280, codé avec des règles distinctives (DER)
PK.A	Clé publique de A
{ ... }	Paquet de données
ICCSNF	Fichier identificateur de la carte à puce
A[B]	B inclus dans A
	Opérateur de composition
A ⊂ B	A inclus dans B
< .. >	Pointeur sur un objet
A ← B	Pointeur à l'intérieur d'un objet
A(B;C;..)	Opérateur, A appliqué sur B et C, etc.

3.6.4 Procédure

3.6.4.1 Authentification et autorisation carte à carte hors ligne

EXIGÉ : L'accès est obtenu conformément au schéma suivant :



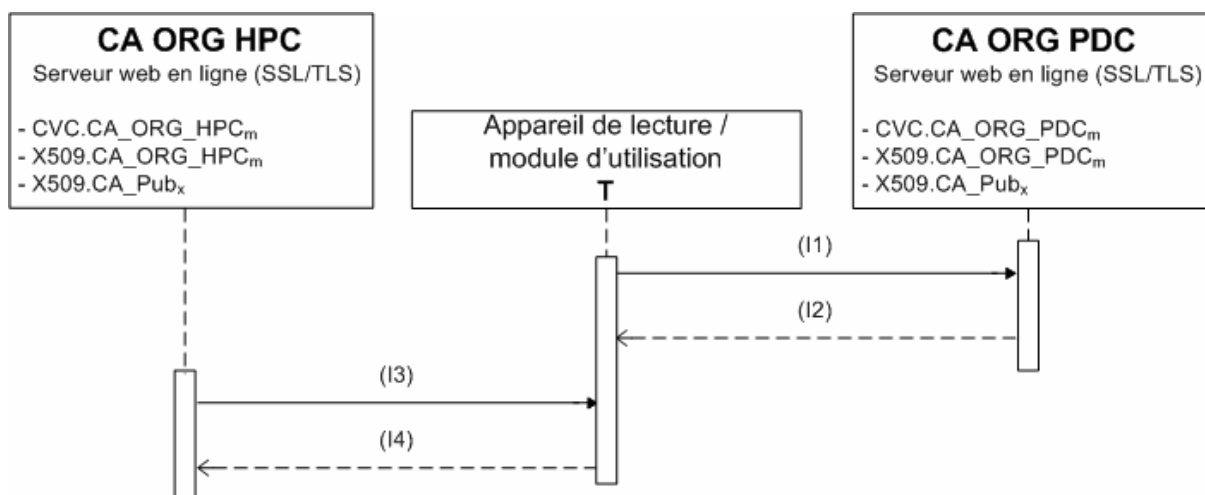
1	(1)	SelectFile ReadRecord {ICCSNF _B }
	REM	Sélection et lecture des fichiers d'identification de la carte à puce
2	(2)	{ICCSNF _B }
	REM	Transmission des fichiers identificateurs de la carte à puce sur la carte d'assuré
3	(3)	SelectFile ReadBinary (EF.CVC.PDC)
	REM	Sélection et lecture du CVC de personne de l'assuré
4	(4)	{CVC.PDC}
	REM	Transmission du CVC de personne de l'assuré
5	(T)	{ MSE SET<PK.CA_ORG_PDC _m ←(CVC. CA_ORG_PDC _m)>
	REM	Installation de la clé racine publique de l'organisation d'assureurs de l'assuré
6	(T)	PSO VERIFY CERTIFICATE(CVC.PDC) → nok→interrompre ; ok→continuer ; enregistrer (CHR _B); extraire (ICCSN _B)
	REM	Vérification du CVC de personne de l'assuré

6a	(T)	Facultatif : comparer (ICCSNF _B [ICCSN _B] ; EF.CVC.PDC[ICCSN _B])
	REM	Vérification du numéro de série de la carte à puce en comparant les numéros figurant sur la carte et dans le CVC de personne
7	(5)	SelectFile ReadRecord {ICCSNF _A }
	REM	Sélection et lecture des fichiers d'identification de la carte à puce
8	(6)	{ICCSNF _A }
	REM	Transmission des fichiers d'identification de la carte à puce figurant sur la carte de fournisseur de prestations
9	(7)	SelectFile ReadBinary (EF.CVC.HPC)
	REM	Sélection et lecture du CVC de fournisseur de prestations
10	(8)	{CVC.HPC}
	REM	Transmission du CVC de fournisseur de prestations
11	(T)	Read Extract(CVC.HPC) -> (CPI = 04, CAR, CHR, CHA) -> enregistrer
	REM	Lecture et enregistrement des attributs de fournisseur de prestations nécessaires provenant du certificat de fournisseur de prestations
12	(T)	Search((CPI = 04, CAR, CHR, CHA), (CVC.CA_ORG_HPC _m)) _m ; -> sélectionner(CVC.CA_ORG_HPC _m)
	REM	Le certificat correspondant des organisations de fournisseurs de prestations est sélectionné à l'aide des attributs de fournisseur de prestations
13	(T)	SelectFile WriteBinary(CVC.CA_ORG_HPC _m) ->
	REM	Le fichier conteneur pour le certificat des organisations de fournisseurs de prestations est sélectionné et doit être décrit
14	(9)	{CVC.CA_ORG_HPC _m } -> EF.CVC.CA_ORG_HPC
	REM	Transmission et enregistrement du certificat des organisations de fournisseurs de prestations
15	(10)	{CVC.HPC[P _A]}
	REM	Le CVC de fournisseur de prestations est transféré à la carte d'assuré pour vérifier si la communication est possible
16	(B)	MSE SET<PK.CA_ORG_PDC _m
	REM	Installation de la clé racine publique de l'organisation d'assureurs de l'assuré
17	(B)	PSO VERIFY CERTIFICATE(CVC.CA_ORG_HPC _m)

		nok→interrompre; ok→continuer; enregistrer (PK.CA_ORG_HPC _m)
	REM	Examen du CVC de l'organisation émettrice correspondante
18	(B)	MSE SET<PK.CA_ORG_HPC _m ←(CVC.CA_ORG_HPC _m)>
	REM	Installation de la clé CA publique de l'organisation de fournisseurs de prestations correspondante
19	(B)	PSO VERIFY CERTIFICATE(CVC.HPC) → nok→interrompre ; ok→continuer
	REM	Examen du CVC de fournisseur de prestations
20	(B)	Store(CHA _n)
	REM	Enregistrement intermédiaire de la valeur caractéristique pour l'autorisation du titulaire de la carte CHA _n , qui est rattachée au certificat de fournisseur de prestations
21	(B)	Generate(R _B)
	REM	Création du nombre aléatoire
22	(11)	{R _B }
	REM	Transmission du nombre aléatoire
23	(A)	sS _A (R _B)
	REM	Attestation du nombre aléatoire par une signature numérique
24	(12)	{sS _A (R _B)}
	REM	Transmission du nombre aléatoire signé
25	(B)	sP _A (sS _A (R _B)); R _B = R _B → ok→continuer; nok→interrompre
	REM	Vérification de la signature du nombre aléatoire
26	(B)	(CHA _n); Autorisation ok!
	REM	La valeur caractéristique pour l'autorisation du titulaire de la carte CHA _n est libérée
27	(13)	L'appareil de lecture / module d'utilisation ne peut intervenir maintenant sur la carte d'assuré qu'au moyen de la valeur caractéristique pour l'autorisation de titulaire de la carte (CHA _n)
	REM	Echange de données entre l'appareil de lecture / module d'utilisation et la carte d'assuré

3.6.4.2 Vérification de certificat en ligne / hors ligne (facultative)

FACULTATIF : Les certificats peuvent être téléchargés pour vérification par l'appareil de lecture / module d'utilisation en ligne et hors ligne.



1	(i1)	Obtenir certificats \subset CA_ORG_PDC _m : - CVC.CA_ORG_PDC _m - X509.CA_ORG_PDC _m - X509.CA_Pub _x
2	(i2)	Télécharger certificats \subset CA_ORG_PDC _m : - CVC.CA_ORG_PDC _m - X509.CA_ORG_PDC _m - X509.CA_Pub _x
3	(i3)	Obtenir certificats \subset CA_ORG_HPC _m : - CVC.CA_ORG_HPC _m - X509.CA_ORG_HPC _m - X509.CA_Pub _x
4	(i4)	Télécharger certificats \subset CA_ORG_HPC _m : - CVC.CA_ORG_HPC _m - X509.CA_ORG_HPC _m - X509.CA_Pub _x

3.6.4.3 PKI hors ligne des organisations émettrices pour l'établissement de CVC

Motivation : Ces exigences sont suffisantes pour définir le CVC PKI hors ligne des organisations émettrices. Ces dernières doivent impérativement les mettre en œuvre pour la vérification facultative des certificats et des chaînes de certificats.

EXIGÉ : Le CVC PKI hors ligne se trouve dans un domaine de sécurité protégé par des zones de sécurité définies, avec des barrières de sécurité et des contrôles d'accès

appropriés.
La création d'une signature sûre exige l'emploi de techniques et de procédés appropriés pour qu'au moins :

- a) **EXIGÉ** : les données utilisées pour créer la signature ne puissent apparaître qu'une fois et que les garanties de leur confidentialité soient suffisantes ;
- b) **EXIGÉ** : il soit suffisamment sûr que l'on ne puisse pas remonter par déduction à ces données et que la signature soit à l'abri de toute falsification lors de l'utilisation des techniques disponibles ;
- c) **EXIGÉ** : le signataire légitime puisse empêcher de façon sûre que les données utilisées pour créer la signature soient utilisées par d'autres ;
- d) **RECOMMANDÉ** : des modules matériels de sécurité (HSM) satisfaisant aux exigences de certification FIPS 140 de niveau 3 doivent être utilisés pour mieux protéger la clé privée.

EXIGÉ : Les clés publiques du CVC PKI hors ligne (PK.CA_ORG_PDC_m, PK.CA_ORG_HPC_m) des organisations émettrices respectives doivent être incluses dans les certificats correspondants (CVC.CA_ORG_PDC_m, CVC.CA_ORG_HPC_m) au format CVC d'après ISO/IEC 7816-8 dans les éléments de données référencés par les balises '7F49' et '5F38' (cf. ch. 6.1). Ces certificats doivent au moyen d'un service en ligne être établis sur un serveur web en utilisant un certificat de serveur public (cf. ch. 6.2), qui est fourni par un fournisseur de services de certifications reconnu au sens de la SCSE comme fichier dans la codification selon ISO/IEC 7616-8. Ils peuvent être téléchargés via Internet par l'appareil de lecture / module d'utilisation pour vérifier la chaîne de certificats ou pour vérifier le CVC de personne sur la carte d'assuré au moyen des protocoles SSL/TLS (étapes du processus (i1, i2) ou (i3, i4)).

EXIGÉ : Les certificats de serveur (X509.CA_ORG_HPC_m.X509.CA_ORG_PDC_m) des services en ligne nécessaires provenant des organisations émettrices doivent également être disponibles sur le serveur web dans le codage DER usuel selon X.690 (ISO/IEC 8825-1), de sorte qu'ils puissent être téléchargés au moyen de SSL/TSL sur Internet via l'appareil de lecture / module d'utilisation. Ces certificats peuvent en outre être utilisés pour prouver électroniquement sur l'appareil de lecture / module d'utilisation une relation de confiance entre le certificat de serveur public de l'organisation émettrice correspondante et le CVC de l'organisation émettrice qui s'y rattache (i1, i2) ou (i3, i4).

EXIGÉ : Les organisations émettrices rendent également disponible sur leur serveur web en ligne, en tant que fichier en codage DER usuel selon X.690 (ISO/IEC 8825-1), le certificat d'émetteur (X509.CA_Pub_x) du fournisseur de services de certification reconnu au sens de

la SCSE. Ce certificat peut ainsi être téléchargé via Internet sur l'appareil de lecture / module d'utilisation au moyen de SSL/TLS. De cette manière, la chaîne de confiance des certificats concernant les certificats de serveur en ligne sur le serveur web des organisations émettrices et les certificats d'émetteur CA des fournisseurs de services de certification reconnus selon la SCSE peut être vérifiée électroniquement par l'appareil de lecture / module d'utilisation (i1, i2) ou (i3, i4).

3.6.4.4 Vérification en ligne / hors ligne des certificats

RECOMMANDÉ : Les vérifications suivantes sont effectuées sur l'appareil de lecture / module d'utilisation :

1. Vérification de la relation entre les certificats de serveur (X509.CA_ORG_HPC_m, X509.CA_ORG_PDC_m) des services web en ligne nécessaires des organisations émettrices et les certificats d'organisation émettrices correspondants (CVC.CA_ORG_PDC_m.CVC.CA_ORG_HPC_m) : par une comparaison des attributs descriptifs dans le champ du sujet du certificat de serveur de l'organisation émettrice et l'élément de données CAR – plus les éléments de données qui contiennent la clé publique correspondante dans le CVC de l'organisation émettrice – un rapport de confiance et une classification peuvent être prouvés électroniquement entre les deux certificats et leurs organisations sur l'appareil de lecture / module d'utilisation au moyen de la transformation correspondante (cf. 6.2.2).
2. Vérification des signatures des certificats de serveur (X509.CA_ORG_HPC_m.X509.CA_ORG_PDC_m) avec les certificats émetteurs (X509.CA_Pub_x) sur l'appareil de lecture / module d'utilisation.
3. Vérification de la chaîne de certificats au moyen des attributs (AuthorityKeyIdentifier, SubjectKeyIdentifier) sur les certificats correspondants (X509.CA_ORG_PDC_m→X509.CA_Pub_x) sur l'appareil de lecture / module d'utilisation.

Les spécifications des CVC et X.509 figurent au chap. 6.

3.6.4.5 Exigences concernant la spécification de détail

EXIGÉ : Les spécifications de détail doivent comporter toutes les commandes de base, les fonctions de base du système d'exploitation, les fonctions et algorithmes de sécurité fondamentaux, les spécifications de détail concernant les structures et les composants des fichiers et sont chargés lors de l'initialisation et de la personnalisation de la carte d'assuré, dans la mesure où ces éléments sont importants pour la garantie de l'interopérabilité dans la communication et l'accès.

EXIGÉ : Les spécifications de détail renferment les messages d'erreurs pré-établis de manière uniforme.

RECOMMANDÉ : L'émetteur de la carte met à disposition une interface de programmation de l'application.

4 Procédure de consultation en ligne au sens de l'art. 15 [OCA]

4.1 Principe

L'assureur propose, pour consulter les données selon l'annexe 3 de l'[ODFI], les trois possibilités suivantes :

EXIGÉ : Accès manuel avec les navigateurs Internet usuels au moyen de HTTP v1.1 sur SSL v3.0 ou TLS v1.0.

EXIGÉ : Accès à la base SOAP via un service web. Le protocole SOAP doit être relié à HTTP v1.1 par SSL v3.0 ou TLS v1.0.

EXIGÉ : Accès direct par réacheminement web en HTTP/1.1, SSL v3.0 ou TLS v1.0.

4.2 Exigences en matière de communication

EXIGÉ : La transmission de données est verrouillée au moyen d'un des protocoles ci-dessous, connus des navigateurs Internet actuels :

- Secure Socket Layer SSL v3.0 (netscape 1996) ; SSL v2.0 exclu !
- Transport Layer Security TLS v1.0 [RFC 2246, RFC 3546] (si l'on a le choix, préférer SSL v3.0).

EXIGÉ : La clé est longue d'au moins 1024 bits pour la procédure de codage asymétrique, d'au moins 168 bits pour la procédure symétrique 3DES et d'au moins 256 bits pour la procédure symétrique AES.

EXIGÉ : Les protocoles et normes suivants sont utilisés pour la consultation en ligne :

- Protocole HTTP (version 1.1, RFC 2616)
- Protocole de transmission SOAP (à partir de la version 1.2)
- XML
- WSDL à partir de la version 1.2

4.3 Accès direct en ligne au moyen de HTTP via SSL/TLS

4.3.1 Navigateur Internet sur l'ordinateur du fournisseur de prestations

EXIGÉ : Les procédures de consultation en ligne ne peuvent fonctionner que sur des navigateurs Internet usuels, sans fonctionnalités spécifiques au produit, pour lesquels les spécifications et protocoles suivants doivent être connus :

- Protocole HTTP (version 1.1, RFC 2616)
- Codage unilatéral, basé sur le certificat du serveur utilisant les protocoles SSL v3.0 ou TLS v1.0

4.3.2 Contrôle d'accès

- EXIGÉ :**
- L'accès est contrôlé au moyen de l'ID et du mot de passe.
 - L'accès est refusé après cinq tentatives infructueuses.
 - L'accès passe par un codage unilatéral basé sur le certificat de serveur.

FACULTATIF : Pour augmenter la sécurité d'accès et diminuer les consultations abusives, des procédures supplémentaires peuvent être utilisées. Par exemple : procédure *challenge-response* (Grid, SMS, etc.), procédure HIP (*Human interactive proof*).

4.4 Accès en ligne direct au moyen de SOAP/HTTP via SSL/TLS

4.4.1 Procédure de consultation en ligne depuis des applications chez le fournisseur de prestations

4.4.1.1 Protocoles d'accès

EXIGÉ : Les spécifications et protocoles suivants doivent être connus :

- Protocole HTTP (version 1.1, RFC 2616)
- Protocole de transmission SOAP (à partir de la version 1.2) pour l'accès direct à la lecture des données administratives, qui est lié à HTTP v1.1.
- Au moins un codage unilatéral, basé sur le certificat, avec les protocoles SSL v3.0 ou TLS v1.0.

REMARQUE : L'OFSP met à disposition les schémas XML et les définitions d'interfaces WSDL.

4.4.1.2 Contrôle de l'accès

EXIGÉ : L'accès est contrôlé par l'ID et le mot de passe. En l'occurrence, l'ID et le mot de passe peuvent être enregistrés dans l'application du fournisseur de prestations pour laquelle une protection de lecture et d'accès doit être mise en place de telle sorte qu'une utilisation abusive soit hautement improbable. L'accès est verrouillé après cinq tentatives de mot de passe au maximum.

FACULTATIF : Les assureurs peuvent demander pour les accès des fournisseurs de prestations ayant un grand volume de consultation un codage double, basé sur le certificat, au moyen des protocoles SSL v3.0 ou TLS V1.0. Ce faisant, les assureurs peuvent créer un fichier avec un fichier conteneur protégé par un mot de passe en format PKCS#12 contenant la clé privée avec le certificat X.509 correspondant selon la norme RFC 3280. Ce fichier sera enregistré dans l'application du fournisseur de prestations avec une protection de lecture et d'accès appropriée de sorte qu'un usage abusif soit hautement improbable.

4.4.2 Procédure de consultation directe en ligne passant par le serveur pour des services chez les fournisseurs de prestations ou des tiers qu'ils ont mandatés

4.4.2.1 Protocole d'accès

EXIGÉ : Les spécifications et les protocoles suivants doivent être connus :

- Protocole HTTP (version 1.1, RFC 2616)
- Protocole de transmission SOAP (à partir de la version 1.2) pour la lecture directe des données administratives, qui est relié à HTTP v1.1
- Codage double, basé sur le certificat, avec les protocoles SSL v3.0 ou TLS v1.0

REMARQUE : L'OFSP met à disposition les schémas XML et les définitions d'interfaces WSDL.

4.4.2.2 Contrôle de l'accès

EXIGÉ : Les assureurs définissent les valeurs caractéristiques d'accès nécessaires pour cette catégorie de services et, le cas échéant, un complément à la définition des interfaces donnée par l'OFSP dans WSDL. L'accès se base, selon les cas, sur une ou plusieurs combinaisons des caractéristiques suivantes :

- ID et mot de passe des fournisseurs de prestations respectifs, qui ont transmis leurs droits d'accès en communiquant à un fournisseur tiers les valeurs de leurs caractéristiques ;
- ID d'accès dédié
- Autres valeurs caractéristiques (p. ex. groupes ID, n°RCC).

Toutes les valeurs de ces caractéristiques doivent être enregistrées dans une banque de données sur le serveur du tiers auprès du fournisseur de prestations ou dans une institution qu'il a mandatée avec une protection d'accès et de lecture appropriée pour que toute utilisation abusive soit exclue. L'accès est verrouillé après cinq tentatives d'accès infructueuses.

FACULTATIF : Les assureurs peuvent dans le cas de service ayant un grand volume de consultations exiger, pour l'accès aux données, un codage double basé sur le certificat, via un canal de communication protégé, au moyen des protocoles SSL v3.0 ou TLS v1.0.

Motivation : Le risque d'abus est beaucoup plus élevé pour les possibilités d'accès modifiées et exige des mesures de sécurité plus strictes.

Pour une meilleure protection de la clé privée et de la connexion sécurisée de l'identité au serveur du fournisseur de prestations, il faut installer un module matériel de sécurité HSM (*Hardware security module*), qui suffit à satisfaire aux exigences selon FIPS 140, niveau 3. Le certificat X.509 selon RFC 3280 qui s'y rattache doit être exigé avec une demande de certificat qui est transmise au service correspondant de l'assureur en format PKCS#10 (RFC 2986). Le service de certification de l'assureur établit sous réserve d'une vérification exacte de l'identité du requérant un certificat signé correspondant sur son PKI -X.509 hors ligne et l'envoie finalement comme fichier en codage DER ou PEM (X.690/ISO 8825 ou RFC 1421-RFC 1424) au requérant. Les assureurs définissent l'échange de données sécurisé nécessaire ainsi que la vérification de l'identité.

EXIGÉ : Les assureurs fixent un accord de niveau de service SLA (*Service level agreement*), qui sert de base pour cette catégorie de consultations en ligne et doit être conclu entre assureurs et fournisseurs de prestations.

4.4.2.3 Connexion client - serveur

La connexion établie entre le client et le serveur de service chez le fournisseur de prestations ou dans une institution qu'il a mandatée doit au moins satisfaire aux exigences techniques suivantes :

EXIGÉ : Connexion verrouillée de bout en bout pour laquelle les exigences concernant le verrouillage doivent au moins satisfaire les définitions du ch. 4.2.

EXIGÉ : L'accès est contrôlé au moins par l'ID et le mot de passe.

4.4.2.4 Service de certification des assureurs pour les certificats selon X.509 (RFC 3280)

EXIGÉ : il suffit que les assureurs utilisent ou fassent utiliser, pour la mise à disposition des certificats et des services de certification demandés, un X.509-PKI hors ligne sans service public de répertoire.

4.5 Accès authentifié par l'intermédiaire d'un fournisseur de services réseau (service d'authentification)

Dans ce mode d'utilisation, l'identification et l'authentification sont effectuées par le fournisseur de services réseau au moyen des services correspondants. L'attribution d'un utilisateur authentifié et identifié à un numéro RCC, le cas échéant à un nom de groupe, ainsi qu'à un ID d'utilisateur autorisé se fait directement par le serveur d'authentification du fournisseur de services réseau. Comme ce serveur transmet ces ID au serveur de service des assureurs par une connexion sûre et sécurisée, l'accès peut être libéré pour la consultation des données du fournisseur de prestations au moyen d'un navigateur Internet ou d'applications du fournisseur de prestations directement, sans étape d'authentification supplémentaire. Une solution d'authentification basée sur le certificat du côté de l'application du fournisseur de prestations n'est plus nécessaire ici.

4.5.1 Gestion de l'identité et des accès

EXIGÉ : Les assureurs mettent à disposition des fournisseurs de services réseau un mode de gestion des accès qui permet aux utilisateurs autorisés d'accéder directement à leur serveur de service pour une consultation en ligne, sans autre authentification.

EXIGÉ : Les assureurs garantissent au moyen d'une procédure appropriée que seuls les utilisateurs autorisés obtiennent d'un fournisseur de services réseau un accès direct de leur réseau maison au serveur de service des assureurs. L'autorisation d'effectuer une consultation en ligne est donnée par les assureurs.

EXIGÉ : La transmission des données nécessaires à l'accès du serveur d'authentification du fournisseur de services réseau au serveur de service des assureurs est effectuée par un message SOAP via un protocole de transport sûr.

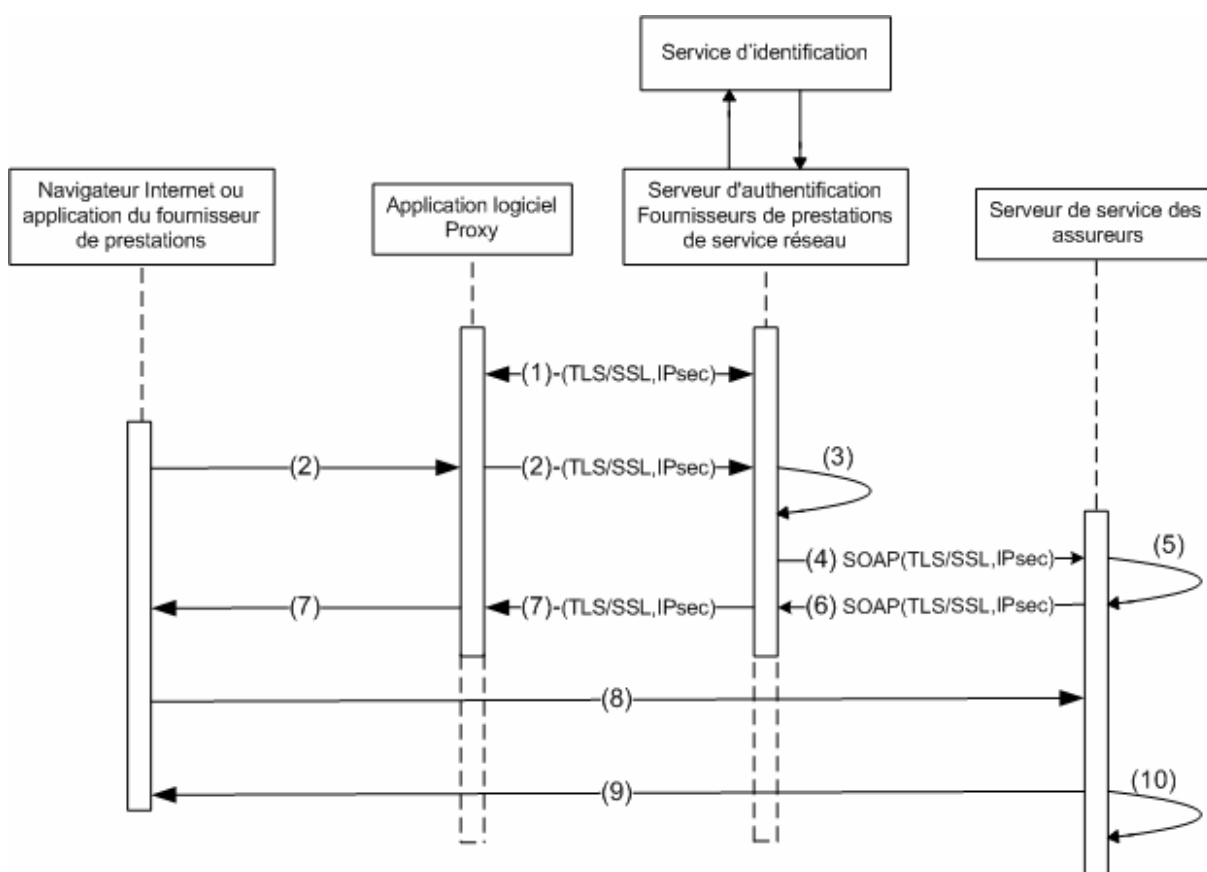
EXIGÉ : Les assureurs définissent sur la base de SOAP un protocole de transmission de message d'accès présentant les caractéristiques suivantes :

- ID pour accès dédié
- autres valeurs caractéristiques (p. ex. ID de groupe, numéro RCC)

EXIGÉ Les assureurs définissent la procédure en utilisant des outils électroniques appropriés qui permettent au fournisseur de services réseau et aux assureurs une gestion des accès sécurisée et imputable avec de faibles frais administratifs. De cette manière, un utilisateur authentifié du réseau maison d'un fournisseur de services réseau peut accéder, sans autre authentification et autorisation, au serveur de service des assureurs pour effectuer une consultation en ligne.

4.5.2 Procédure d'accès

EXIGÉ : La procédure décrite ci-dessous doit être respectée. L'utilisation d'un proxy est néanmoins facultative.



- (1) Le fournisseur de prestations s'authentifie de son réseau maison sur le serveur d'authentification du fournisseur de services réseau au moyen d'un logiciel mandataire dédié et suivant une authentification mutuelle client/serveur forte. Si l'authentification réussit, un canal de données chiffré sûr est établi entre le service mandataire sur la

- plate-forme des fournisseurs de prestations et le service de communication du fournisseur de services réseau.
- (2) Le fournisseur de prestations demande sur le serveur d'authentification du fournisseur de services réseau, à partir de son navigateur Internet (http, SSL/TLS) ou de sa propre application (SOAP/http, SSL/TLS), au moyen d'une adresse dédiée (URL), le service de consultation en ligne des assureurs.
 - (3) Le serveur d'authentification du fournisseur de services réseau intègre dans le protocole de transmission de message d'accès SOAP défini l'ID dédié et la valeur d'autorisation spécifique de l'utilisateur dûment enregistré pour l'accès au serveur de service des assureurs au moyen des données d'identification qui sont fournies par le service d'identification du fournisseur de services réseau.
 - (4) Le serveur d'authentification du fournisseur de services réseau envoie le message d'accès SOAP au serveur de service des assureurs via un protocole de transport sûr.
 - (5) Le serveur de service des assureurs reçoit et traite le message d'accès SOAP, vérifie l'ID dédié et la valeur d'autorisation spécifique, génère un ID de session aléatoire, crée et admet l'autorisation d'accès spécifique (URL, ID de session, temps limite) et intègre dans un nouveau message d'accès SOAP, pour réacheminement HTTP sur le web, l'URI et l'ID de session.
 - (6) Le serveur de service des assureurs envoie ce message d'accès SOAP au serveur d'authentification du fournisseur de services réseau.
 - (7) Le serveur d'authentification du fournisseur de services réseau crée, à partir des données contenues dans le message d'accès SOAP, le réacheminement HTTP dédié sur le web et l'envoie dans le canal de données chiffré, par le service mandataire identifié, au navigateur Internet ou à l'application du fournisseur de prestations.
 - (8) Le navigateur Internet ou l'application du fournisseur de prestations se connecte au moyen du réacheminement HTTP (URL, ID de session) au portail de consultation dédié du serveur de service des assureurs de telle sorte qu'un codage unilatéral de bout en bout, basé sur un certificat, puisse être garanti au moyen du protocole de transport sûr (SSL 3.0/TLS 1.0). Le canal de données chiffré (SSL/TLS) entre le navigateur Internet ou l'application du fournisseur de prestations et le serveur de service des assureurs peut passer soit à l'intérieur du canal de données du fournisseur de services réseau, soit à l'extérieur, via Internet.
 - (9) En cas de déconnexion normale, la session est fermée et, le cas échéant, le vecteur d'adresse est rendu au navigateur Internet ou à l'application du fournisseur de prestations par réacheminement HTTP via le fournisseur de services réseau.
 - (10) En cas de déconnexion anormale ou en l'absence de déconnexion, la session est fermée automatiquement après un temps limite défini.

EXIGÉ : Les assureurs fixent un accord de niveau de service (*Service level agreement* SLA) qui sert de base à cette catégorie de services de consultations en ligne et doit être conclu entre les assureurs et les fournisseurs de prestations.

5 Essais pilotes cantonaux au sens de l'art. 16 [OCA]

- **EXIGÉ** : La carte d'assuré contient un répertoire dédié (fichier répertoire DF) réservé aux essais pilotes cantonaux.
- **EXIGÉ** : Les fichiers de données utiles, les fichiers logiques, les fichiers de clé et les fichiers avec certificat (CVC, X.509) sont archivés exclusivement dans un tel répertoire dédié (DF).
- **EXIGÉ** : L'on veille à ce que les essais pilotes cantonaux n'entravent ni ne compromettent en aucune manière les procédures, applications, fichiers de données utiles et fichiers logiques définis dans la présente norme technique pour la carte d'assuré qui ne sont pas soumis à des essais pilotes.
- **EXIGÉ** : Les assureurs et/ou leurs organisations émettrices n'enregistrent pas et ne gèrent pas administrativement la paire de clés générée lors de l'initialisation et de la personnalisation de la carte d'assuré pour les essais dans le cadre des essais pilotes cantonaux.
- **EXIGÉ** : La paire de clés générée lors de l'initialisation et de la personnalisation de la carte d'assuré pour les essais dans le cadre des essais pilotes cantonaux est soumise exclusivement au cycle de vie défini par les assureurs.
- **EXIGÉ** : Les assureurs ne sont pas responsables de la perte ou des dommages de toute sorte survenus – ou qui pourraient survenir – dans le cadre de l'utilisation de la paire de clés pour les essais dans le cadre des essais pilotes cantonaux.

6 Définition des certificats

EXIGÉ : Toutes les définitions figurant dans le présent chapitre sont respectées.

6.1 Spécification des CVC selon ISO/IEC 7816-8 avec recouvrement des messages selon ISO/IEC 9796-2

Balise	Balise	Balise	Nom	Description	Longueur
'7F21'	CVC				[octets]
	'5F37'	Signature			M
		'6A'	Élément de remplissage	Remplissage conforme à la norme [ISO 9796-2]	
		'5F29'	CPI	Identificateur de profil du certificat	1
		'42'	CAR	Référence de l'autorité de certification	8
		'5F20'	CHR	Référence du détenteur du certificat	16
		'5F4C'	CHA	Autorisation du détenteur du certificat	7
		'06'	OID	Identificateur d'objet := codage OID	8 - 9
		'7F49'	PK_Part1	= 'xx..xx' (MSB \Rightarrow LSB); $N_{1/2}$	$N_{1/2}$
			Hash	'xx..xx' = Hash (20 octets)	20
	'BC'	Label de fin	Signature numérique formée via le bloc de données, délimitée par '6A..'BC'		
	'5F38'	PK_Part2 = 'xx..xx' (MSB \Rightarrow LSB); $N_{2/2}$ PK_exp = '00 01 00 01'; e = 64 bits			$N_{2/2} + e$
	'42'	CAR : Référence de l'autorité de certification			8

Balise de l'élément de données	Longueur
'5F37'	M = 128 octets, [1024 Bit]
'7F49'	$N_{1/2}$ = 64 octets, [512 Bit]
'5F38'	$N_{2/2} + e$ = 72 octets et $N_{2/2}$ = 64 octets [512 Bit]

6.1.1 CVC ['7F21']

Titulaire	CVC ['7F21']
Assuré (certificat de personne)	CVC.PDC
Fournisseur de prestations (certificat de personne)	CVC.HPC
Organisation émettrice des assureurs	CVC.CA_ORG_PDC _m
Organisation émettrice des fournisseurs de prestations	CVC.CA_ORG_HPC _m

6.1.2 Signature ['5F37']

Titulaire	Signature ['5F37']
Assuré : CVC.PDC	Sig(CA_ORG_PDC _m);n= 1024 bits
Fournisseur de prestations : CVC.HPC	Sig(CA_ORG_HPC _m);n= 1024 bits
Organisation émettrice des assureurs : CVC.CA_ORG_PDC _m	Sig(CA_ORG_PDC ₁)*;n= 1024 bits
Organisation émettrice des fournisseurs de prestations : CVC.CA_ORG_HPC _m	Sig(CA_ORG_PDC ₁)*;n= 1024 bits

(*): Premiers CVC-PKI des assureurs mis en service hors ligne

6.1.3 CPI - Identificateur de profil du certificat ['5F29']

L'« identificateur de profil du certificat » (CPI) a pour but d'afficher la structure exacte d'un CVC. On opère ici une distinction entre certificat d'utilisateur ('04') et certificat de SC (certificat d'organisation émettrice) ('03').

CPI - Identificateur de profil du certificat ['5F29']	Codage CPI : ['01'..'7E']
Carte d'assuré : PDC	'04'
Carte de fournisseur de prestations : HPC	'04'
Organisation émettrice des assureurs : CA_ORG_PDC	'03'
Organisation émettrice des fournisseurs de prestations : CA_ORG_HPC	'03'

6.1.4 CAR - Référence de l'autorité de certification (Authority Key Identifier)

Cet élément sert à identifier le service de certification (SC) qui délivre le certificat.

CAR ['42']	Nom du SC [5 octets]		Extension pour le référencement de la clé			
	Pays	Nom	Indicateur du service	Information spécifique au SC	Référence algorithmique	Date de création de la clé SC
Longueur	[2 octets]	[3 octets]	[1 DCB]	[1 DCB]	[2 DCB]	[2 DCB]
PDC	'CH'	NNN	'1'	'0'	'01'	'YY'
HPC	'CH'	NNN	'1'	'1'	'01'	'YY'
CA_ORG_PDC	'CH'	NNN	'6'	'0'	'01'	'YY'
CA_ORG_HPC	'CH'	NNN	'6'	'1'	'01'	'YY'

Pays	Code du pays selon la norme ISO 3166 (2 octets CH = Suisse)
Date de création de la clé du SC	Contient les derniers chiffres de l'année durant laquelle la paire de clés a été générée pour le codage des certificats.
Référence algorithmique	- [01] : SHA1 avec algorithme de signature RSA utilisant les règles de remplissage ISO 9796
Information spécifique au SC	- [0] : Certificat établi par le SC de l'organisation émettrice des assureurs - [1] : Certificat établi par le SC de l'organisation émettrice des fournisseurs de prestations

Indicateur de service	[1 DCB]	Nom : NNN	[3 octets]
Signature numérique	'0'	p. ex. Centre Cada	VKC
Authentification d'entité	'1'	p. ex. FMH	FMH
Codage de clé	'2'	p. ex. Ofac	OFC
Codage de données	'3'	p. ex. Infirmiers	ASI
Accord de chiffrement	'4'	etc.
Authentification d'entité (C)	'5'		
CertSign (sans indication de service)	'6'		
CertSign pour authentification et codage de clé	'7'		
CertSign pour authentification et accord de chiffrement	'8'		

6.1.5 CHR - Référence du détenteur du certificat (Subject Key Identifier)

Cet élément sert à identifier le détenteur du certificat. Sa longueur est de 16 octets.

Certificats d'émetteur :

CHR ['5F20']	Nom du SC [5 octets]			Extension pour référencement de la clé			
	Elément de remplissage	Pays	Nom	Indicateur de service	Information spécifique au SC	Référence algorithmique	Date de création de la clé SC
Longueur	[8 octets]	[2 oct]	[3 oct]	[1 DCB]	[1 DCB]	[2 DCB]	[2 DCB]
CA_ORG_PDC	'00000000'	'CH'	NNN	'6'	'0'	'01'	'YY'
CA_ORG_HPC	'00000000'	'CH'	NNN	'6'	'1'	'01'	'YY'

Cf. ch. 6.1.4 Référence de l'autorité de certification

Certificats d'assuré :

CHR ['5F20']		
	Remplissage	ICCSN
Longueur	[6 octets]	[10 octets]
PDC	'000000'	'xxxxxxxxxx'

Certificats de fournisseurs de prestations, certificats FP :

CHR ['5F20']				
	Numéro ID FP	Détenteur	Séparateur	ICCSN
Longueur	[4 octets] binaire	[2 DCB]	[2 DCB]	10 octets
Titulaire HPC	'.....' B	'00'	'00'	'aaaaaaaaaa'
HPC délégué_1	id. caract. FP	'01'	'00'	'bbbbbbbbbb'
HPC délégué_n	id. caract. FP	'99'	'00'	'zzzzzzzzzz'

6.1.6 CHA - Autorisation du détenteur du certificat

L'« autorisation du détenteur du certificat » (CHA) a pour but de fixer les droits d'accès du détenteur de la carte à des données qui sont mémorisées sur une autre carte.

Carte / Certificat	ID profil CHA	CHA ['5F4C']	Explication
PDC	CHA ₀ = 00	AID(DF.NOT) '00'	Aucun accès aux données
HPC	CHA ₁ = 01	AID(DF.NOT) '01'	Accès aux données d'urgence
HPC	CHA ₂ = 02	AID(DF.NOT) '02'	Accès aux données d'urgence
HPC	CHA ₃ = 03	AID(DF.NOT) '03'	Accès aux données d'urgence
HPC	CHA ₄ = 04	AID(DF.NOT) '04'	Accès aux données d'urgence
HPC	CHA ₅ = 05	AID(DF.NOT) '05'	Accès aux données d'urgence
HPC	CHA ₆ = 06	AID(DF.NOT) '06'	Accès aux données d'urgence
HPC	CHA ₇ = 07	AID(DF.NOT) '07'	Accès aux données d'urgence
HPC	CHA ₈ = 08	AID(DF.NOT) '08'	Accès aux données d'urgence
HPC	CHA ₉ = 09	AID(DF.NOT) '09'	Accès aux données d'urgence
HPC	CHA ₁₀ = 10	AID(DF.NOT) '10'	Accès aux données d'urgence
CA_ORG_PDC	CHA ₀ = 00	AID(DF.NOT) '00'	Aucun accès aux données
CA_ORG_HPC	CHA ₀ = 00	AID(DF.NOT) '00'	Aucun accès aux données

6.1.7 Codage OID

Carte / Certificat	Codage OID ['06'] selon ISO 8825	Numéro OID	Nom de l'OID	Autorité d'enregistrement
PDC	- 2B 0E 03 02 0F -	- 1.3.14.3.2.15 -	- SHA avec algorithme de signature RSA utilisant les règles de remplissage conformes à ISO 9796-2- -	OIW
HPC	- 2B 0E 03 02 0F -	- 1.3.14.3.2.15 -	- SHA avec algorithme de signature RSA utilisant les règles de remplissage conformes à ISO 9796-2 -	OIW
CA_ORG_PDC	- 2B 0E 03 02 0F - 1	- 1.3.14.3.2.15 -	- SHA avec algorithme de signature RSA utilisant les règles de remplissage conformes à ISO 9796-2 -	OIW
CA_ORG_HPC	- 2B 0E 03 02 0F -	- 1.3.14.3.2.15 -	- SHA avec algorithme de signature RSA utilisant les règles de remplissage conformes à ISO 9796-2 -	OIW

Clé publique RSA	
Balise '81'	Module
Balise '82'	Exposant public

6.2 Certificats de serveur conformes à X.509 (RFC 3280) pour le service en ligne

6.2.1 Définition des certificats

Certificats		X509.CA_ORG_PDC _m X509.CA_ORG_HPC _m
Attributs	Valeurs	Remarques
Version	Version 3	
serialNumber	Nombre entier clair	Numéro de série
signature	{1 2 840 113549 1 1 5}	sha1WithRSASignature
issuer	Nom distinctif du fournisseur de services de certification reconnu conformément à la SCSE	p. ex. Swisscom, SwissSign, QuoVadis, OFIT
validity	- à partir du : - jusqu'au :	TUC, ETSI TS 102 280
subject	Nom distinctif de l'organisation émettrice : {DESCRIPTION=carpukcvc, CN=, CN=, OU=, O=, L= , C=}	- OU : organisation émettrice - O : organisation exploitante - OID (description) = {2.5.4.13} - carpukcvc → cf. 6.2.2 p. ex. O=Swisscom, OU=FMH p. ex. O=Veka-C, OU=Veka-C
subjectPublicKeyInfo	- algorithm : 1 2 840 113549 1 1 1 - subjectPublicKey : 1024 bits	rsaEncryption
authorityKeyIdentifier	- keyIdentifier : sha1(subjectPublicKey) - authorityCertIssuer - authorityCertSerialNumber	du fournisseur de services de certification reconnu conformément à la SCSE
subjectKeyIdentifier	sha1 (subjectPublicKey)	Identifie la clé du titulaire
keyUsage	- critical = TRUE - digitalSignature - keyEncipherment	Utilisation de la clé pour l'authentification du serveur pour le service en ligne
certificatePolicies	OID des directives de certification du fournisseur de services de certification reconnu applicable à ce certificat	- Reconnaissance des directives - Information qualifiant les directives
crIDistributionPoints	URL du fournisseur de services de certification reconnu	Point de distribution des listes de blocage par un fournisseur de services de certification reconnu
extKeyUsage	serverAuth : 1 3 6 1 5 5 7 3 1	Authentification du serveur
AuthorityInfoAccess	- accessMethod : id-ad-calssuers - accessLocation : [uRI]	Accès avec autre information du fournisseur de services de certification [http], év.
signatureAlgorithm	- algorithm : 1 2 840 113549 1 1 5 - signature : au moins 2048 octets	sha1WithRSASignature

6.2.2 DESCRIPTION (2.3.4.13) : carpukcvc

Cet attribut descriptif sert à référencier et à identifier les valeurs caractéristiques du CVC-PKI hors ligne de l'organisation émettrice mentionnée dans ce certificat de serveur.

Variable : carpukcvc [40 octets]						Format : DirectoryString{printableString}
CAR- Référence de l'autorité de certification						- PK.CA_ORG_PDC _m - PK.CA_ORG_HPC _m
Pays [2 octets]	Nom [3 octets]	Service [1 BCD]	Info SC [1 BCD]	Réf algo [2 BCD]	Date Clé SC [2 BCD]	Clé publique dans une représentation en code HEX [64 BCD]

6.3 Certificats d'émetteur conformes à X.509 (RFC 3280) [X509.CA_Pub_x]

Ces certificats d'émetteur publics doivent être établis par les fournisseurs de services de certification qui figurent dans la liste des fournisseurs reconnus selon l'art. 5 SCSE au moins selon toutes les normes conformes à la SCSE, l'OSCSE et aux PTA-SCSE. Pour établir ces certificats, les fournisseurs de services de certification doivent utiliser les mêmes procédures techniques et organisationnelles ainsi que la même infrastructure technique ou une structure équivalente que celles servant à l'établissement de certificats qualifiés selon la SCSE.

7 Exclusion de responsabilité – Droits de tiers

Les normes élaborées par l'Association **eCH** et mises gratuitement à la disposition des utilisateurs, ainsi que les normes de tiers adoptées, ont seulement valeur de recommandations. L'Association **eCH** ne peut en aucun cas être tenue pour responsable des décisions ou mesures prises par un utilisateur sur la base des documents qu'elle met à disposition. L'utilisateur est tenu d'étudier attentivement les documents avant de les mettre en application et au besoin de procéder aux consultations appropriées. Les normes **eCH** ne remplacent en aucun cas les consultations techniques, organisationnelles ou juridiques appropriées dans un cas concret.

Les documents, méthodes, normes, procédés ou produits référencés dans les normes **eCH** peuvent le cas échéant être protégés par des dispositions légales sur les marques, les droits d'auteur ou les brevets. L'obtention des autorisations nécessaires auprès des personnes ou organisations détentrices des droits relève de la seule responsabilité de l'utilisateur.

Bien que l'Association **eCH** mette tout en œuvre pour assurer la qualité des normes qu'elle publie, elle ne peut fournir aucune assurance ou garantie quant à l'absence d'erreur, l'actualité, l'exhaustivité et l'exactitude des documents et informations mis à disposition. La teneur des normes **eCH** peut être modifiée à tout moment sans préavis.

Toute responsabilité relative à des dommages que l'utilisateur pourrait subir par suite de l'utilisation des normes **eCH** est exclue dans les limites des réglementations applicables.

8 Droits d'auteur

Tout auteur de normes **eCH** en conserve la propriété intellectuelle. Il s'engage toutefois à mettre gratuitement, et pour autant que ce soit possible, la propriété intellectuelle en question, ou ses droits à une propriété intellectuelle de tiers, à la disposition des groupes de spécialistes respectifs ainsi qu'à l'association **eCH**, pour une utilisation et un développement sans restriction dans le cadre des buts de l'association.

Les normes élaborées par les groupes de spécialistes peuvent, moyennant mention des auteurs **eCH** respectifs, être utilisées, développées et déployées gratuitement et sans restriction.

Les normes **eCH** sont complètement documentées et libres de toute restriction relevant du droit des brevets ou de droits de licence. La documentation correspondante peut être obtenue gratuitement.

Les présentes dispositions s'appliquent exclusivement aux normes élaborées par **eCH**, non aux normes ou produits de tiers auxquels il est fait référence dans les normes **eCH**. Les normes incluront les références appropriées aux droits de tiers.

Annexe A – Glossaire et abréviations

Les expressions spécialisées et les abréviations utilisées dans la norme sont documentées dans les normes référencées et les normes RFC.

Actif	Fichier sur la CA auxquels on peut accéder de l'extérieur
AM	Carte à puce : mode accès
CA	Carte d'assuré
CVC	<i>Card Verifiable certificate</i> , certificat pour l'authentification carte à carte
FP	Fournisseurs de prestations (médicales)
HPC	<i>Health professional Card</i> , carte électronique de fournisseur de prestations
Internal	Fichiers sur la CA auxquels seul le système d'exploitation des cartes a l'accès
n°RCC	Numéro du RCC pour les fournisseurs de prestations qui établissent leurs factures selon la loi sur l'assurance-maladie
PDC	Carte de patient, carte d'assuré
RCC	Registre du code créancier, tenu par santésuisse
RFC	<i>Remote Function call</i>
SC	Carte à puce : <i>Security condition</i>
Structure	Carte à puce : structure du fichier élémentaire
Type	Carte à puce : type de fichier élémentaire

Annexe B – Références et bibliographie

[OCA]	Ordonnance sur la carte d'assuré dans l'assurance obligatoire des soins (RS 832.105)
[ODFI]	Ordonnance du DFI sur les prescriptions techniques et graphiques de la carte d'assuré dans l'assurance obligatoire des soins (RS 832.105.1)
[LPD]	Loi fédérale sur la protection des données (RS 235.1)
[OLPD]	Ordonnance relative à la loi fédérale sur la protection des données (RS 235.11)
[Décision CE N° 190]	Décision N° 190 du 18 juin 2003 de la Commission administrative des Communautés européennes pour la sécurité sociale des travailleurs migrants concernant les caractéristiques techniques de la carte européenne d'assurance maladie
[ISO 8601 : 2004]	Eléments de données et formats d'échange - Echange d'informations - Représentation de la date et de l'heure
[RFC 2119 : 1997]	Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence
[RFC 3280 : 2002]	Infrastructure de clé publique Internet X.509, profil de certificat et de liste de révocation de certificats (CRL)
[RFC 2246 : 1999]	Protocole TLS, version 1.0
[RFC 2616 : 1999]	Protocole de transfert Hypertexte - HTTP/1.1
[RFC 3546 : 2003]	Sécurité de la couche Transport - Extensions (TLS)
[ISO 3166-1 : 2006]	Codes pour la représentation des noms de pays et de leurs subdivisions - Partie 1 : Codes pays
[ISO 7810 : 2003]	Cartes d'identification - Caractéristiques physiques
[ISO 7816-1 : 1998]	Cartes d'identification - Cartes à circuit(s) intégré(s) à contacts - Partie 1 : Caractéristiques physiques
[ISO 7816-2 : 1999]	Cartes d'identification - Cartes à circuit intégré à contacts - Partie 2 : Cartes à contact - Dimensions et emplacements des contacts
[ISO 7816-3 : 2006]	Cartes d'identification - Cartes à circuit intégré - Partie 3 : Cartes à contacts - Interface électrique et protocoles de transmission
[ISO 7816-4 : 2005]	Cartes d'identification - Cartes à circuit intégré - Partie 4 : Organisation, sécurité et commandes pour les échanges

- [ISO 7816-6 : 2004] Cartes d'identification - Cartes à circuit intégré - Partie 6 : Éléments de données intersectoriels pour les échanges
- [ISO 7816-8 : 2004] Cartes d'identification - Cartes à circuit intégré - Partie 8 : Commandes pour des opérations de sécurité
- [ISO 7816-9 : 2004] Cartes d'identification - Cartes à circuit intégré - Partie 9 : Commandes pour la gestion des cartes
- [ISO 8825-1 : 2002][ITU-T : X690 : 2002] Technologies de l'information - Règles de codage ASN.1: Spécification des règles de codage de base (BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER)
- ISO 9796-2 : 2002 Technologies de l'information - Techniques de sécurité - Schémas de signature numérique rétablissant le message - Partie 2 : Mécanismes basés sur une factorisation entière
- ISO 9798-1 : 1997 Technologies de l'information - Techniques de sécurité - Authentification d'entité - Partie 1: Généralités
- ISO 9798-3 : 1998 Technologies de l'information - Techniques de sécurité - Authentification d'entité - Partie 3: Mécanismes utilisant des techniques de signature numériques

Annexe C – Collaboration et rédaction

Hannes Bösch (Arpage SA)
Marc Defalque (Swisscom IT Services)
Marzio Della Santa (CDS)
Martin Denz
Nguyen Don (Telekurs)
Stephan Hänsenberger (H+)
Christian Hausammann (Accarda)
Simon Hölzer (H+)
Siegfried Isele (HP Suisse Sàrl)
Michèle Kathriner (PwC)
Birgit Lang (SUVA)
Hansjörg Looser (SG)
Christian Lovis (HUG)
Andreas Lux (Debold&Lux)
Jérôme Magnin (CdC)
Urs Mathis (Trüb SA)
René Meier (Intercard)
Daniel Muscionico (Ofac)
Beat Nussbaumer (Swisscom)
Rolf Oppliger (USIC)
Bernhard Ostertag (Intercard SA)
Thomas Räber (CSS)
Serge Reichlin (Siemens MED Solutions)
Xavier Rossmanith (OFAS)
Stefano Salvadè (TI)
Rolf Schmidiger (SUVA)
Hans-Peter Schönenberger (santésuisse)
Christoph Schöni (H+)
Burkhard Schwalm (PFPDT)
Pawel Silberring (Celsi SA)
Urs Stromer (La Poste Suisse)
Urs Suter (Siemens)
Michael Vetterli (Signpool)
David Voltz (Ofac)
Judith Wagner (FMH)
Michael Ziegler (H-Net)