



POLITIQUES DE CERTIFICATION DE L'IGC "CPS"

**Autorité de Certification "PROFESSIONNEL - Classe 1"
Certificats de signature et d'authentification**

Statut¹	: Document Final
Version	: 1.01
Date mise à jour	: 13/12/2004
Date prise d'effet	: 13/12/2004
Référence	: GIP-CPS_PC_PROF-CL1
Diffusion²	: Libre

¹ Document de Travail / Document Final

² Libre / Restreinte / Confidentielle



Historique des versions et révisions

Historique des versions et révisions

Version	Nature de la mise à jour	Date
1.00	Version validée par le Comité de Direction du GIP "CPS" du 11/10/2004	04/10/2004
1.01	Précisions concernant les domaines d'utilisation applicables (paragraphe 1.4.1 et 4.5.1) ; validation CODIR de ce jour.	13/12/2004



Sommaire

1.	Introduction	1
1.1	Présentation générale	1
1.2	Identification	4
1.3	Entités intervenant dans l'IGC	5
1.4	Usage des certificats	12
1.5	Gestion de la PC	14
1.6	Définitions et acronymes	15
2.	Responsabilités concernant la mise à disposition des informations devant être publiées	21
2.1	Entités chargées de la mise à disposition des informations	21
2.2	Informations devant être publiées	21
2.3	Délais et fréquences de publication	22
2.4	Contrôle d'accès aux informations publiées	22
3.	Identification et authentification	23
3.1	Nommage	23
3.2	Validation initiale de l'identité	24



Sommaire

3.3	Identification et validation d'une demande de renouvellement des clés	25
3.4	Identification et validation d'une demande de révocation	26
4.	Exigences opérationnelles sur le cycle de vie des certificats	27
4.1	Demande de certificat	27
4.2	Traitement d'une demande de certificat	27
4.3	Délivrance du certificat	28
4.4	Acceptation du certificat	28
4.5	Usages du bi-clés et du certificat	29
4.6	Renouvellement d'un certificat	30
4.7	Délivrance d'un nouveau certificat suite à changement du bi-clé	30
4.8	Modification du certificat	31
4.9	Révocation et suspension des certificats	32
4.10	Service d'état des certificats	35
4.11	Expiration de l'abonnement des porteurs	36
4.12	Séquestre de clé et recouvrement	36
5.	Mesures de sécurité non techniques	37
5.1	Mesures de sécurité physiques	37
5.2	Mesures de sécurité procédurales	37
5.3	Mesures de sécurité vis-à-vis du personnel	38
5.4	Procédures de constitution des données d'audit	39



Sommaire

5.5	Archivage des données	41
5.6	Changement de clé d'AC	42
5.7	Reprise suite à compromission et sinistre	42
5.8	Fin de vie de l'IGC	43
6.	Mesures de sécurité techniques	45
6.1	Génération et installation de bi clés	45
6.2	Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques	46
6.3	Autres aspects de la gestion des bi-clés	48
6.4	Données d'activation	48
6.5	Mesures de sécurité des systèmes informatiques	49
6.6	Mesures de sécurité des systèmes durant leur cycle de vie	49
6.7	Mesures de sécurité réseau	50
6.8	Horodatage	50
7.	Profils des certificats, OSCP et des LCR	51
7.1	Profil des certificats	51
7.2	Profil des LCR	52
7.3	Profil OSCP	52
8.	Audit de conformité et autres évaluations	53
8.1	Fréquences et / ou circonstances des évaluations	53



Sommaire

8.2	Identités / qualifications des évaluateurs	53
8.3	Relations entre évaluateurs et entités évaluées	53
8.4	Sujets couverts par les évaluations	53
8.5	Actions prises suite aux conclusions des évaluations	53
8.6	Communication des résultats	54
9.	Autres problématiques métiers et légales	55
9.1	Tarifs	55
9.2	Responsabilité financière	55
9.3	Confidentialité des données professionnelles	56
9.4	Protection des données personnelles	57
9.5	Droits sur la propriété intellectuelle et industrielle	58
9.6	Interprétations contractuelles et garanties	59
9.7	Limite de garantie	60
9.8	Limite de responsabilité	60
9.9	Indemnités	61
9.10	Durée et fin anticipée de validité de la PC	61
9.11	Notifications individuelles et communications entre les participants	62
9.12	Amendements à la PC	62
9.13	Dispositions concernant la résolution de conflits	63
9.14	Juridictions compétentes	64



**POLITIQUES DE CERTIFICATION
DE L'IGC "CPS"**
Autorité de Certification "PROFESSIONNEL - Classe 1"
Certificats de signature et d'authentification

Diffusion Libre
Version 1.01 du
13/12/2004

Sommaire

9.15	Conformité aux législations et réglementations	64
9.16	Dispositions diverses	64
9.17	Autres dispositions	65
Annexe 1 - Documents de référence		66
1.	Documents de nature juridique	66
2.	Documents de nature technique	67
3.	Documents internes GIP "CPS"	68



1. Introduction

1.1 Présentation générale

Ce document constitue les Politiques de Certification (PC) de l'Autorité de Certification Intermédiaire (ACI) "Classe 1", rattachée à l'Autorité de Certification Racine (ACR) "Professionnel" de l'Infrastructure de Gestion de Clés du GIP "CPS" (IGC "CPS"), pour les certificats de signature et d'authentification de cette classe (cf. § 1.3.1 ci-dessous).

Sa structure est conforme au document [RFC3647].

1.1.1 Le Groupement d'intérêt Public "Carte de Professionnel de Santé"

Le rôle et les missions dévolus au GIP "CPS" sont définis par un certain nombre de textes réglementaires, notamment :

Art. 2 de la Convention constitutive du Groupement d'Intérêt public "Carte de Professionnel de Santé" : Arrêté du 28 janvier 1993 modifié par l'Assemblée Générale du 17 décembre 1998.

« Le groupement d'intérêt public "Carte de professionnel de Santé" a pour objet de créer les conditions garantissant l'indépendance et la responsabilité des différents acteurs du secteur sanitaire et social dans l'utilisation des cartes électroniques.

Pour ce faire, il assurera (...) l'émission, la gestion et la promotion d'une carte de professionnel de santé, d'une carte de professionnel de santé en formation et d'une carte de personnel d'établissement destinée au personnel non professionnel de santé des établissements sanitaires et sociaux ou aux personnes qualifiées ayant une activité dans le secteur sanitaire et social et ne relevant pas des critères d'attribution de la CPS (...).

« Professionnel de santé » s'entend au sens des catégories réglementées par le code de la santé publique, c'est à dire les professions médicales (médecins, chirurgiens-dentistes, sages-femmes), les pharmaciens et les auxiliaires médicaux (professions paramédicales) (...)

Art. R. 161-54 de [Décret 98-271].

« Le groupement d'intérêt public « Carte de Professionnel de Santé » émet, délivre et gère les cartes de professionnel de santé. Il veille à leur bon usage et assure la fiabilité des mécanismes et la protection des clés sur lesquelles reposent la confidentialité des données chiffrées et la validité des signatures électroniques produites à l'aide de ces cartes. »

Art. R.161-58 de [Décret 98-271].



Introduction

« Pour les applications télématiques et informatiques du secteur de la santé, la signature électronique produite par la carte de professionnel de santé est reconnue par les administrations de l'Etat et les organismes de sécurité sociale comme garantissant l'identité et la qualité du titulaire de la carte ainsi que l'intégrité du document signé. Ainsi signés, les documents électroniques mentionnés à l'article L.161-33 sont opposables à leur signataire. »

1.1.2 Objectifs et domaine d'application de la présente Politique de Certification

L'objectif de ce document est de définir les engagements du GIP "CPS", via son IGC "CPS", dans la délivrance et la gestion des certificats de signature et des certificats d'authentification de classe 1 des cartes CPS tout au long de leur cycle de vie.

La documentation liée à une IGC peut se décomposer en trois niveaux :

- Le niveau "**politique / objectifs / engagements**", qui correspond aux objectifs que l'IGC se fixe en interne et vis-à-vis de l'extérieur en matière de niveaux de sécurité, de qualité de service, de performance, etc., liés à la gestion des clés et des certificats. Ce niveau est extrêmement stable dans le temps. Une fois les objectifs et les engagements posés, ils ne sont revus qu'en cas d'évolution importante des choix politiques du GIP "CPS".
- Le niveau "**stratégie**", qui identifie les moyens à mettre en œuvre, en termes de ressources humaines, d'organisation, de procédures, de matériels / logiciels, pour atteindre les objectifs fixés. Ce niveau est relativement stable mais doit être revu en cas d'évolution dans les moyens nécessitée par une évolution des risques ou des changements importants d'organisation (changement de locaux, évolution vers une nouvelle génération de matériel, etc.).
- Le niveau "**mise en œuvre opérationnelle**", qui est la déclinaison opérationnelle de la stratégie qui a été définie, au travers de la spécification des procédures opérationnelles, des contrats de fourniture de matériel, logiciels et services, des contrats de travail, etc. Ce niveau évolue en permanence en fonction de l'activité du GIP "CPS" (mise à niveau d'une procédure suite à un incident, modification des paramètres d'un système, etc.).

Les objectifs et les engagements du GIP "CPS" concernant les différents aspects du cycle de vie des certificats gérés par l'IGC sont regroupés dans les politiques de certification. Les présentes PC ne porte que sur les certificats de signature et d'authentification de classe 1 des cartes CPS à partir de la génération "CPS2ter" ; elle ne concerne pas les cartes de générations antérieures.



Introduction

Les autres types de certificats gérés par le GIP "CPS" font l'objet de politiques de certification distinctes. Ces politiques constituent le fondement des relations de l'IGC avec l'extérieur : utilisateurs (porteurs de certificats et accepteurs de certificats), mais également partenaires (autres IGC que le GIP "CPS" souhaite reconnaître et desquelles il souhaite être reconnu), autorités publiques et organismes privés d'évaluation et de reconnaissance (qualification, labellisation WebTrust, etc.).

Cependant, compte tenu de la complexité des éléments à la fois techniques et juridiques contenus dans une politique de certification, notamment pour des utilisateurs non-spécialistes, ces politiques sont traduites dans des documents spécifiques à destination des utilisateurs que sont les protocoles d'usage de la CPS qui sont joints aux formulaires d'abonnement et disponibles sur le site Web du GIP "CPS" (cf. [PUC_CPS]). Ces protocoles correspondent aux PKI Disclosure Statement décrit dans [RFC3647] et [TS102042].

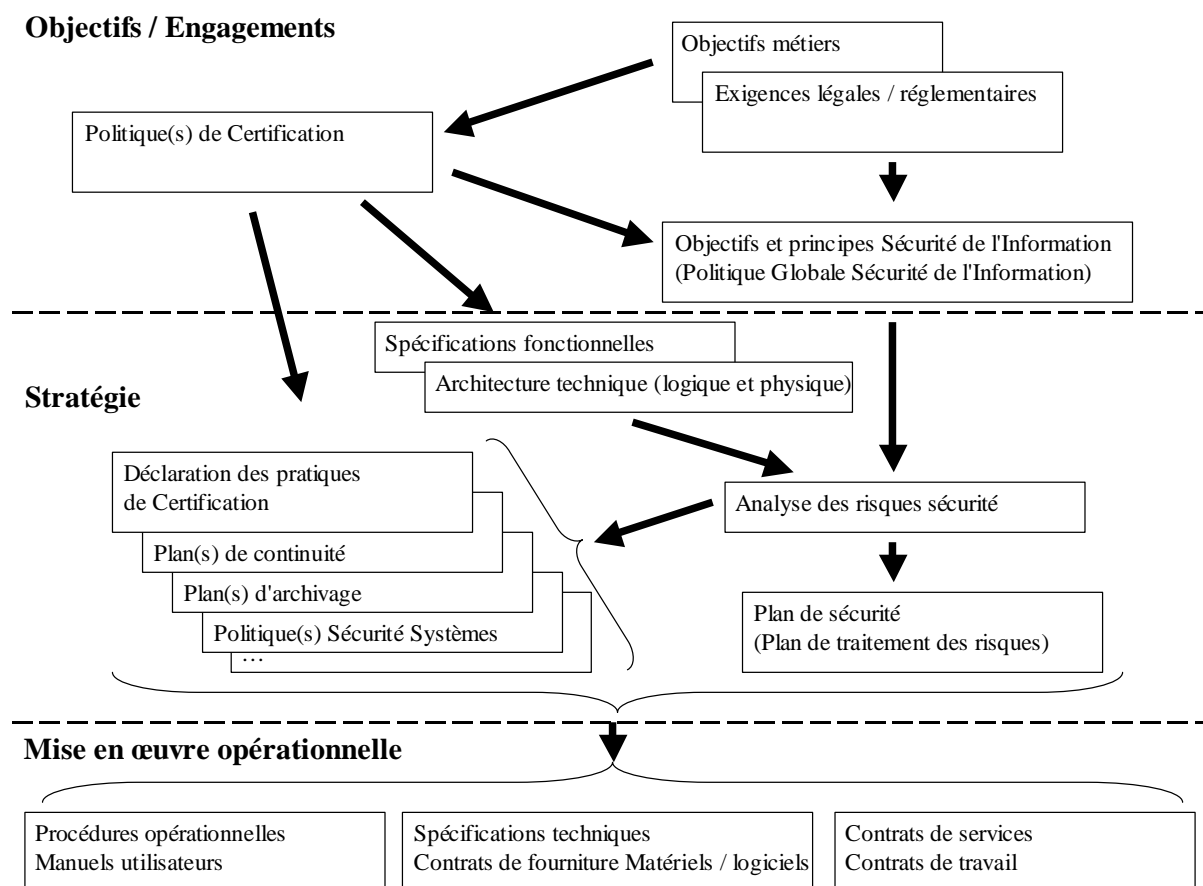
Les engagements arrêtés dans les présentes PC correspondent :

- aux exigences imposées au GIP "CPS" par la réglementation et par ses membres ;
- aux objectifs que se fixe le GIP "CPS" en matière de services, de sécurité, de qualité et de performances afin de satisfaire les utilisateurs (porteurs et accepteurs) de ses certificats et d'être reconnu, si nécessaire, par les différents schémas d'évaluation / référencement en matière d'IGC.

La figure ci-dessous présente de manière schématique les 3 niveaux de documentation :



Introduction



Les présentes PC, comme les autres PC du GIP "CPS", sont des documents publics. Les autres documents qui découlent de ces PC sont des documents internes au GIP "CPS" qui peuvent être accessibles, si besoin, moyennant un accord de confidentialité (auditeurs externes, organismes de qualification, autorités publiques, etc.).

1.2 Identification

Compte tenu de la très grande similarité entre les certificats de signature et les certificats d'authentification de l'ACI "Professionnel - Classe 1" de l'IGC "CPS", le présent document rassemble les deux PC correspondant à chacun de ces deux types de certificats.

Pour chacune de ces types de certificats, le tableau ci-dessous présente le nom de la PC, sa référence et l'identifiant d'objet (OID) correspondant.



Introduction

	ACI PROFESSIONNEL CLASSE 1 Signature	ACI PROFESSIONNEL CLASSE 1 Authentification
Nom	Politique de Certification de l'Autorité de Certification "Professionnel Classe1" Signature	Politique de Certification de l'Autorité de Certification "Professionnel Classe1" Authentification
OID	{iso(1) member-body(2) france(250) type-org(1) gip-cps(71) icp(3) doc(7) PC2004-Exploit(8) PC-Professionnel(1) CLASSE-1(1) Signature(2) Version-PC(1)}	{iso(1) member-body(2) france(250) type-org(1) gip-cps(71) icp(3) doc(7) PC2004-Exploit(8) PC-Professionnel(1) CLASSE-1(1) Authentification(1) Version-PC(1)}

Les exigences et les engagements définis dans le présent document s'appliquent à ces deux types de certificats, sauf mention explicite contraire. Dans le cas où un paragraphe ne s'applique qu'à un type de certificat, il est précédé du type entre crochets (par exemple [SIGNATURE] désigne un paragraphe ne s'appliquant qu'aux certificats de type signature).

1.3 Entités intervenant dans l'IGC

1.3.1 Autorités de certification

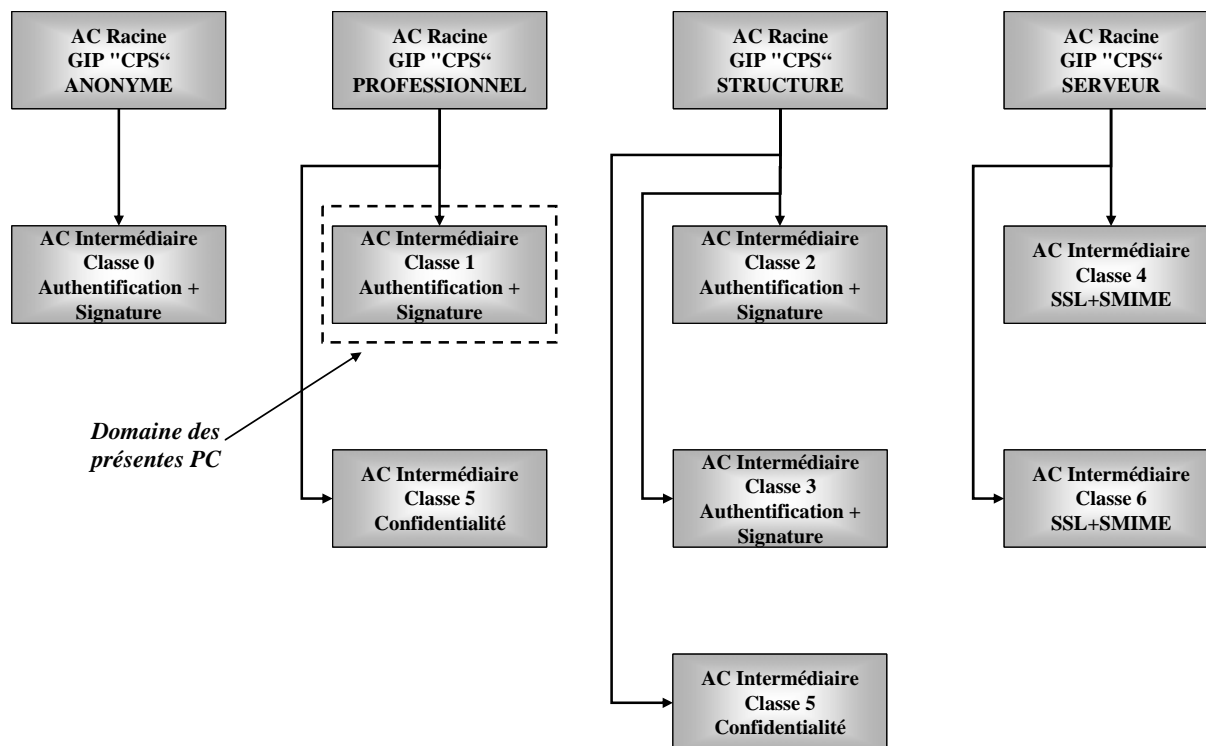
Le GIP "CPS" est prestataire de services de certification (PSC) pour le secteur santé-social, au sens de [DIR_SIGN] et [DEC_SIGN]. A ce titre, il est donc responsable, vis-à-vis de toutes entités externes à l'IGC "CPS" (utilisateurs finaux, autorités publiques, etc.), des différentes Autorités de Certification qui composent l'IGC "CPS".

L'IGC "CPS" est en effet constituée d'une hiérarchie de 3 niveaux de certificats : AC Racines / AC intermédiaires / porteurs de certificats (cf. [CERT_CPS]).

Au niveau des porteurs, les présentes PC couvrent les certificats de signature et les certificats d'authentification de classe 1 rattachés à l'ACI "Professionnel Classe 1" de l'IGC "CPS", elle-même rattachée à l'ACR "Professionnel" (cf. schéma ci-dessous).



Introduction



L'ACI "Professionnel Classe 1", à laquelle les présents certificats sont rattachés, répond aux exigences et engagements de la PC de l'ACR "Professionnel" (cf. [PC_ACR-PRO])

Afin d'assurer sa mission de gestion des certificats et des cartes CPS, l'IGC "CPS" est constituée de différents services fonctionnels (cf. [TS102042] et [TS101456]). Le terme "service" tel qu'utilisé ici correspond bien à la notion de service fonctionnel et non pas de service au sens d'un département dans une structure. Dans la pratique, la mise en œuvre opérationnelle d'un service fonctionnel est effectuée par un ou plusieurs opérateur(s) technique(s), internes et/ou externes au GIP "CPS".

Ces services peuvent différer suivant qu'il s'agit de la gestion des certificats des porteurs (utilisateurs finals) ou des certificats d'AC. Le tableau ci-dessous présente les services fonctionnels intervenant dans la gestion des certificats porteurs de classe 1, objet du présent document.

Service	Définition / Commentaires
Service d'enregistrement	Après avoir effectué les vérifications étant de son ressort sur les informations du futur porteur de carte CPS (cf. chapitre 1.3.2 ci-dessous), ce service formate et transmet les demandes de génération de cartes CPS au service de fourniture des cartes CPS.



**POLITIQUES DE CERTIFICATION
DE L'IGC "CPS"**
Autorité de Certification "PROFESSIONNEL - Classe 1"
Certificats de signature et d'authentification

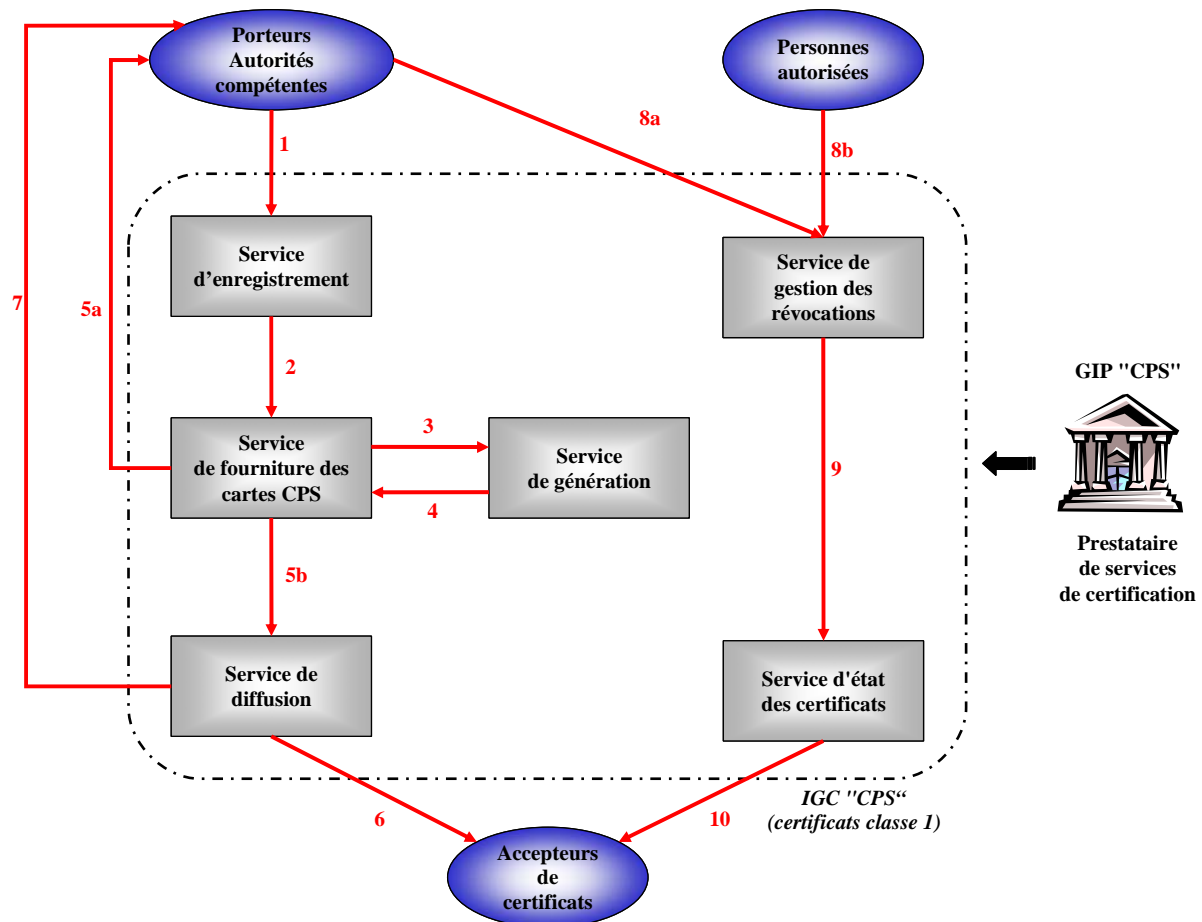
Diffusion Libre
Version 1.01 du
13/12/2004

Introduction

Service	Définition / Commentaires
Service de fourniture des cartes CPS	Ce service personnalise les cartes CPS à partir des demandes transmises par le service d'enregistrement en s'appuyant sur le service de génération pour la fourniture des bi-clés et des certificats correspondants. Les cartes CPS étant spécifiques au GIP "CPS", en amont de la personnalisation, ce service comprend également la fabrication des composants et l'encartage de ces cartes.
Service de génération des clés et des certificats	Ce service génère les bi-clés des porteurs et les certificats correspondant (création du format, signature électronique avec la clé privée de l'AC), à partir des informations transmises par le service de fourniture des cartes CPS.
Service de diffusion	Ce service met à disposition : <ul style="list-style-type: none">- des accepteurs de certificats, les certificats produits,- de l'ensemble des utilisateurs (porteurs et accepteurs de certificats), les informations d'accès et d'utilisation des certificats et des cartes CPS (politiques de certification, charte d'accès à l'annuaire, etc).
Service de gestion des révocations	Ce service traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via le service d'état des certificats.
Service d'état des certificats	Ce service fournit aux utilisateurs de certificats des informations sur l'état des certificats (valides ou révoqués).

A titre d'illustration, les principaux flux génériques entre les différents services sont indiqués dans le schéma ci-dessous :

Introduction



- (1) L'Autorité Compétente présente au service d'enregistrement l'ensemble des éléments requis qui les vérifie.
- (2) Le service d'enregistrement met en forme la demande de fourniture de la carte CPS puis la transmet au service de fourniture des cartes CPS.
- (3) Le service de fourniture demande au service de génération de lui fournir les bi-clés et les certificats correspondants de la carte CPS à personnaliser.
- (4) Le service de fourniture personnalise la carte CPS à partir des informations transmises par le service d'enregistrement et des éléments cryptographiques retournés par le service de génération.
- (5) Une fois la carte personnalisée, elle est transmise à son porteur (5a), ainsi que les codes d'activation, et les certificats correspondants sont transmis au service de diffusion (5b).
- (6) Le service de diffusion met les certificats à disposition des accepteurs de certificats via un annuaire.



Introduction

- (7) Ce service met également à disposition de tous les utilisateurs (porteurs et accepteurs) les différents engagements du GIP "CPS" et les différentes conditions et restrictions d'usages.
- (8) Les demandes de révocation sont transmises au service de gestion des révocations par une entité autorisée (Autorité Compétente / porteur (8a) ou autre entité autorisée (8b)).
- (9) Après traitement de la demande, le service de gestion des révocations modifie le statut du certificat correspondant et transmet l'information au service d'état des certificats.
- (10) Le service d'état des certificats fournit aux accepteurs de certificats les informations concernant l'état des certificats via des listes de certificats révoqués.

Pour assurer les fonctions opérationnelles correspondant à ces différents services fonctionnels, le GIP "CPS" s'organise de la façon qui lui convient le mieux :

- en prenant directement en charge une partie de ces fonctions ;
- en sous-traitant l'autre partie, sous son contrôle et sous sa responsabilité, à un ou plusieurs Opérateur(s) Techniques.

La Déclaration des Pratiques de Certification (DPC), qui répond aux exigences des présentes PC, décrit l'organisation opérationnelle de l'IGC "CPS" et la répartition des rôles entre les différentes entités qui la composent.

Dans le cadre de ses fonctions opérationnelles, qu'il assume directement ou qu'il sous-traite à des Opérateurs Techniques, le GIP "CPS" :

- génère, et renouvelle lorsque nécessaire, les bi-clés et les certificats associés de signature et d'authentification des porteurs de cartes CPS, les insère dans les cartes CPS correspondantes en s'assurant de ne conserver aucune copie des clés privées, remet de manière sécurisée chaque carte CPS et les codes d'activation correspondant à son porteur légitime, diffuse les certificats des porteurs aux utilisateurs ;
- met en œuvre les différents services identifiés ci-dessus, notamment en matière de diffusion, de gestion des révocations et d'information sur l'état des certificats ;
- met en œuvre tout ce qui est en son pouvoir pour respecter les engagements définis dans les présentes PC, notamment en terme de fiabilité, de qualité et de sécurité ;

1.3.2 Service d'enregistrement

Le [RFC3647] utilise le terme Autorité d'Enregistrement, alors que les documents [TS102042] et [TS101456] utilisent le terme Service d'Enregistrement. Dans les présentes



Introduction

PC, il est préféré l'utilisation de ce dernier terme afin de réserver la notion d'autorité aux Autorités de Certification et aux Autorités Compétentes.

Pour les certificats de classe 1, objet des présentes PC, le processus d'enregistrement se fait via une ou plusieurs Autorités Compétentes (cf. chapitre 1.3.5.2 ci-après).

Le futur porteur de certificats CPS classe 1 remet son dossier de demande d'enregistrement (formulaire de demande + pièces justificatives) à l'Autorité Compétente correspondant à sa profession.

Ce dossier est traité par cette Autorité Compétente ainsi que, selon les cas, par une ou plusieurs autres Autorités Compétentes. Chaque Autorité Compétente a en charge la vérification et la validation des parties de ce dossier d'enregistrement qui sont de son ressort.

La dernière Autorité Compétente intervenant dans la validation du dossier transmet la demande au service d'enregistrement de l'IGC "CPS". Le service d'enregistrement s'assure alors de l'origine (présence des visas nécessaires en fonction du secteur d'activité du porteur), de l'intégrité et de la cohérence des données reçues, puis lance le processus de génération des certificats et de la carte correspondante auprès du service de fourniture des cartes CPS.

Le processus de vérification et de validation du dossier de demande par les différentes Autorités Compétentes permet de garantir l'identité du futur porteur et son habilitation à être titulaire de certificats de signature et d'authentification de classe 1 (cf. chapitre 1.3.3 ci-après). Ce processus comporte soit un face-à-face direct avec le futur porteur, soit une méthode apportant un niveau de garantie équivalent, en s'appuyant notamment sur des données préalablement validées par les Autorités Administratives adéquates.

Le site Web du GIP "CPS" (www.gip-cps.fr) précise aux demandeurs la démarche à suivre.

1.3.3 Porteurs de cartes CPS

Les certificats de Classe 1 "Professionnel de Santé" sont associés aux cartes dont les porteurs sont les Professionnels de Santé (PS) (diplômés ou en formation) appartenant à une profession réglementée par le code de la Santé Publique. Les porteurs PS peuvent exercer à titre libéral, salarié ou être responsable légal d'une structure. La délivrance de tels certificats engage une responsabilité juridique de nature pénale du demandeur, et requiert des vérifications par les Autorités Compétentes.

Le tableau ci-dessous présente la correspondance entre cette classe et les types de carte CPS concernés, ainsi que les principales populations concernées.



Introduction

CLASSE DE CERTIFICAT	TYPE DE CARTE	QUALITE / FONCTION
CLASSE 1	CPS	Professionnels de santé en exercice, régis par le code de la santé public, appartenant à un Ordre
		Professionnels de santé en exercice, régis par le code de la santé public, n'appartenant pas à un Ordre
	CPF	Professionnels de santé en formation

Le GIP "CPS" émet également d'autres types de cartes ("CPE", "CPA", "CDE") correspondant à d'autres classes de certificats. Mais seules les cartes de types "CPS" ou "CPF" peuvent comporter des certificats de classe 1. Par extension, et sauf mention explicite contraire, lorsque le terme "carte CPS" est utilisé dans le présent document, il recouvre de manière générique les deux types "CPS" et "CPF".

Un porteur d'un certificat de classe 1, et de la carte CPS correspondante, qui est de plus responsable légal d'une structure est Mandataire de Certification pour cette structure. Il peut demander, sous sa responsabilité, l'attribution de certificats de classe 3 pour les employés de sa structure. Il peut également désigner un ou plusieurs Mandataires de Certification Délégués, qui seront eux-mêmes porteurs de certificats de classe 3 et qui disposeront des habilitations adéquates pour demander / révoquer des certificats de classe 3 pour d'autres employés de leur structure.

1.3.4 Accepteurs de certificats

Les accepteurs de certificats CPS sont les personnes et les entités qui sont amenées à s'appuyer sur un certificat CPS pour authentifier un porteur d'une carte CPS ou vérifier une signature électronique générée à l'aide d'une carte CPS.

Un accepteur de certificats peut être lui-même porteur d'une carte CPS (cas, par exemple, d'échange d'un message électronique signé entre deux PS) ou ne pas être porteur d'une telle carte et même être totalement en dehors du domaine de la santé (cas, par exemple, de l'utilisation des cartes CPS dans des téléprocédures administratives, où l'accepteur de certificats est l'administration concernée).

L'accepteur d'un certificat de l'IGC "CPS" lié à une carte CPS peut connaître sa classe en affichant le contenu du certificat et en contrôlant le champ *Emetteur (Issuer)*. Pour les certificats objet des présentes PC (classe 1), ce champ est le suivant :

C=FR, O=GIP-CPS, OU=GIP-CPS PROFESSIONNEL, CN=GIP-CPS CLASSE-1



1.3.5 Autres participants

1.3.5.1 Autres services de l'IGC

Les différents services fonctionnels composants l'IGC "CPS" sont présentés au chapitre 1.3.1 ci-dessus.

1.3.5.2 Autorités Compétentes

Les Autorités Compétentes sont des entités externes à l'IGC "CPS" qui interviennent dans le processus d'enregistrement des porteurs et dans le processus de gestion des révocations.

Pour les certificats de classe 1, elles sont notamment responsables de la vérification de l'identité du porteur du certificat et de ses qualités.

Les Autorités Compétentes, dans le cadre des présentes PC, sont soit directement des Autorités Administratives, soit des entités dont le fonctionnement est réglementé par les Autorités Administratives.

Il s'agit notamment :

- des Ordres (médecins, pharmaciens, etc. ;
- des Directions Départementales / Régionales des Affaires Sanitaires et Sociales (DDASS / DRASS) ;
- du Service de Santé des Armées ;
- de la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés (CNAM-TS).

Les Autorités Compétentes disposent d'une organisation, de procédures et de moyens de contrôle qui découlent des réglementations qui leur sont applicables et qui garantissent la fiabilité des opérations dont elles ont la charge. Notamment, dans leur rôle de vérification des dossiers de demandes d'enregistrement, elles ont accès aux informations administratives adéquates pour répondre aux exigences des présentes PC.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

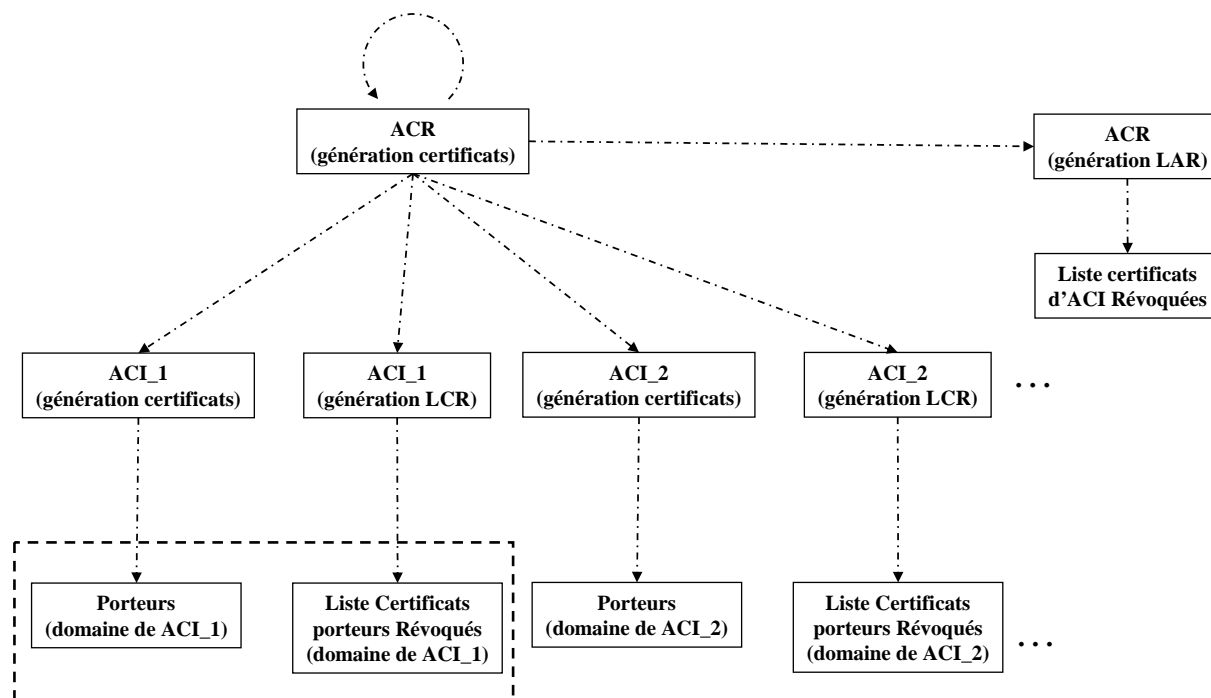
Les présentes PC couvrent les certificats suivants (cf. [CERT_CPS]) :



Introduction

les certificats de porteurs de classe 1, certificats qui se décomposent en deux types : un certificat à fins de signature et un certificat à fins d'authentification (certificats signés par l'ACI "Professionnel Classe 1").

Le schéma ci-dessous présente le positionnement des différents certificats et LCR de l'IGC "CPS" et ceux concernés par les présentes PC :



*Eléments couverts
par la présente PC*

A **B** = Certificat ou liste B signé par A

Dans la suite du présent document, ces différents certificats et les bi-clés correspondants sont regroupés sous la dénomination "bi-clés et certificats de classe 1".

Les certificats porteurs émis en vertu des présentes politiques sont appropriés pour établir le lien entre l'identité d'un porteur et une clé publique pour les applications suivantes, dans un cadre strictement limité aux activités professionnelles non-commerciales³ du porteur du domaine santé-social :

³ A titre d'illustration, les cartes CPS, les bi-clés et les certificats correspondants, peuvent être utilisés pour la sécurisation de télédéclarations administratives professionnelles, moyennant la reconnaissance de ces certificats par les administrations visées.



Introduction

- [SIGNATURE] : la carte comporte un bi-clé et un certificat dits "**de signature**" qui permettent au porteur d'apposer sa signature sur des données électroniques ; cette signature électronique permet de garantir, outre l'authenticité et l'intégrité de documents électroniques ainsi signés, le consentement du signataire quant au contenu de ces documents ; la clé privée correspondante a une longueur de 2048 bits ;
- [AUTHENTIFICATION] : la carte comporte un bi-clé et un certificat dits "**d'authentification**" permettant d'assurer l'authentification du porteur et, éventuellement, de garantir l'origine et l'intégrité de données transmises par celui-ci dans le cadre d'échanges dématérialisés (télé-procédure notamment) ; toutefois, cette authentification ne constitue pas une signature au sens juridique du terme (cf. paragraphe précédent), car elle ne signifie pas que le porteur manifeste son consentement sur les données échangées (la garantie de non répudiation n'est donc pas offerte) ; de plus, la clé privée utilisée ici est limitée à 1024 bits.

Les classes n'ont aucune implication directe sur les niveaux d'habilitation pouvant être mis en œuvre par les applications et au sein de chaque entité. Ces habilitations peuvent être basées sur les niveaux de confiance à accorder aux certificats mais ne sont pas placées sous la responsabilité du GIP "CPS".

1.4.2 Domaines d'utilisation interdits

Toute utilisation d'un certificat de classe 1 autre que celles prévues dans le cadre des présentes PC et du protocole d'usage de la carte (cf. [PUC_CPS]), notamment dans un cadre commercial (signature de contrats commerciaux, paiement), est interdite. En cas de non respect de cette interdiction, la responsabilité du GIP "CPS" ne saurait être engagée (cf. chapitre 9.8 ci-dessous).

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

Le GIP "CPS", en tant que prestataire de services de certification, est responsable de la gestion des présentes PC.

Le processus d'évolution et d'amendements aux présentes PC est précisé au chapitre 9.12 ci-dessous.



1.5.2 Point de contact

La personne à contacter concernant les présentes PC est le Responsable Sécurité des Systèmes d'Information (RSSI) du GIP "CPS" :

Groupement d'Intérêt Public
Carte de Professionnel de Santé
8 bis, rue de Châteaudun 75009 Paris
Tél. : 01.44.53.36.53
Fax : 01.40.16.90.15
e-mail : gip@gip-cps.fr

1.5.3 Entité déterminant la conformité d'une DPC avec cette PC

La détermination qu'une DPC répond ou non aux exigences des présentes PC est prononcée par le Comité de Direction du GIP "CPS".

1.5.4 Procédures d'approbation de la conformité de la DPC

La procédure d'approbation de la conformité d'une DPC est identifiée dans la DPC concernée.

1.6 Définitions et acronymes

Les acronymes utilisés dans les présentes PC sont les suivants :

AC	Autorité de Certification
CC	Critères Communs
CDE	Carte de Directeur d'Etablissement
CISSI	Commission Interministérielle pour la SSI
CODIR	Comité de Direction du GIP "CPS"
CPA	Carte de Personnel Administratif
CPE	Carte de Personnel d'Etablissement
CPF	Carte de Professionnel en Formation
CPS	Carte de Professionnel de Santé
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DDASS	Direction Départementale à l'Action Sanitaire et Sociale
DHOS	Direction de l'Hospitalisation et de l'Organisation des Soins
DPC	Déclaration des Pratiques de Certification
DRASS	Direction Régionale à l'Action Sanitaire et Sociale
GIP "CPS"	Groupement d'Intérêt Public "Carte de Professionnel de Santé"
IGC	Infrastructure de Gestion de Clés.



**POLITIQUES DE CERTIFICATION
DE L'IGC "CPS"**
Autorité de Certification "PROFESSIONNEL - Classe 1"
Certificats de signature et d'authentification

Diffusion Libre
Version 1.01 du
13/12/2004

Introduction

LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
MES	Ministère en charge des affaires sociales et de la santé
OID	Object Identifier
PC	Politique de Certification
PP	Profil de Protection
PS	Professionnel de Santé
PSC	Prestataire de Services de Certification électronique
RSA	Rivest Shamir Adelman
URL	Unique Resource Locator

Les termes utilisés dans les présentes PC sont les suivants :

Accepteur : toute entité (personne physique, personne morale ou application informatique) acceptant un certificat qui lui est soumis et qui doit en vérifier l'authenticité et la validité.

Administrateur : un administrateur met en œuvre les Politiques de Certification et Déclarations des Pratiques de Certification au sein de la composante qu'il administre. Il est responsable de l'ensemble des services rendus par cette composante.

Autorité de Certification (AC) : composante de l'IGC qui dispose d'une plate-forme lui permettant de générer et émettre des certificats en lesquels une communauté d'utilisateurs a confiance [PC2].

Autorité de Certification intermédiaire : à chaque classe de certificats porteur correspond une AC intermédiaire dont le certificat est signé par la clé privée de l'AC racine de l'IGC "CPS".

Autorité de Certification racine : AC prise comme référence par une communauté d'utilisateurs (incluant d'autres AC). Elle est un élément essentiel de la confiance qui peut lui être accordée dans un contexte donné [PC2].

Autorité Compétente : Pour certaines classes de certificats et certains types de cartes, les Autorités Compétentes sont chargées de vérifier et de garantir l'identité et la qualité des demandeurs de cartes qui contiennent les certificats. Elles ne font pas partie de l'IGC "CPS".

Bi-clé : couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptologie basée sur des algorithmes asymétriques. Trois types de bi-clés interviennent dans



Introduction

l'infrastructure de gestion de clés CPS décrite dans la présente Politique de Certification :

- les bi-clés d'AC racine et intermédiaires, dont la clé privée est utilisée par l'AC correspondante à des fins de signature de certificat ou de signature d'informations de révocation de ces certificats et la clé publique à des fins de vérification de ces mêmes informations ;
- les bi-clés de signature des porteurs, dont la clé privée est utilisée à des fins de signature et la clé publique à des fins de vérification ;
- les bi-clés d'authentification des porteurs, servant à l'établissement de sessions sécurisées entre le porteur et une autre entité (serveur Web, application informatique, etc.).

Boîtier de sécurité : boîtier cryptographique sécurisé, dans lequel a lieu la génération des clés.

Certificat : ensemble d'informations, dont la clé publique, d'un utilisateur rendu infalsifiable par le chiffrement, avec la clé secrète de l'AC qui l'a délivré, d'un condensat calculé sur l'ensemble de ces informations. Un certificat contient des informations telles que :

- l'identité du porteur de certificat ;
- la clé publique du porteur de certificat ;
- la durée de vie du certificat ;
- l'identité de l'AC qui l'a émis ;
- la signature de l'AC qui l'a émis.

Un format standard de certificat est défini dans la recommandation X.509 v3.

Composante de l'IGC : plate-forme constituée d'au moins un poste informatique, une application, un support réseau et jouant un rôle déterminé au sein de l'IGC. Une composante peut être une AC, une AE, une Autorité d'Horodatage, une Tierce Partie de Confiance, etc.

Contrôle de conformité : action qui consiste à réaliser un examen le plus exhaustif possible afin de vérifier l'application stricte des procédures et de la réglementation au sein d'un organisme.

Déclaration relative aux Pratiques de Certification (DPC) : énoncé des procédures et pratiques effectivement respectées par une IGC pour la gestion des certificats qu'elle émet.

DeltaLCR : LCR particulière ne contenant que les changements intervenus depuis la publication de la dernière LCR complète dont le numéro est indiqué.



Introduction

Domaine de certification : chemin constitué d'une chaîne de certificats d'Autorités de Certification (la signature du certificat d'une AC est vérifiée en utilisant le certificat de l'AC signataire et ainsi de suite). Un domaine de certification peut être contraint par des restrictions liées au nommage, aux politiques de certification ou à la longueur maximale du chemin.

Données d'activation : données privées associées à un utilisateur final permettant de mettre en œuvre sa clé privée.

Empreinte (ou hash) : résultat d'une fonction de hachage c'est-à-dire d'une fonction calculant le condensat d'un message de telle sorte qu'une modification même infime du message entraîne la modification de ce condensat.

Enregistrement : action qui consiste pour une autorité à valider une demande de certificat, conformément à une politique de certification.

Exploitant : personne travaillant pour le compte de l'IGC et disposant de droits d'accès à une autorité associés aux rôles qui lui sont attribués.

Génération (émission) d'un certificat : action qui consiste pour l'AC à intégrer les éléments constitutifs d'un certificat, à les contrôler et à signer le certificat.

Infrastructure de gestion de clés (IGC) : ensemble organisé de composantes, fonctions et procédures dédiées à la gestion de clés publiques et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique, équivalent de PKI (Public Key Infrastructure).

Journalisation : fait d'enregistrer dans un fichier dédié à cet effet certains types d'événements provenant d'une application ou du système d'exploitation d'un poste informatique. Le fichier résultant facilite la traçabilité et l'imputabilité des opérations effectuées.

Mandataire de certification : représentant légal d'une structure publique ou privée et mandaté par cette structure pour y gérer les porteurs de cartes CPS, notamment pour l'enregistrement de ces porteurs auprès du GIP "CPS" et la révocation des certificats.

Mandataire de certification délégué : représentant d'une structure publique ou privée désigné par un Mandataire de Certification de cette structure pour y gérer, par délégation, les porteurs de cartes CPS au sein de cette structure, notamment pour l'enregistrement de ces porteurs auprès du GIP "CPS" et la révocation des certificats.



Introduction

Partenaire : promoteur d'application ou opérateur de réseau.

Politique de certification (PC) : ensemble de règles, identifié par un nom, qui définit le type d'application auxquelles un certificat est adapté ou dédié.

Porteur : toute entité (personne physique, personne morale ou process) détenant un certificat de clé généré par une composante de l'IGC.

Prestataire de Services de Certification (PSC) : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique

Publication d'un certificat : fait de mettre un certificat dans un annuaire, à disposition d'utilisateurs susceptibles d'avoir à vérifier une signature ou à chiffrer des informations.

Renouvellement de certificat : action effectuée à la demande d'un utilisateur ou en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat pour un porteur. La re-génération d'un certificat après révocation n'est pas un renouvellement.

Révocation de certificat : action demandée par une Autorité Compétente, une AC, un MC ou un Porteur de certificat, et dont le résultat est la suppression de la caution de l'AC sur un certificat donné, avant la fin de sa période de validité. Cette action peut être la conséquence de différents types d'événements tels que la perte de la carte, la compromission d'une clé, le changement d'informations contenues dans un certificat, etc.

Service d'Horodatage : délivre un temps de confiance pour le compte de l'IGC. Ce temps sert de référence aux informations contenues dans les journaux d'événements. Il sert également de référence aux informations contenues dans un certificat ou une LCR, sur la période de validité d'un certificat ou la date d'émission d'une LCR. Ce service peut être rendu par une Autorité d'Horodatage ou directement par l'AC [PC2].

Service de Publication : le Service de Publication rend disponible les certificats de clés publiques émis par une AC, à l'ensemble des utilisateurs potentiels de ces certificats. Il publie une liste de certificats reconnus comme valides et une liste de certificats révoqués (LCR). Ce service peut être rendu par un annuaire (par exemple de type X.500), un serveur d'information (WEB), une délivrance de la main à la main, une application de messagerie, etc.



Introduction

Système "CPS" : ensemble composé des cartes de la famille "CPS", des systèmes d'information gérant les processus liés à la carte ainsi que l'organisation et les procédures inhérentes.

Utilisateur Final : porteur ou accepteur de certificat.

Vérification de certificat : la procédure de vérification d'un certificat consiste en un ensemble d'opérations destinées à s'assurer que les informations contenues dans le certificat ont été validées par une Autorité de Confiance. La vérification d'un certificat inclut la vérification de sa période de validité, de son état (révoqué ou non), ainsi que de la signature de l'AC génératrice.

Vérification de signature : la vérification d'une signature consiste à déchiffrer la signature d'un message, en mettant en œuvre la clé publique du signataire supposé. Si le clair obtenu est identique à l'empreinte calculée à partir du message reçu, alors il est garanti que le message est intègre et qu'il a été signé par le porteur de la clé privée correspondante à la clé publique utilisée pour la vérification.



Responsabilités concernant la mise à disposition des informations devant être publiées

2. Responsabilités concernant la mise à disposition des informations devant être publiées

2.1 Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des utilisateurs (porteurs et accepteurs), le GIP "CPS" met en oeuvre au sein de son IGC un service de diffusion et un service d'état des certificats (cf. chapitre 1.3.1 ci-dessus).

Le service de diffusion s'appuie :

- sur un annuaire de type X.500, accessible par des requêtes LDAP ou HTTP, à l'adresse annuaire.gip-cps.fr ;
- sur un serveur Web, accessible en HTTP à l'adresse www.gip-cps.fr.

Le service d'état des certificats s'appuie sur la génération de LCR et leur publication dans l'annuaire X.500. Il n'y a pas de service d'état de certificat en ligne (OCSP).

Ces services ont pour missions :

- de garantir les conditions de mise à jour et de disponibilité de l'Annuaire "CPS" et du site Web "CPS" ;
- de gérer les droits d'accès à l'annuaire conformément à la "Charte d'accès à l'Annuaire CPS" qui lui est propre [ACC_ANN].

Les engagements de disponibilité et de continuité d'activité de ces services (serveur Web et annuaire, générateur de LCR) sont précisés au chapitre 0 ci-dessous.

2.2 Informations devant être publiées

Les informations suivantes sont diffusées via le site Web du GIP "CPS" <http://www.gip-cps.fr> :

- ☞ les présentes PC ;
- ☞ la charte d'accès à l'annuaire (cf. [ACC_ANN]) ;
- ☞ les formats de certificats et de LCR objet des présentes PC (cf. [CERT_CPS]) ;

Les informations suivantes sont diffusées via l'annuaire du GIP "CPS" :

- ☞ les certificats valides (non révoqués, non expirés) des porteurs ;



Responsabilités concernant la mise à disposition des informations devant être publiées

☞ les LCR et delta-LCR.

Les formulaires vierges de demande de carte sont obtenus auprès du GIP "CPS", soit directement (en contactant le Service d'Information Téléphonique du GIP "CPS", cf. <http://www.gip-cps.fr>), soit via l'Autorité Compétente dont dépend le porteur.

D'autres informations liées au certificats d'AC sont également diffusées (certificats d'ACR et d'ACI, LAR, etc.) : cf. les PC correspondantes.

Certaines informations liées à l'activité et la mise en œuvre de l'IGC "CPS" ne sont pas publiées (notamment : la déclaration des pratiques de certification) En cas de besoin (demande d'une autorité administrative ou judiciaire, processus d'audit et d'évaluation, établissement d'un accord de reconnaissance avec une autre IGC, etc.), ces informations peuvent être obtenues auprès du GIP "CPS", après signature le cas échéant d'un accord de confidentialité.

2.3 Délais et fréquences de publication

Toute nouvelle version d'un document (PC, charte d'accès à l'annuaire, formats des certificats) est diffusée via le site Web du GIP "CPS" dans les 24h ouvrées suivant sa validation. Le site est accessible 24 heures / 24 et 7 jours / 7.

Dans l'annuaire, également accessible 24 heures / 24 et 7 jours / 7 :

- les certificats des porteurs sont diffusés dans les 24h ouvrées suivant leur génération ;
- les LCR et delta-LCR sont diffusées toutes les 24h (week-ends et jours fériés compris).

2.4 Contrôle d'accès aux informations publiées

Les informations diffusées via le site Web du GIP "CPS" sont en accès libre en lecture.

L'accès aux informations diffusées via l'annuaire du GIP "CPS" est régi par la charte d'accès à l'annuaire (cf. [ACC_ANN]).



3. Identification et authentification

3.1 Nommage

3.1.1 *Convention de noms*

Les noms utilisés dans les certificats émis par l'IGC "CPS" sont conformes aux spécifications de la norme X.500.

Dans chaque certificat de classe 1, le champ "issuer" (AC émettrice) et le champ "subject" (porteur) correspondent à un Distinguished Name (DN).

Pour les porteurs, ce DN est construit à partir des Identifications Nationales des Professionnels de Santé, conformément à ce qui est décrit dans [CERT-CPS].

3.1.2 *Nécessité d'utilisation de noms explicites*

Les noms utilisés dans les champs "issuer" et "subject" d'un certificat de porteur sont explicites dans le domaine santé-social puisqu'ils utilisent les identifications nationales des professionnels de santé, ainsi que le nom d'exercice et le prénom usuel du porteur.

3.1.3 *Anonymisation ou pseudonymisation des porteurs*

N/A.

3.1.4 *Règles d'interprétation des différentes formes de nom*

Les significations des différents champs du DN, aussi bien de l'"issuer" que du "subject", sont décrites dans [CERT_CPS].

3.1.5 *Unicité des noms*

Dans chaque certificat X.509 de classe 1, le DN du champ "issuer" (AC émettrice) et du champ "subject" (AC ou porteur) est unique sur le domaine de certification de l'IGC "CPS".



3.1.6 Identification, authentification et rôle des marques déposées

N/A.

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

N/A.

Les bi-clés ne sont pas générés par le demandeur mais par les boîtiers cryptographiques, rattachés aux unités de personnalisation des cartes CPS, préalablement à la création des certificats. Les bi-clés sont ensuite transférés dans chaque carte de façon sécurisée et chiffrée sans aucune possibilité de conservation d'une copie des clés privées.

3.2.2 Validation de l'identité d'un organisme

Pour les certificats de classe 1, il n'y a pas d'identifiant de structure mais un identifiant national du professionnel de santé (numéro ADELI).

3.2.3 Validation de l'identité d'un individu

Pour les certificats de classe 1, le contrôle de la validité des informations communiquées par le futur porteur, concernant son identité, est réalisé par une Autorité Compétente, et ceci sous sa responsabilité.

La DPC de l'IGC "CPS", et les documents qui l'accompagnent, précisent les différentes catégories de population et les processus d'enregistrement correspondants.

3.2.4 Informations non vérifiées du porteur

Pour les certificats de classe 1, toutes les informations concernant les porteurs figurant dans ces certificats ont fait l'objet de vérifications par les Autorités Compétentes concernées.



3.2.5 Validation de l'autorité du demandeur

Cette étape est effectuée en même temps que la validation de l'identité de l'individu par les Autorités Compétentes concernées.

3.2.6 Critères d'interopérabilité

La décision que l'IGC "CPS" reconnaisse et/ou soit reconnue par une autre IGC est du ressort du Conseil d'Administration du GIP "CPS".

3.3 Identification et validation d'une demande de renouvellement des clés

3.3.1 Identification et validation pour un renouvellement courant des clés

Pour les clés et les certificats de classe 1, le renouvellement s'effectue en même temps que le renouvellement de la carte CPS correspondante (clés, certificats et carte CPS ont la même durée de vie, soit 3 ans). Ce renouvellement est automatique, sans re-vérification préalable de l'identité du porteur.

En effet, les Autorités Compétentes doivent signaler à l'IGC "CPS" tout changement dans l'activité d'un porteur nécessitant le retrait (définitif ou pour mise à jour) de la carte de ce porteur et des certificats correspondants (radiation de l'Ordre, départ à la retraite, etc.).

Tant que l'IGC "CPS" ne reçoit pas d'informations contraires de la part de ces Autorités Compétentes, elle renouvelle automatiquement les cartes CPS (et les clés et les certificats correspondants) sur la base des informations d'enregistrement initial.

3.3.2 Identification et validation pour un renouvellement des clés après révocation

Pour les certificats de classe 1, en cas de perte, vol ou dysfonctionnement de la carte associée, la procédure est la même que pour un renouvellement courant ; dans tout autre cas, la procédure est celle d'un enregistrement initial.



3.4 Identification et validation d'une demande de révocation

La demande de révocation doit provenir d'une entité autorisée (cf. chapitre 4.9.2 ci-dessous).

Une demande de révocation peut se faire par téléphone, au numéro indigo mentionné sur le protocole d'usage de la carte [PUC_CPS] (hotline de l'IGC "CPS"), par messagerie électronique, par fax ou par courrier recommandé avec accusé de réception adressé au GIP "CPS".

Toute personne autorisée souhaitant faire révoquer un certificat CPS, quel que soit le moyen utilisé, doit préalablement s'adresser à la hotline de l'IGC "CPS" qui lui précisera la démarche à suivre ainsi que les informations justificatives à fournir.



4. Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

L'objet de ce paragraphe est de décrire l'étape de constitution du dossier de demande de carte et des certificats associés.

4.1.1 Origine d'une demande de certificat

Pour les certificats de classe 1, les demandes d'enregistrement, transmises au service d'enregistrement de l'IGC "CPS", proviennent de la dernière Autorité Compétente intervenant dans la validation du dossier (cf. chapitre 1.3.2).

4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

Pour les certificats de classe 1, les Autorités Compétentes se chargent, selon leurs propres procédures et sous leur responsabilité, d'apporter les services suivants pour toute demande de certificat :

- établir l'identité du demandeur ;
- vérifier l'autorisation des attributs demandés, lorsque cela est approprié, selon des tables établies conformément à la réglementation ;
- transmettre les demandes validées au service d'enregistrement de l'IGC "CPS".

La génération des bi-clés est assurée ultérieurement par le service de génération, le porteur ne génère donc lui-même aucune clé.

4.2 Traitement d'une demande de certificat

Le service d'enregistrement s'assure de l'origine, de l'intégrité et de la cohérence de la demande transmise par une Autorité Compétente

Ensuite, si aucun problème n'est détecté, il formate et transmet la demande au service de fourniture des cartes CPS.



Exigences opérationnelles sur le cycle de vie des certificats

Le délai moyen entre le dépôt du dossier de demande auprès des Autorités Compétentes et la création des cartes et des certificats associés est de 14 jours.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Le service de fourniture des cartes reçoit les ordres de fabrication du service d'enregistrement.

Les ordres concernant la génération des données cryptographiques sont alors transmis au service de génération qui fournit les bi-clés et les certificats correspondants de la carte CPS à personnaliser.

Le service de fourniture personnalise ensuite la carte CPS en insérant les informations transmises par le service d'enregistrement et les éléments cryptographiques produits par le service de génération.

Le service de fourniture des cartes CPS transmet enfin les certificats générés au service de diffusion (Annuaire "CPS") et expédie la carte contenant les certificats à son porteur. Les codes d'activation et de déblocage de la carte font l'objet d'un envoi distinct de l'envoi de la carte. Un compte rendu est également retourné au service d'enregistrement.

4.3.2 Notification par l'AC de la délivrance du certificat au porteur

Le porteur est implicitement informé de la génération de ses certificats par la réception de sa carte "CPS".

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

La première utilisation de sa carte par le porteur vaut acceptation des certificats qu'elle contient. Le GIP "CPS" recommande au porteur d'en vérifier le contenu avant usage.



4.4.2 Publication du certificat

Le certificat est publié dans un annuaire X500 qui peut être consulté en mode LDAP ou HTTP à l'adresse : annuaire.gip-cps.fr.

4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat

Le service de fourniture des cartes CPS notifie au service d'enregistrement l'envoi au porteur de la carte contenant ses certificats.

4.5 Usages du bi-clés et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le porteur

L'utilisation de la clé privée et du certificat associé est limitée aux conditions d'usage définies dans les présentes PC (cf. § 1.4) et ceci conformément à l'utilisation spécifique décrite dans le contenu du certificat (attribut *key usage* et *extended key usage*, cf. [CERT_CPS]).

L'utilisation du bi-clé et du certificat de signature est réservée à la signature de documents au sens juridique du terme (manifestation du consentement du signataire sur le contenu du document). L'utilisation du bi-clé et du certificat d'authentification est réservée à l'authentification du porteur, l'authentification de l'origine et la garantie de l'intégrité des données transmises par le porteur.

L'utilisation d'une clé privée n'est autorisée que pendant la période de validité du certificat associé et vaut acceptation des conditions d'usage par le porteur.

4.5.2 Utilisation de la clé publique et du certificat par l'accepteur du certificat

L'utilisation du certificat et de la clé publique associée est limitée aux conditions d'usage définies dans les présentes PC (cf. § 1.4) et à l'usage prévu indiqué dans le certificat (attribut *key usage* et *extended key usage*, cf. [CERT_CPS]).

L'accepteur est tenu de vérifier la validité du certificat et la conformité de son utilisation.

La responsabilité du GIP "CPS" ne peut être engagée pour une utilisation ne correspondant pas aux conditions d'usage.



4.6 Renouvellement d'un certificat

Dans le contexte du GIP "CPS", un renouvellement de certificat sans renouvellement de la carte CPS et donc des bi-clés correspondants est impossible. Une demande de renouvellement entraîne donc automatiquement la fabrication d'un nouveau support et la génération de nouveaux bi-clés (cf. chapitre 4.7 ci-dessous). Ce chapitre n'est donc pas applicable dans le cas de l'IGC "CPS".

4.7 Délivrance d'un nouveau certificat suite à changement du bi-clé

Il est à noter que le changement de bi-clé ne peut se faire que dans le cas du renouvellement de la carte CPS correspondante.

4.7.1 Causes possibles de changement d'un bi-clé

La cause principale de la délivrance de nouveaux certificats et bi-clés est l'arrivée à la date de fin de validité de la carte. La durée de validité des cartes CPS est de 3 ans. Les bi-clés doivent être en effet périodiquement renouvelés afin de minimiser les risques d'attaque cryptographique.

Un renouvellement peut être aussi réalisé de manière anticipée, suite à un événement ou un incident déclaré par le porteur de carte, les plus fréquents étant la perte, le vol ou le dysfonctionnement de la carte.

Une modification des informations contenues dans la carte entraîne également la délivrance d'une nouvelle carte.

4.7.2 Origine d'une demande d'un nouveau certificat

Pour les cartes arrivées à expiration, le processus de renouvellement est automatiquement déclenché par l'IGC "CPS".

Dans les autres cas, la demande est faite selon les mêmes processus qu'une demande initiale (cf. chapitre 4.1 ci-dessus).

4.7.3 Procédure de traitement d'une demande d'un nouveau certificat

Pour les cartes renouvelées suite à expiration, le traitement est automatique (une vérification est effectuée qu'aucune demande de modification n'est en cours).



Exigences opérationnelles sur le cycle de vie des certificats

Dans les autres cas, la procédure de traitement est la même que pour une demande initiale.

4.7.4 Notification au porteur de l'établissement du nouveau certificat

La notification au porteur est réalisée par la réception de la nouvelle carte CPS.

4.7.5 Démarche d'acceptation du nouveau certificat

La première utilisation de sa nouvelle carte par le porteur vaut l'acceptation des certificats qu'elle contient. Il appartient au porteur d'en vérifier le contenu avant usage.

4.7.6 Publication du nouveau certificat

L'annuaire de publication des certificats est mis à jour en cas de changement de carte.

4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Le service de fourniture des cartes CPS notifie au service d'enregistrement l'envoi au porteur de la carte contenant ses certificats.

4.8 Modification du certificat

Lorsqu'une donnée quelconque du certificat doit faire l'objet d'une modification, une nouvelle carte avec de nouveaux certificats, et de nouveaux bi-clés, est obligatoirement délivrée et les anciens certificats automatiquement révoqués.

De même lorsque des données de la carte CPS hors certificat doivent être modifiées, la carte est renouvelée, ainsi que les bi-clés et certificats correspondants, et les anciens certificats automatiquement révoqués.

4.8.1 Causes possibles de modification d'un certificat

Les événements pouvant conduire à une modification des données du certificat sont, par exemple, la modification du nom d'exercice ou de l'identification nationale du porteur.



4.8.2 Origine d'une demande de modification d'un certificat

La demande de modification des données contenues dans un certificat provient de l'Autorité Compétente *ad hoc*.

4.8.3 Procédure de traitement d'une demande de modification d'un certificat

Cf. § 4.7.3.

4.8.4 Notification au porteur de l'établissement du certificat modifié

Cf. § 4.7.4.

4.8.5 Démarche d'acceptation du certificat modifié

Cf. § 4.7.5.

4.8.6 Publication du certificat modifié

Cf. § 4.7.6.

4.8.7 Notification par l'AC aux autres entités de la délivrance du certificat modifié

Cf. § 4.7.7.

4.9 Révocation et suspension des certificats

Il n'y a pas de suspension possible de certificat. Seule la révocation définitive des certificats, correspondant à la mise en opposition de la carte CPS, peut être réalisée.

4.9.1 Causes possibles d'une révocation

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat de classe 1 :

- la clé privée du porteur est perdue, volée, inutilisable (dysfonctionnement carte), compromise ou suspectée de compromission (demande du porteur lui-même) ;



Exigences opérationnelles sur le cycle de vie des certificats

- les informations ou les attributs du porteur figurant dans son certificat ne sont plus valides ou plus en cohérence avec l'utilisation prévue du certificat, ceci avant l'expiration normale du certificat ;
- il a été démontré que le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le certificat d'AC intermédiaire de la classe concernée est révoqué (ce qui entraîne la révocation des certificats signés par la clé privée correspondante) ;
- le porteur ne satisfait plus aux conditions professionnelles requises (cessation d'activité, décès).

Les causes de révocation ne sont jamais publiées dans les LCR ou DeltaLCR.

4.9.2 Origine d'une demande de révocation

Les entités qui peuvent demander la révocation d'un certificat de classe 1 sont les suivantes :

- le porteur au nom duquel le certificat a été émis ;
- l'Autorité Compétente qui a validé la demande ;
- le GIP "CPS".

4.9.3 Procédure de traitement d'une demande de révocation

La validation de la demande inclut la vérification de l'origine de la demande et de l'applicabilité de la cause invoquée. Après cette validation, le service de gestion des révocations formate et transmet la demande au service d'état des certificats chargé d'ajouter les n° de série de certificats à révoquer dans les prochaines LCR et DeltaLCR à générer et publier. Les certificats révoqués sont également retirés de l'annuaire.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

N/A

4.9.5 Délai de traitement par l'AC d'une demande de révocation

Les demandes de révocation sont traitées dans les 24h suivant la réception de la demande, 7 jours / 7 (week-ends et jours fériés compris), hors révocations consécutives à des demandes de modification des données du porteur.



4.9.6 Exigences de vérification de la révocation par les accepteurs de certificats

Les accepteurs des certificats CPS doivent vérifier la non-révocation des certificats sur lesquels ils vont baser leur confiance. Cette vérification se fait en consultant les LCR ou DeltaLCR disponibles via l'annuaire (annuaire.gip-cps.fr).

4.9.7 Fréquence d'établissement des LCR

Le service d'état des certificats publie une mise à jour quotidienne des LCR et des DeltaLCR. Chaque LCR (ou DeltaLCR) contient la date et l'heure prévisionnelles de publication de la LCR (ou DeltaLCR) suivante.

Par mesure de sécurité, les LCR et DeltaLCR ont une durée de validité de 2 jours ouvrés.

4.9.8 Délai maximum de publication d'une LCR

Le délai maximum entre les publications de deux LCR ou DeltaLCR consécutives est de 24h, 7 jours/7.

4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

N/A (seul le mécanismes de LCR / Delta-LCR est mis en œuvre au sein de l'IGC "CPS").

4.9.10 Exigences de vérification en ligne de la révocation des certificats par les accepteurs de certificats

N/A

4.9.11 Autres moyens disponibles d'information sur les révocations

N/A (seul le mécanisme de LCR / Delta-LCR est mis en œuvre au sein de l'IGC "CPS" pour les certificats de porteurs).

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Il n'y a pas de mesures particulières, concernant les clés privées des porteurs, autres que la révocation des certificats correspondants.



4.9.13 Causes possibles d'une suspension

Les certificats ne peuvent être révoqués que de façon définitive. Il n'est pas envisagé de possibilité de révocation temporaire (suspension).

4.9.14 Origine d'une demande de suspension

N/A

4.9.15 Procédure de traitement d'une demande de suspension

N/A

4.9.16 Limites de la période de suspension d'un certificat

N/A

4.10 Service d'état des certificats

4.10.1 Caractéristiques opérationnelles

L'état des certificats peut être vérifié en consultant les LCR et DeltaLCR qui peuvent être téléchargées en mode LDAP à l'adresse :

ldap://annuaire.gip-cps.fr/c=fr,o=gip-cps,ou=gip-cps professionnel,cn=gip-cps classe 1

4.10.2 Disponibilité du service

Le service est disponible 24 heures / 24 et 7 jours / 7 via l'annuaire du GIP "CPS" :
annuaire.gip-cps.fr.

4.10.3 Dispositifs optionnels

N/A.



4.11 Expiration de l'abonnement des porteurs

A l'expiration de l'abonnement des porteurs (notamment fin de l'activité ayant justifié l'attribution d'une carte de la famille CPS), tous les certificats liés à cette carte sont révoqués.

4.12 Séquestre de clé et recouvrement

N/A (les clés de signature et d'authentification ne sont stockées que dans les cartes CPS des porteurs et ne sont pas séquestrées).



5. Mesures de sécurité non techniques

Ce chapitre traite des mesures de sécurité non techniques (c. à d. concernant la sécurité physique, les procédures et la gestion du personnel) appliquées dans le but de sécuriser les fonctions de génération de clé, d'authentification des individus, de délivrance des certificats, de révocation des certificats, d'audit et d'archivage.

Ces mesures concernent l'ensemble des composantes de l'IGC "CPS" (GIP "CPS" et opérateurs techniques). La DPC répondant aux présentes PC précise le contenu de ces mesures et à quelle(s) composante(s) de l'IGC elles s'appliquent.

5.1 Mesures de sécurité physiques

Le GIP "CPS" s'engage à (faire) mettre en œuvre et à (faire) maintenir un niveau de sécurité physique conforme aux règles de bonne pratique concernant les locaux d'exploitation des composantes de l'ensemble de son IGC.

La DPC précise les règles et modalités d'application concernant les points suivants :

- situation géographique et construction du site,
- accès physique,
- énergie et air conditionné,
- vulnérabilité aux dégâts des eaux,
- prévention et protection incendie,
- conservation des supports,
- mise hors service des supports,
- sauvegardes hors-site.
-

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

On distingue au sein de l'IGC "CPS" quatre types de rôles de confiance concernant respectivement :

- la sécurité cryptographique,
- la gestion des processus de l'IGC,
- les opérations du service d'enregistrement,



Mesures de sécurité non techniques

- l'exploitation.

Les tâches et les différents intervenants de ces rôles sont décrits dans la DPC.

5.2.2 Nombre de personnes requises par tâches

Selon le type et la sensibilité de l'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes (en tant qu'acteurs ou témoins) peuvent être différents. Le nombre minimum d'exploitants exigé par chaque type d'opération est précisé dans la DPC.

5.2.3 Identification et authentification pour chaque rôle

Toutes les composantes de l'IGC "CPS" font vérifier l'identité et les autorisations de tout membre de leur personnel avant toute action de la liste suivante :

- que son nom soit ajouté à la liste de contrôle d'accès aux locaux des différents services de l'IGC ;
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement aux systèmes de l'IGC ;
- qu'un certificat lui soit délivré pour accomplir le rôle qui lui est dévolu dans l'IGC ;
- qu'un compte soit ouvert en son nom dans les systèmes de l'IGC.

5.2.4 Rôles exigeant une séparation des attributions

Le cumul de plusieurs tâches par un même intervenant peut être admis à condition de respecter la séparation des attributions définie dans la DPC. Enfin, certaines tâches particulièrement sensibles peuvent requérir des intervenants ayant des rôles différents.

5.3 Mesures de sécurité vis-à-vis du personnel

Les contrôles de sécurité vis-à-vis du personnel s'appliquent à l'ensemble du personnel lié à l'activité de l'IGC "CPS", qu'il s'agisse du personnel interne au GIP "CPS" ou du personnel d'entités sous-traitantes exploitant certaines composantes de l'IGC. En fonction de la sensibilité des tâches affectées, ces mesures concernent :

- les qualifications, les compétences, les habilitations requises ;
- la vérification des diplômes et des antécédents professionnels ;
- les exigences en matière de formation initiale ;



Mesures de sécurité non techniques

- la fréquence et les exigences concernant la formation continue ;
- les sanctions en cas d'action non autorisée ;
- la documentation fournie au personnel.

La DPC précise les pratiques associées à ces mesures pour le GIP "CPS" et ses sous-traitants.

5.4 Procédures de constitution des données d'audit

5.4.1 Type d'événements à enregistrer

Toute opération sensible, c'est à dire manipulant des biens protégés, fait l'objet d'une trace fiable et auditable. La journalisation des événements est sous la responsabilité de chaque composante de l'IGC "CPS" pour les événements qui la concernent.

Les événements sont journalisés soit automatiquement, sous forme électronique, soit manuellement, sous forme électronique ou papier.

Les événements journalisés se décomposent en deux grandes catégories :

- les événements relatifs aux services de l'IGC (enregistrement des porteurs, génération des éléments cryptographiques, personnalisation des cartes, etc.) ;
- les événements relatifs à la sécurité et au fonctionnement des systèmes (initialisation / mise en route d'un système, accès à un système ou une application, modification des droits d'accès, accès à une zone sensible, interventions de maintenances, etc.).

Les informations stockées dépendent du type d'événement mais comprennent au minimum les champs suivants :

- les date et heure de l'opération ;
- le type et la description de l'opération ;
- les intervenants : responsable de l'opération et entité ayant généré l'entrée dans le journal d'événements ;

La DPC précise les événements enregistrés et les informations correspondantes.



5.4.2 Fréquence de traitement des journaux d'événements

Les journaux d'événements sont revus sur incident impactant la sécurité. Un contrôle approfondi est alors immédiatement diligenté afin d'identifier et de corriger les anomalies.

5.4.3 Période de conservation des journaux d'événements

La période de conservation des journaux d'événements est précisée dans la DPC suivant le type d'exploitation.

5.4.4 Protection des journaux d'événements

Les journaux d'événements sont classifiés et font l'objet de mesures de protection adaptées, notamment quant aux procédures d'accès, à la protection de leur intégrité et à leur sauvegarde. Ces mesures de sécurité sont décrites dans la DPC.

5.4.5 Procédure de sauvegarde des journaux d'événements

La procédure de sauvegarde des journaux d'événements est décrite dans la DPC.

5.4.6 Système de collecte des journaux d'événements

La collecte des journaux d'événements est de la responsabilité de chaque composante de l'IGC "CPS" pour les journaux qui la concerne. Les journaux relatifs aux services de l'IGC sont également transmis systématiquement au GIP "CPS".

5.4.7 Notification de l'enregistrement d'un événement au responsable de l'événement

N/A

5.4.8 Evaluation des vulnérabilités

Les journaux d'événements sont utilisés pour analyser les causes et origines de toute tentative, réussie ou non-réussie, d'action non autorisée.



5.5 Archivage des données

5.5.1 Types de données à archiver

Les informations concernant l'ensemble de l'IGC "CPS" sont conservées sous la responsabilité du GIP "CPS", notamment les PC et la DPC.

Au titre des présentes PC, sont archivées les informations concernant les porteurs, c'est à dire :

- les formulaires de demande de cartes ;
- les certificats et les LCR tels qu'émis ou publiés ;
- les justificatifs d'identités des porteurs fournies lors des demandes de révocation ;
- les documents contractuels et conventions.

Sont également archivées les informations de suivi de la sécurité de l'IGC, selon modalités figurant dans la DPC.

Pour les documents propres à chaque composante de l'IGC "CPS" et notamment les informations sur la configuration des équipements informatiques, la conservation est de la responsabilité de la composante concernée.

5.5.2 Période de conservation des archives

Les formulaires de demande de cartes sont conservés pendant trente ans.

Les certificats de clés de signature et d'authentification, ainsi que les LCR produites par l'AC, sont archivés pendant cinq ans après l'expiration des clés.

Les journaux des évènements relatifs aux fonctions de l'IGC tels que décrits en 5.4.1 sont archivés 5 ans après génération.

Les durées d'archivage des informations de suivi de la sécurité de l'IGC sont précisées dans la DPC.

5.5.3 Protection des archives

Les archives sont dûment protégées contre les risques d'accès illicite, de modification et de destruction ou d'altération. Les moyens de protection mis en œuvre sont conformes au niveau de classification des données archivées.



5.5.4 Procédure de sauvegarde des archives

Les procédures correspondantes sont décrites dans la DPC.

5.5.5 Exigences d'horodatage des données

Les pratiques d'horodatage des données archivées sont précisées dans la DPC.

5.5.6 Système de collecte des archives

Les archives font l'objet d'une centralisation qui est précisée dans la DPC.

5.5.7 Procédures de récupération et de vérification des archives

Les archives ne sont accessibles que par les entités et composantes concernées au sein de l'IGC. Les procédures correspondantes sont décrites dans la DPC.

5.6 Changement de clé d'AC

L'ACI ne peut pas générer de certificat porteur dont la date de fin serait postérieure à la date d'expiration de son bi-clé de signature de certificats.

De ce fait, la période de validité de son certificat est supérieure à celle des certificats des porteurs, et la conséquence en est nécessairement un chevauchement des périodes de validité des certificats de l'ACI.

Lorsqu'un nouveau certificat d'ACI est émis, le certificat d'ACI précédent peut toujours être utilisé pour vérifier l'authenticité des certificats porteurs émis sous cet ancien certificat, et ce jusqu'à ce que ces certificats porteurs aient expiré.

5.7 Reprise suite à compromission et sinistre

5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

Les différentes composantes de l'IGC "CPS" disposent des procédures permettant de traiter de manière graduelle et adéquate tout incident.



5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Chaque composante de l'IGC "CPS" dispose d'un plan de continuité garantissant, en cas de sinistre majeur, une reprise dans des délais compatibles avec les exigences de sécurité requises par l'IGC.

5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une entité

La DPC précise les mesures prises en cas de compromission :

- d'une clé privée interne à une entité utilisée pour sécuriser les activités de cette entité ;
- d'une clé privée d'AC racine ou intermédiaire.

5.7.4 Capacités de continuité d'activités suite à un sinistre naturel ou autre

Les mesures de sécurité permettant la reprise d'activités après un sinistre sont spécifiées dans la DPC.

5.8 Fin de vie de l'IGC

En cas d'interruption de ses activités, le GIP "CPS" s'engage à en aviser immédiatement les porteurs et à prendre des dispositions pour que les certificats et les informations de ses AC continuent d'être archivées selon les indications et la période stipulée dans les présentes PC.

En outre, le GIP "CPS" s'engage à :

- communiquer avec un préavis de six mois son intention de cesser son activité ;
- mettre en œuvre tous les moyens dont il dispose pour informer ses partenaires de ses intentions ;
- révoquer ses certificats d'AC (sauf en cas de transfert) ;
- révoquer tous les certificats valides signés par son IGC (sauf en cas de transfert) ;
- assurer la pérennité des LCR émises ;
- remettre ses archives ainsi que l'ensemble des données dont il dispose à une entité fiable.



**POLITIQUES DE CERTIFICATION
DE L'IGC "CPS"**
Autorité de Certification "PROFESSIONNEL - Classe 1"
Certificats de signature et d'authentification

Diffusion Libre
Version 1.01 du
13/12/2004

Mesures de sécurité non techniques

En cas de transfert des activités de l'IGC "CPS" à un autre PSC, ce dernier devra offrir le même niveau d'assurance (niveau de confiance dans la sécurité des processus mis en œuvre).



6. Mesures de sécurité techniques

6.1 Génération et installation de bi clés

6.1.1 Génération des bi-clés

La génération des bi-clés des porteurs est effectuée dans des boîtiers cryptographiques sécurisés, lors de la personnalisation des cartes CPS, sans que soit conservée la moindre trace des clés privées suite à la personnalisation.

Le boîtier cryptographique assure également la génération des certificats de clés publiques.

6.1.2 Transmission de la clé privée à son propriétaire

Les clés privées relatives aux certificats d'authentification et de signature sont confinées, suite à la personnalisation de la carte CPS, dans une zone de la puce protégée, dont l'accès est réservé au microprocesseur de la carte. Le transfert des clés privées entre le boîtier cryptographique et les cartes CPS est réalisé en garantissant l'intégrité et la confidentialité de ces clés.

Les cartes "CPS" et les codes porteurs associés sont expédiés aux porteurs par courriers séparés.

6.1.3 Transmission de la clé publique à l'AC

La génération de bi-clés et la génération de certificats sont réalisées dans le même boîtier cryptographique par le service de génération au moment de la personnalisation de la carte CPS. Après génération du bi-clé, la clé publique est directement associée au futur porteur dans un certificat. La conception du boîtier garantit que la clé publique ne peut être falsifiée avant certification.

6.1.4 Transmission de la clé publique de l'AC aux accepteurs de certificats

Cf. [PC_ACR-PRO]



6.1.5 Tailles des clés

Les bi-clés de signature et d'authentification des porteurs de cartes "CPS" utilisent des clés RSA respectivement de 2048 bits et de 1024 bits.

6.1.6 Vérification de la génération des paramètres des clés publiques et de leur qualité

Les paramètres de génération sont explicités dans le document référencé [CERT_CPS].

6.1.7 Objectifs d'usage de la clé

[SIGNATURE] Les bi-clés de signature sont utilisés à des fins de non répudiation.

[AUTHENTIFICATION] Les bi-clés d'authentification sont utilisés à des fins d'authentification.

Les différents usages possibles des clés sont définis et contraints par l'utilisation d'une extension de certificat X.509v3.

6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

Les modules cryptographiques utilisés pour la génération des bi-clés et la fabrication des certificats sont des boîtiers cryptographiques sécurisés : cf. [PC_ACR-PRO].

Les cartes CPS, dans lesquelles sont stockées et mises en oeuvre les clés privées des porteurs, font l'objet d'une certification sécurité (cf. chapitre 6.2.11).

6.2.2 Contrôle de la clé privée par plusieurs personnes

Les clés privées de signature et d'authentification des porteurs de cartes "CPS" sont protégées par la carte à puce et le code d'activation correspondant. Elles sont donc strictement personnelles et ne peuvent être utilisées que par les porteurs eux-mêmes.



6.2.3 Séquestre de la clé privée

Les clés privées de porteurs ne sont en aucun cas séquestrées.

6.2.4 Copie de secours de la clé privée

Les clés privées des porteurs sont dûment protégées au sein de la carte, et leur processus de génération interdit de générer toute copie de secours.

6.2.5 Archivage de la clé privée

Les clés privées de signature et d'authentification ne sont pas archivées : elles sont détruites "à la volée" dans le boîtier cryptographique après chargement dans les cartes.

6.2.6 Transfert de la clé privée vers / depuis le module cryptographique

Dans le cas des données cryptographique des porteurs, le transfert depuis le boîtier cryptographique vers la carte CPS se fait de manière sécurisée. Le mécanisme de sécurité de cet échange est précisé dans la DPC.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées de porteur sont stockées et mises en œuvre uniquement au sein de la carte CPS, sans possibilité de les en faire sortir.

6.2.8 Méthode d'activation de la clé privée

L'activation des clés privées du porteur se fait par la fourniture d'un code PIN, appelé **code porteur**. Les clés ne sont actives que pendant l'insertion de la carte dans le lecteur et pendant une période déterminée qui dépend du logiciel associé au lecteur choisi par le porteur.

6.2.9 Méthode de désactivation de la clé privée

Le retrait de la carte ou la déconnexion par le porteur du service utilisé ayant requis l'activation interdit l'utilisation de la clé (la clé n'est à aucun moment chargée en mémoire). La fourniture du code d'activation est à nouveau requise.



6.2.10 Méthode de destruction des clés privées

La destruction d'une clé privée porteur est réalisée définitivement par la destruction physique de la carte la supportant, par le porteur ou par le GIP "CPS" pour les cartes qui lui sont retournées.

6.2.11 Niveau d'évaluation sécurité du module cryptographique

Les composants des cartes CPS des porteurs sont certifiés ITSEC E3 fort.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques sont archivées dans le cadre de l'archivage des certificats.

6.3.2 Durées de vie des bi-clés et des certificats

La durée de vie des bi-clés et des certificats porteur est de 3 ans.

6.4 Données d'activation

Les données d'activation sont des données personnelles et confidentielles. Le porteur se doit d'en protéger la confidentialité et l'intégrité.

6.4.1 Génération et installation des données d'activation

Les données d'activation (code porteur et code de déblocage) sont uniques, générées de façon aléatoire et incluses dans la carte lors de sa personnalisation. Elles ont pour objet de protéger les clés privées et les données du porteur de la carte contre toute utilisation frauduleuse.

Le porteur a la possibilité de modifier à volonté son code porteur :

- par saisie de son code actuel puis de son nouveau code ;
- par saisie de son code de déblocage et de son nouveau code.



6.4.2 Protection des données d'activation

Le code porteur est composé de 4 caractères numériques. Il est envoyé au porteur de la carte par courrier séparé.

Le porteur doit protéger son code porteur et ne pas l'inscrire à proximité de sa carte.

Le blocage de la carte s'effectue après trois tentatives successives infructueuses de connexion.

En cas de blocage, le porteur dispose d'un code de déblocage et d'un logiciel de gestion "CPS", lui permettant de réactiver sa carte.

En cas de perte de son code de déblocage, le porteur peut en demander par courrier la réexpédition à son adresse par le GIP "CPS".

6.4.3 Autres aspects liés aux données d'activation

Le code porteur lié à la carte est le même pour l'authentification et la signature.

6.5 Mesures de sécurité des systèmes informatiques

Les systèmes informatiques de l'IGC "CPS" répondent aux exigences suivantes :

- identification et authentification des opérateurs ;
- contrôle des habilitations d'accès aux services ;
- sécurisation de la session ;
- protection contre les virus informatiques ;
- protection du réseau contre les intrusions et protection des flux ;
- journalisation des opérations et trace d'audit.

Les solutions mises en œuvre peuvent être fournies par une combinaison de procédures et/ou de mécanismes offerts par les matériels et logiciels composant les systèmes et par des mesures de protection physique. Dans tous les cas, le niveau minimal des mesures de sécurité est conforme à l'état de l'art et est précisé dans la DPC.

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

L'implémentation d'un système permettant de mettre en œuvre les services de l'IGC "CPS" est documentée et respecte, dans la mesure du possible, des normes de modélisation et d'implémentation.



Mesures de sécurité techniques

La configuration des composantes ainsi que toutes modifications et mises à niveau sont documentées et contrôlées. Elles apparaissent dans les procédures de fonctionnement interne de la composante concernée. La DPC précise la démarche retenue permettant d'assurer l'intégrité des logiciels, ainsi que de contrôler la configuration des systèmes de l'IGC.

6.7 Mesures de sécurité réseau

Les mesures de sécurité réseau sont précisées dans la DPC et permettent d'assurer le bon fonctionnement des systèmes de l'IGC. Elles couvrent notamment l'interconnexion vers des réseaux publics.

6.8 Horodatage

Les LCR, les certificats ainsi que les journaux d'événements sont horodatés par l'AC.



7. Profils des certificats, OSCP et des LCR

Cf. [CERT_CPS]. Ce document est en consultation libre et disponible sur le site Internet du GIP "CPS" <http://www.gip-cps.fr>.

7.1 Profil des certificats

7.1.1 Numéro de version

Cf. [CERT_CPS].

7.1.2 Extensions du certificat

Cf. [CERT_CPS].

7.1.3 OID des algorithmes

Cf. [CERT_CPS].

7.1.4 Forme des noms

Cf. chapitre 3.1 ci-dessus.

7.1.5 Contraintes sur les noms

Cf. chapitre 3.1 ci-dessus.

7.1.6 OID des PC

Cf. chapitre 1.2 ci-dessus.

7.1.7 Utilisation de l'extension "contraintes de politique"

Cf. [CERT_CPS].



7.1.8 Sémantique et syntaxe des qualifiants de politique

Cf. [CERT_CPS].

7.1.9 Sémantiques de traitement des extensions critiques de la PC

Cf. [CERT_CPS].

7.2 Profil des LCR

7.2.1 Numéro de version

Cf. [CERT_CPS].

7.2.2 Extensions de LCR et d'entrées de LCR

Cf. [CERT_CPS].

7.3 Profil OSCP

Les mécanismes OSCP ne sont pas mis en œuvre par l'IGC "CPS" au titre des présentes PC.

7.3.1 Numéro de version

N/A

7.3.2 Extensions OCSP

N/A



8. Audit de conformité et autres évaluations

8.1 Fréquences et / ou circonstances des évaluations

Un contrôle de conformité est réalisé de manière régulière, au moins tous les deux ans, afin de vérifier la conformité de la mise en œuvre opérationnelle par rapport à la DPC.

8.2 Identités / qualifications des évaluateurs

Le GIP "CPS", en tant que PSC responsable de l'ensemble des composantes de l'IGC "CPS", fait réaliser les opérations de contrôle par une entité d'audit indépendante.

L'entité d'audit est choisie par le GIP "CPS" en fonction de ses compétences en sécurité des systèmes d'information.

8.3 Relations entre évaluateurs et entités évaluées

L'évaluateur doit être indépendant de l'entité évaluée. Les composantes de l'IGC "CPS" n'auront aucun lien structurel avec cette entité. Les modalités de vérification des relations entre l'évaluateur et l'entité sont précisées dans la DPC.

8.4 Sujets couverts par les évaluations

Le contrôle de conformité périodique porte sur l'ensemble de l'architecture de l'IGC "CPS" et vise à vérifier le respect des engagements et pratiques définies dans les présentes PC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5 Actions prises suite aux conclusions des évaluations

Selon les résultats et les recommandations du contrôle de conformité, le GIP "CPS" a la responsabilité de mettre en œuvre les mesures correctrices éventuellement nécessaires,



d'engager, si besoin, des investigations complémentaires, voire de suspendre temporairement certaines opérations de l'IGC "CPS".

8.6 Communication des résultats

Les modalités de communication des résultats sont précisées dans la DPC.



9. Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Ces tarifs sont fournis avec les contrats d'abonnement.

9.1.2 Tarifs pour accéder aux certificats

Ce service est fourni gratuitement.

9.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats

Ce service est fourni gratuitement.

9.1.4 Tarifs pour d'autres services

N/A.

9.1.5 Politique de remboursement

N/A.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

Le GIP "CPS" a contracté une assurance couvrant son activité de prestataire de services de certification.



9.2.2 Autres ressources

N/A.

9.2.3 Couverture et garantie concernant les entités utilisatrices

N/A.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations classifiées

Les informations classées secrètes⁴ sont au minimum les clés privées des porteurs ainsi que les clés cryptographiques (clés privées et clés secrètes) de gestion des différentes entités de l'IGC "CPS".

Les informations considérées comme confidentielles⁵ sont au minimum :

- le code porteur ;
- le code de déblocage des cartes des porteurs ;
- la DPC de l'IGC "CPS" ;
- les journaux d'événements des composantes de l'IGC "CPS" ;
- certaines spécifications des systèmes de sécurité.

Les informations sensibles⁶ sont des données propres aux porteurs de certificats et soumises à la déclaration CNIL.

Les causes de révocation peuvent être connues des Autorités Compétentes (selon la classe du certificat et les procédures de l'Autorité Compétente concernée) mais ne sont pas transmises à l'IGC "CPS" (sauf par le porteur en cas de perte, vol, destruction, etc.). De ce fait, les causes de révocation ne peuvent être divulguées par l'IGC "CPS".

⁴ Les informations classées secrètes sont les informations dont la divulgation pourrait mettre en péril les activités de l'IGC "CPS", de ses clients, ou plus généralement des tiers avec lesquels le GIP "CPS" est en relation.

⁵ Les informations classées confidentielles sont des informations dont la divulgation pourrait nuire de façon significative à l'IGC "CPS", à ses clients ou plus généralement à des tiers avec lesquels le GIP "CPS" est en relation, sans mettre en cause leur pérennité.

⁶ Les informations classées sensibles sont des informations dont la divulgation pourrait entraîner un léger préjudice pour l'IGC "CPS" ou pour ses clients, mais dont la diffusion ne saurait être restreinte à une liste de personnes identifiées.



9.3.2 Informations hors du périmètre des informations classifiées

Les informations non classifiées sont dites "libres"⁷ et peuvent être publiées sans restriction.

9.3.3 Responsabilités en terme de protection des informations classifiées

Le GIP "CPS" s'engage à ne pas divulguer les informations classées confidentielles au public et à ne les diffuser qu'à des personnes nominativement identifiées.

Les destinataires d'informations classifiées sont responsables d'en assurer le niveau de confidentialité adéquat.

Les informations classées secrètes soit ne sont pas accessibles (par exemple, clés privées des porteurs qui ne sont sous forme déchiffrée qu'à l'intérieur des boîtiers cryptographiques et des cartes CPS), soit sont accessibles uniquement aux personnes justifiant du besoin d'en connaître et dûment autorisées (par exemple, parties de "secrets d'IGC").

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

Le GIP "CPS" est soumis à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

9.4.2 Informations à caractère personnel

Toutes les données d'enregistrement des porteurs des cartes CPS sont considérées comme personnelles.

9.4.3 Informations non à caractère personnel

Toutes les autres données, autres que les données d'enregistrement ne sont pas considérées comme personnelles.

⁷ Les informations classées libres sont destinées à une libre circulation.



9.4.4 Responsabilité en termes de protection des données personnelles

Le GIP "CPS" ne transmet pas de fichiers d'informations personnelles à des tiers.

9.4.5 Notification et consentement d'utilisation des données personnelles

La demande d'une carte CPS implique de la part du demandeur son consentement pour l'utilisation de ses données personnelles devant figurer dans ses certificats. Ces certificats sont accessibles via Internet sur l'Annuaire "CPS" sauf demande spécifique de mise sur liste rouge de la part du demandeur.

9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Le GIP "CPS" se conforme à la législation en vigueur.

9.4.7 Autres circonstances de divulgation d'informations personnelles

N/A

9.5 Droits sur la propriété intellectuelle et industrielle

Le GIP "CPS" est titulaire de l'ensemble des droits de propriété intellectuelle et industrielle attachés aux éléments de toute nature et notamment logiciel, bases de données, documentation, matériel, système, savoir-faire utilisés au titre du service proposé et fourni par l'IGC "CPS", ou a obtenu des titulaires desdits droits, les autorisations nécessaires aux fins d'exécution dudit service.

Les logiciels, bases de données, documentation, matériel, système, savoir-faire et tout autre produit, élément, document, utilisés au titre du service proposé et fourni par l'IGC "CPS", ainsi que tous les droits de propriété intellectuelle et industrielle qui y sont attachés (droit d'auteur, brevet, marque, etc.), restent en toutes circonstances la propriété exclusive du GIP "CPS" (et/ou, selon le cas, de son concédant), quel qu'en soit l'état d'achèvement.

En conséquence, la fourniture du service par l'IGC "CPS" ne saurait être interprétée comme entraînant la cession d'un quelconque droit de propriété intellectuelle et industrielle appartenant au GIP "CPS" ou, le cas échéant, à ses concédants, et afférent aux éléments précités.



Le porteur de carte "CPS" s'engage à maintenir sur tous les exemplaires et copies, mêmes partielles, des éléments précités, les mentions de propriété au profit du GIP "CPS" et/ou, selon le cas, de son concédant, et à n'effectuer aucune adjonction ou modification, rendant notamment ces mentions de propriété illisibles, sans avoir obtenu l'accord préalable écrit du GIP "CPS".

9.6 Interprétations contractuelles et garanties

9.6.1 Autorités de Certification

Au titre des présentes PC, et pour le domaine qu'elles couvrent (cf. chapitres 1.3 et 1.4 ci-dessus), le GIP "CPS", en tant que PSC, garantit le respect des engagements décrits dans le présent document.

Notamment, le GIP "CPS" garantit que l'identité et la qualité du porteur mentionnées dans le certificat sont strictement conformes aux informations transmises par l'Autorité Compétente habilitée.

9.6.2 Service d'enregistrement

Le service d'enregistrement fait partie de l'IGC "CPS" et est donc couvert par les garanties du GIP "CPS" en tant que PSC : cf. § 9.6.1 ci-dessus.

9.6.3 Porteurs de certificats

Le porteur de certificats CPS, et de la carte CPS correspondante, est responsable de l'utilisation des bi-clés associés aux seules fins pour lesquelles ces bi-clés sont générés. A ce titre, il est tenu de :

- respecter les exigences et recommandations du présent document ;
- respecter les règles d'usage définies dans le présent document qui correspondent au type et à la classe du certificat concerné ;
- s'engager quant à la sincérité des informations fournies lors de sa demande initiale ou de renouvellement de ses certificats et de sa carte ;
- respecter les conditions d'utilisation de ses certificats et de sa carte portées à sa connaissance ;
- informer les Autorités Compétentes de toute évolution concernant les informations figurant dans ses certificats et/ou dans sa carte ;



Autres problématiques métiers et légales

- protéger ses secrets, notamment le code porteur et le code de déblocage de sa carte ;
- informer immédiatement le service de gestion des révocations de l'IGC "CPS", dont les coordonnées sont données dans le formulaire d'abonnement et sont rappelées sur le site Web du GIP "CPS", en cas de perte ou de vol de sa carte CPS pour que celle-ci soit mise en opposition et que les certificats associés soient révoqués.

9.6.4 *Accepteurs de certificats*

Les accepteurs de certificats doivent :

- respecter les règles d'usage définies dans les présentes PC qui correspondent au type et à la classe du certificat concerné ;
- vérifier l'authenticité du certificat traité ;
- vérifier que le certificat n'est pas expiré ;
- vérifier la validité du certificat par rapport à la LCR (état du certificat dans la LCR et validité de la LCR) avec la fréquence qu'ils jugent adaptée aux garanties qu'ils souhaitent ;
- respecter les exigences et recommandations des présentes PC.

Les accepteurs de certificats sont responsables des vérifications qu'ils effectuent sur l'authenticité et la validité du certificat.

9.6.5 *Autres participants*

Les Autorités Compétentes garantissent que les informations qu'ils fournissent à l'IGC "CPS" sont exactes et sont bien validées suivant les procédures internes qui leur sont propres.

9.7 Limite de garantie

N/A

9.8 Limite de responsabilité

Le GIP "CPS", en tant que PSC, décline toute responsabilité vis à vis de l'utilisation, dans des conditions autres que celles prévues par les présentes PC, des certificats qu'il émet à des fins de signature ou d'authentification, ainsi que des clés privées associées. Il décline



Autres problématiques métiers et légales

notamment sa responsabilité pour tout dommage résultant d'un emploi de la Carte de Professionnel de Santé pour un usage (tel qu'engagement de payer) autre que ceux prévus dans le "protocole d'usage de la carte" ([PUC_CPS]) signé par le professionnel de santé, comme pour tout dommage résultant d'actes délictueux dans la commission desquels serait intervenue l'utilisation de la carte.

Le GIP "CPS", en tant que PSC, décline également sa responsabilité pour tout dommage résultant des erreurs ou inexactitudes entachant les informations contenues dans la Carte de Professionnel de Santé, lorsque ces erreurs ou inexactitudes résultent directement du caractère erroné des informations qui lui ont été transmises et confirmées par les Autorités Compétentes ou les mandataires de certification.

9.9 Indemnités

N/A

9.10 Durée et fin anticipée de validité de la PC

9.10.1 *Durée de validité*

Ces PC restent en application jusqu'à la fin de vie du dernier certificat émis au titre de la PC considérée.

9.10.2 *Fin anticipée de validité*

La cessation d'activité de l'IGC "CPS", programmée ou suite à sinistre, entraîne la fin de validité des présentes PC.

9.10.3 *Effets de la fin de validité et clauses restant applicables*

La fin de validité des présentes PC rend caduques les engagements du GIP "CPS" qui y sont portés, à l'exception des clauses traitant de la fin de vie de l'IGC, de l'archivage et du transfert d'activité.



9.11 Notifications individuelles et communications entre les participants

N/A

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

Ces PC sont revues régulièrement pour assurer leur conformité aux normes de sécurité et à l'évolution des mises en œuvre du marché.

Les évolutions sont classées en deux catégories :

- les évolutions mineures, qui ne modifient ni les engagements ni le contenu des services et prestations définis dans ces PC (il s'agit des modifications de forme, des corrections de fautes d'orthographe, etc.) ;
- les évolutions majeures, qui modifient les engagements et/ou les services et prestations définis dans ces PC.

Chaque version est identifiée par un numéro sous la forme "V.RR" où V est le numéro de version principale et RR le numéro de version secondaire. Une évolution mineure entraîne une incrémentation du numéro de version secondaire et une évolution majeure une incrémentation du numéro de version principale.

A noter que le numéro de version principale (V) se retrouve dans l'OID de chaque PC (cf. chapitre 1.2).

Toute évolution doit être approuvée par la Direction du GIP "CPS" en Comité de Direction, après avis de ce dernier. Le compte-rendu de la réunion du Comité de Direction au cours de laquelle l'évolution est approuvée doit préciser le numéro de version du document et la date correspondante.

9.12.2 Mécanisme et période d'information sur les amendements

Toute nouvelle version est disponible en format électronique sur le site Internet du GIP "CPS" dès son approbation par la Direction du GIP "CPS", à l'adresse URL suivante : <http://www.gip-cps.fr>.

Elle prend effet dès sa publication.



9.12.3 Circonstances selon lesquelles l'OID doit être changé

Toute évolution majeure entraîne une évolution du numéro de version principale et, donc, une modification de l'OID.

9.13 Dispositions concernant la résolution de conflits

Le GIP "CPS" s'engage à essayer de résoudre à l'amiable tout litige qui surviendrait concernant ses services, selon la démarche décrite ci-dessous. Afin d'éviter toutes situations de blocage en cours d'exécution des prestations, les parties s'engagent à mettre en œuvre, en cas de litige, de contestation ou de difficulté, la procédure amiable suivante, et ce, préalablement à toute procédure judiciaire.

Désignation d'un Expert

La volonté de saisir un expert sera notifiée par la partie la plus diligente à l'autre partie par lettre recommandée avec avis d'accusé de réception. A compter de la réception de ladite lettre, les parties disposent d'un délai de quinze jours afin de procéder, d'un commun accord, à la désignation d'un expert amiable. A défaut d'accord dans le délai précité de quinze jours, il est fait attribution de compétence auprès du Tribunal Administratif de Paris.

Mission de l'Expert

L'expert désigné a pour mission de tenter de concilier les parties et ce, dans un délai de deux mois à compter de sa saisine. Les parties pourront décider, d'un commun accord, de prolonger ce délai de deux mois, si elles l'estiment nécessaire. L'expert exprimera sa position dans le cadre d'un rapport d'expertise, qui conservera en tout état de cause un caractère strictement confidentiel et ne pourra être produit qu'entre les parties et pour les besoins exclusifs de la procédure d'expertise amiable.

Le financement de l'intervention de l'expert sera convenu dans le cadre de la mission d'expertise attribuée à l'expert.

Les parties s'attacheront à se conformer à la position qui sera exprimée par l'expert.

En cas de conciliation, les parties signeront, s'il y a lieu, un accord transactionnel qui devra préciser si l'ensemble contractuel liant les parties continue à s'appliquer.

A défaut d'accord amiable entre les parties, l'expert établira un procès-verbal de non-conciliation en trois exemplaires datés et signés. Un exemplaire sera remis à chacune des parties. Aucune action contentieuse ne pourra être introduite par l'une ou l'autre des parties, avant l'expiration d'un délai d'un jour franc à compter de la date figurant sur le



procès verbal de non-conciliation. Il est alors fait attribution de compétence auprès du Tribunal Administratif de Paris.

9.14 Juridictions compétentes

Cf. § 9.13.

9.15 Conformité aux législations et réglementations

Le GIP "CPS" se conforme aux législations et réglementations en vigueur.

9.16 Dispositions diverses

9.16.1 Accord global

N/A

9.16.2 Transfert d'activités

Cf. chapitre 5.8 ci-dessus.

9.16.3 Conséquences d'une clause non valide

Au cas où une clause des présentes PC s'avèrerait être non valide au regard de la loi applicable, ceci ne remettrait pas en cause la validité et l'applicabilité des autres clauses.

9.16.4 Application et renonciation

N/A



9.16.5 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français ainsi que toutes autres conventions pouvant lier les parties.

Le GIP "CPS" ne saurait être tenu pour responsable et n'assume aucun engagement pour tout retard dans l'exécution ou pour toute inexécution d'obligations résultant de la présente Politique de Certification lorsque les circonstances qui en sont à l'origine relèvent de la force majeure au sens de l'article 1148 du Code Civil.

9.17 Autres dispositions

N/A



Annexe 1 - Documents de référence

1. Documents de nature juridique

Renvoi	Version	Date	Titre du document / Référence
[ARR_CC]		28/01/1993	Arrêté du 28 janvier 1993 (J.O. du 5 février 1993), modifié par l'Assemblée Générale du 17 décembre 1998, définissant la Convention Constitutive du Groupement d'Intérêt Public « Carte de Professionnel de Santé ».
[ARR_CPS]		09/04/1998	Arrêté du 9 avril 1998 relatif aux spécifications physiques et logiques de la Carte de Professionnel de Santé.
[ARR_Cryp_Aut]		17/03/1999	Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie.
[ARR_QUAL]		31/05/2002	Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation
[DEC_Agr_seq]		24/02/1998	Décret n° 98-102 définissant les conditions dans lesquelles sont agréés les organismes gérant, pour le compte d'autrui, des conventions secrètes de cryptologie.
[DEC_Cat_Decl]		17/03/1999	Décret n° 99-199 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.
[DEC_Cat_Libre]		17/03/1999	Décret n° 99-200 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable.
[DEC_CPS]		09/04/1998	Décret 98-271 relatif à la carte de professionnel de santé et modifiant le code de la sécurité sociale et de la santé publique.
[DEC_Decl_Aut]		24/02/1998	Décret n° 98-101, modifié par le décret n° 2002-688 du 02/05/2002, définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie.
[DEC_Obl_Fourn]		16/07/2002	Décret n° 2002-997 relatif à l'obligation mise à la charge des fournisseurs de prestations de cryptologie.
[DEC_SIGN]]		30/03/2001	Décret n° 2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique



Annexe 1 - Documents de référence

Renvoi	Version	Date	Titre du document / Référence
[DIR_Perso]			Directives du Parlement Européen et du Conseil concernant : - n° 95/46/CE : la protection des données à caractère personnel ; - n° 97/66/CE : le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.
[DIR_SIGN]			Directive 1999/93/CE du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques.
[LOI_Cryp]		29/12/1990 26/07/1996	Article 28 de la loi n° 90-1170 du 29 décembre 1990, modifié par l'article 17 de la loi de réglementation des télécommunications n° 96-659 du 26 juillet 1996.
[LOI_LSQ]		15/11/2001	Articles 30 et 31 de la loi sur la sécurité quotidienne n° 2001-1062 du 15/11/2001
[LOI_SIGN]		13/03/2000	Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
[ORD_Depenses]		24/04/1996	Ordonnance 96-345 relative à la maîtrise médicalisée des dépenses de soins.

2. Documents de nature technique

Renvoi	Version	Date	Titre du document / Référence
[BS7799-2]		05/09/2002	BS7799-2:2002 - Information security management systems - Specification with guidance for use
[CWA14167-1]		06/2003	CEN CWA14167-1 "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements"
[CWA14167-2]		03/2002	CEN CWA14167-2 "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)"
[CWA14167-3]		06/2003	CEN CWA14167-3 "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)"
[ISO17799]		01/12/2000	ISO 17799:2000 - Information technology - Code of practice for information security management
[PC_Type]	3.0	09/2002	Ministère de l'Economie des Finances et de l'Industrie - Politique de Certification Type
[PC2]	2.2	22/01/2001	Commission Interministérielle pour la Sécurité des Systèmes d'Information - Procédures et Politiques de Certification de Clés



Annexe 1 - Documents de référence

Renvoi	Version	Date	Titre du document / Référence
[RFC3039]		01/2001	IETF - RFC3039 - Qualified Certificate Profile
[RFC3280]		04/2002	IETF - RFC3280 - Certificate and Certificate Revocation List (CRL) Profile
[RFC3647]		11/2003	IETF - RFC3647 - Certificate Policy and Certification Practices Framework
[TS101456]	1.2.1	04/2002	ETSI TS 101456 "Policy requirements for certification authorities issuing qualified certificates"
[TS102042]	1.1.1	04/2002	ETSI TS 102042 " Policy requirements for certification authorities issuing public key certificates"
[TS101862]	1.2.1	06/2001	ETSI TS 101862 "Qualified certificate profile"

3. Documents internes GIP "CPS"

[Les versions et dates des documents ci-dessous sont fournies à titre indicatif et sont celles en vigueur au moment de la publication des présentes PC.]

Renvoi	Version	Date	Titre du document / Référence
[ACC_ANN]	1.6	16/10/003	Charte d'accès à l'annuaire
[CERT_CPS]	1.4b	30/11/2004	GIP "CPS" - Les certificats X.509 et les CRLs des cartes CPS2ter du système CPS
[KEY_CEREM]		10/09/2004	Key Ceremony
[PC_ACR-PRO]	1.00	11/10/2004	GIP "CPS" - Politique de Certification de l'Autorité de Certification Racine "Professionnel"
[PUC_CPS]		01/03/2004	GIP "CPS" - Protocoles d'usage de la CPS