POLITIQUES DE CERTIFICATION DE L'IGC "CPS"

Autorités de Certification Racines

Statut[1]	:	Document Final
Version	:	1.00
Date mise à jour	:	04/10/2004
Date prise d'effet	:	11/10/2004
Référence	:	GIP-CPS_PC_RACINES
Diffusion[2]	:	Libre

[1] Document de Travail / Document Final
[2] Libre / Restreinte / Confidentielle

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

Sommaire

Sommaire

Sommaire

1. Introduction

1.1 Présentation générale

Ce document constitue les Politiques de Certification (PC) des Autorités de Certification Racines (ACR) de l'Infrastructure de Gestion de Clés du GIP "CPS" (IGC "CPS") (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].

« 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 gestion de ses AC Racines et des certificats sous la responsabilité de ces ACR, à savoir les propres certificats des ACR et les certificats des AC Intermédiaires (ACI) rattachées à ces ACR, ceci tout au long du cycle de vie de ces certificats.

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.).

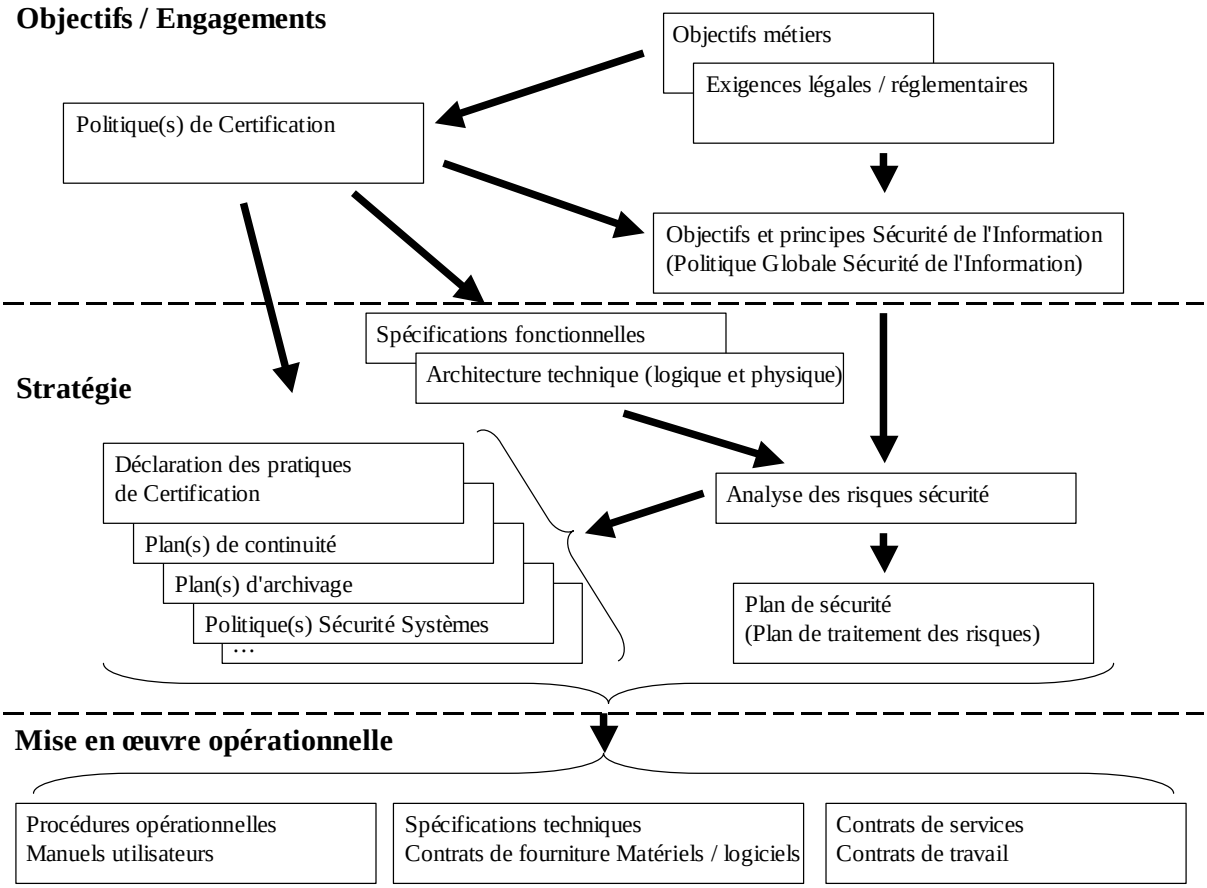
Les objectifs et les engagements du GIP "CPS" concernant les différents aspects du cycle de vie des certificats gérés par l'IGC sont regroupés dans les politiques de certification. Les présentes PC ne portent que sur les certificats des AC (racines et intermédiaires); les certificats des utilisateurs finaux 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 :



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 différentes ACR de l'IGC "CPS", le présent document rassemble les PC de toutes ces ACR, à savoir :

- AC Racine "Anonyme"
- AC Racine "Professionnel"
- AC Racine "Structure"
- AC Racine "Serveur"

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

	ACR ANONYME	ACR PROFESSIONNEL	ACR STRUCTURE	ACR SERVEUR
Nom	Politique de Certification de l'Autorité de Certification Racine "Anonyme"	Politique de Certification de l'Autorité de Certification Racine "Professionnel"	Politique de Certification de l'Autorité de Certification Racine "Structure"	Politique de Certification de l'Autorité de Certification Racine "Serveur"
Réf.	GIP-CPS_PC-RACINE_ANONYME	GIP-CPS_PC-RACINE_PROFESSIONNEL	GIP-CPS_PC-RACINE_STRUCTURE	GIP-CPS_PC-RACINE_SERVEUR
OID	{iso(1) member-body(2) france(250) type-org(1) gip-cps(71) icp(3) doc(7) PC2004-Exploit(8) PC-Anonyme(0) AC-Racine(0) Clé-AC(0) 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) AC-Racine(0) Clé-AC(0) Version-PC(1)}	{iso(1) member-body(2) france(250) type-org(1) gip-cps(71) icp(3) doc(7) PC2004-Exploit(8) PC-Structure(2) AC-Racine(0) Clé-AC(0) Version-PC(1)}	{iso(1) member-body(2) france(250) type-org(1) gip-cps(71) icp(3) doc(7) PC2004-Exploit(8) PC-Serveur(3) AC-Racine(0) Clé-AC(0) Version-PC(1)}

Les exigences et les engagements définis dans le présent document s'appliquent à l'ensemble des ACR de l'IGC "CPS", sauf mention explicite contraire. Dans le cas où un paragraphe ne s'applique qu'à une des ACR, il est précédé du nom de l'ACR entre crochets (par exemple [ANONYME] désigne un paragraphe ne s'appliquant qu'à l'ACR "Anonyme").

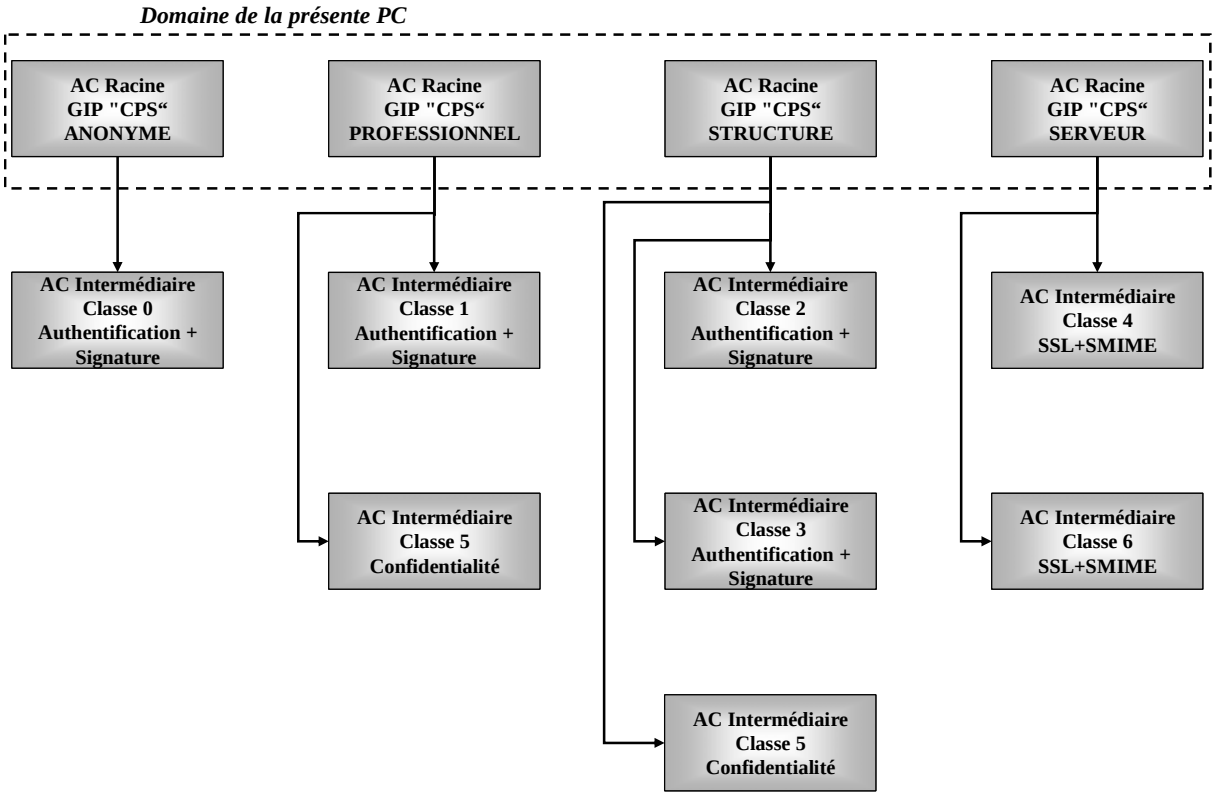
1.3 Entités intervenant dans l'IGC

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]).

Les présentes PC couvrent les 4 ACR de l'IGC "CPS" (cf. schéma ci-dessous).



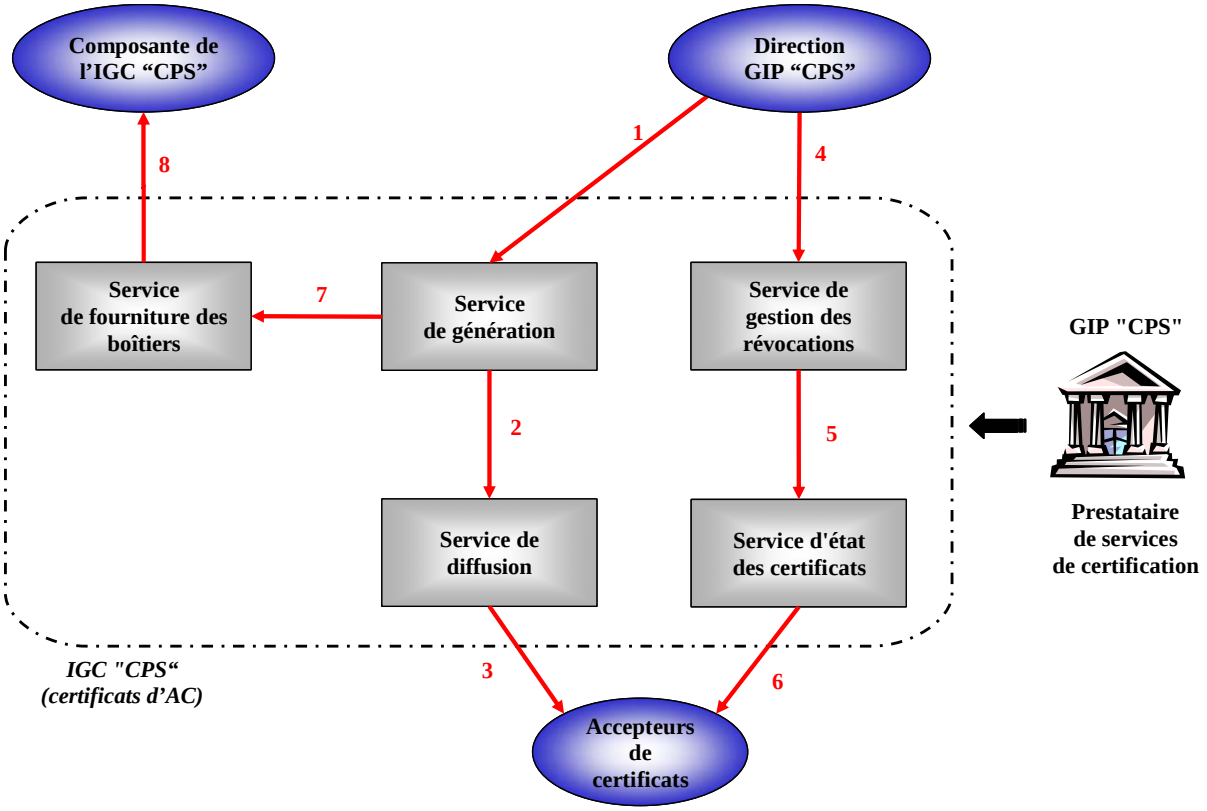
Afin d'assurer sa mission de gestion des certificats et des cartes CPS, l'IGC "CPS" est constituée de différents services fonctionnels (cf. [TS102042] et [TS101456]). Le terme "service" tel qu'utilisé ici correspond bien à la notion de service fonctionnel et non pas de service au sens d'un département 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 d'AC, objet du présent document.

Service	Définition / Commentaires
Service d'enregistrement	Concernant uniquement des certificats d'AC, il n'y a pas de processus d'enregistrement ni de service d'enregistrement. La création d'une nouvelle AC (racine ou intermédiaire) fait l'objet d'une décision formelle prise par la Direction du GIP "CPS", qui définit le nom de l'AC et la PC correspondante (domaine d'application, exigences de gestion et de sécurité, etc.).

Service	Définition / Commentaires
Service de fourniture des boîtiers cryptographiques	Les clés d'AC sont générées et mises en oeuvre dans des boîtiers cryptographiques qui peuvent être différents (la génération se fait dans un boîtier, la mise en oeuvre dans un ou plusieurs autres boîtiers attachés aux unités de personnalisation des cartes CPS, aux serveurs de génération de certificats, aux serveurs de génération des LCR, etc.). Ce service a en charge, à partir des éléments cryptographiques fournis par le service de génération, la préparation des boîtiers cryptographiques et leur diffusion aux composantes concernées de l'IGC "CPS" pour mise en oeuvre.
Service de génération des clés et des certificats	Ce service génère les bi-clés des AC et les certificats correspondants, à la demande de la Direction du GIP "CPS" (génération des clés, création du format de certificat, signature électronique avec la clé privée de l'AC émettrice). Les clés et les certificats d'AC sont générés au cours de "cérémonies de clés". Ce service a également en charge la conservation sécurisée des clés d'ACR et d'ACI.
Service de diffusion	Ce service met à disposition des porteurs et des accepteurs de certificats : - les certificats d'AC produits, - les informations d'accès et d'utilisation des certificats (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 accepteurs de certificats des informations sur l'état des certificats (valides ou révoqués).

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



(1) La Direction du GIP "CPS" décide de la génération d'une nouvelle clé et du certificat correspondant d'une ACR et/ou d'une ACI. Elle transmet l'ordre de génération au service de génération.

(2) Le service de génération génère les bi-clés et les certificats correspondants. Il transmet les certificats au service de diffusion et conserve les clés privées.

(3) Le service de diffusion met les certificats à disposition des accepteurs de certificats via un annuaire. 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.

(4) En cas de besoin, les demandes de révocation sont transmises au service de gestion des révocations par la Direction du GIP "CPS".

(5) 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.

(6) Le service d'état des certificats fournit aux accepteurs de certificats les informations concernant l'état des certificats via des listes de certificats révoqués.

(7) Lorsque des boîtiers cryptographiques doivent être préparés ou mis à jour, le service de génération transmet les clés privées d'AC concernées (clés de signature

de certificats ou clés de signature de LCR) au service de fourniture qui personnalise le ou les boîtiers.

(8) Une fois le ou les boîtiers personnalisés, ils sont transmis à la composante de l'IGC "CPS" chargée de les mettre en oeuvre, ainsi que les codes d'activation.

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 des différentes autorités de certification de la hiérarchie; conserve de manière sécurisée les clés privés des ACR (en cas de création de nouvelles ACI) et des ACI (en cas de préparation de nouveaux boîtiers); diffuse les certificats d'AC aux utilisateurs ;
- prépare les boîtiers cryptographiques requis par les composantes de l'IGC "CPS" chargées de leur mise en oeuvre; remet de manière sécurisée chaque boîtier et les codes d'activation correspondant à la composante concernée ;
- 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

N/A (cf. chapitre 1.3.1).

1.3.3 Porteurs de certificats

Dans le cas des présentes PC, portant sur les ACR de l'IGC "CPS", les porteurs de certificats sont en fait les ACI.

Afin d'assurer une cohérence entre les différents documents de l'IGC "CPS", le terme "porteur de certificats" est réservé aux utilisateurs finaux détenteurs d'une carte CPS et/ou de certificats CPS.

Dans la suite du présent document, le terme "Autorité de Certification Intermédiaire" (ACI) sera donc utilisé pour désigner les entités disposant de certificats fournis par une des ACR.

1.3.4 Accepteurs de certificats

Les accepteurs de certificats sont les personnes et les entités qui sont amenées à s'appuyer sur un certificat CPS (pour authentifier un porteur d'une carte CPS, vérifier une signature électronique générée à l'aide d'une carte CPS, chiffrer un message à destination d'un porteur d'un certificat CPS, etc.) et ainsi à vérifier l'ensemble de la chaîne de certificats, du certificat du porteur au certificat de l'ACR correspondante.

Un accepteur de certificats peut être lui-même porteur de certificats CPS (cas, par exemple, d'échange d'un message électronique signé entre deux PS) ou ne pas être porteur de tels certificats 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).

1.3.5 Autres participants

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

1.4 Usage des certificats

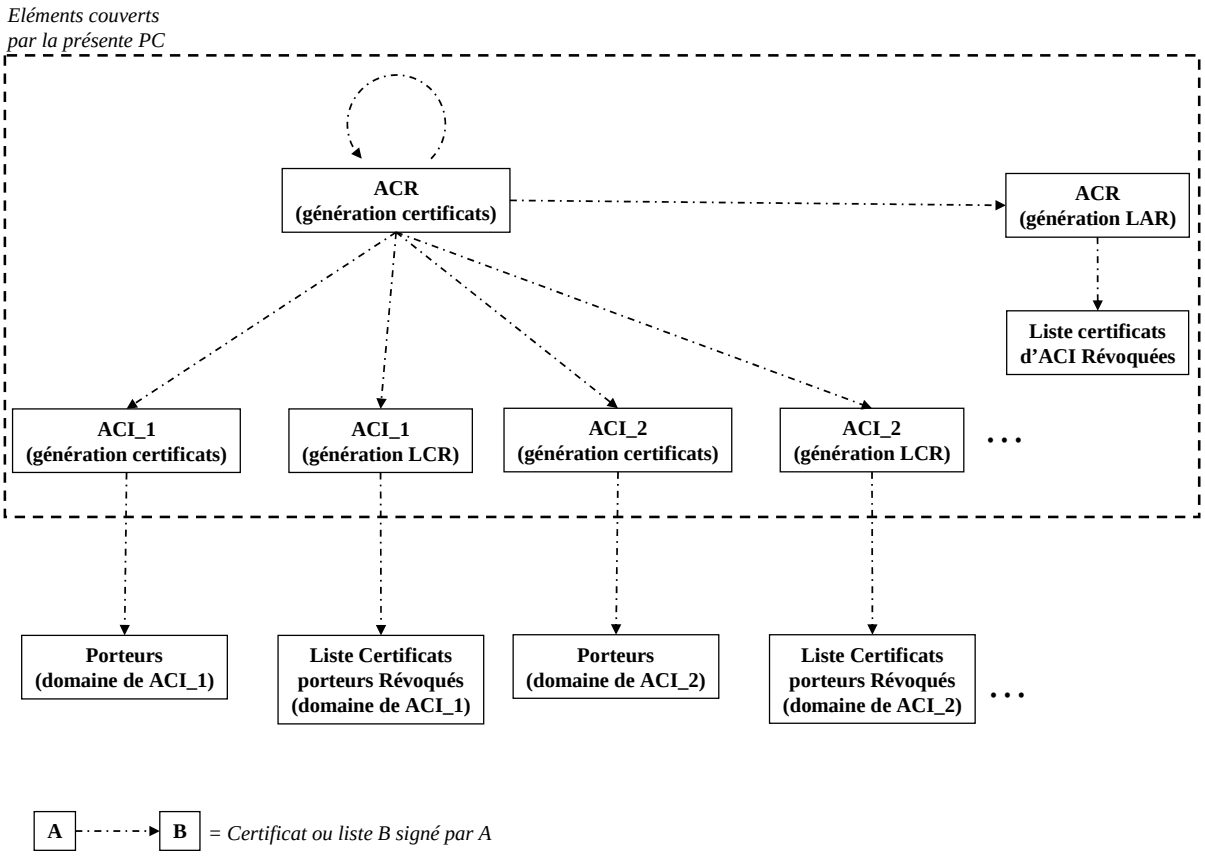
1.4.1 Domaines d'utilisation applicables

Pour chacune des PC correspondant à chacune des ACR de l'IGC "CPS", le présent document couvre les certificats suivants (cf. [CERT_CPS]) :

- le certificat de l'ACR (certificat autosigné), utilisé pour signer les certificats de la hiérarchie d'AC (certificats des AC intermédiaires, certificat de signature de la Liste des certificats d'AC révoquées (LAR), certificats de signature des Listes de Certificats porteurs Révoqués (LCR)) ;
- le certificat de signature de la Liste des certificats d'AC Révoqués (LAR) des ACI rattachées à l'ACR (certificat signé par l'AC Racine) ;

- ☞ les certificats des AC intermédiaires rattachées à l'ACR (certificats signés par l'ACR) ;
- ☞ les certificats de signature des Listes des Certificats porteurs Révoqués des porteurs pour chacune des ACI rattachées à l'ACR (certificats signés par l'AC Racine) ;

Le schéma ci-dessous présente le positionnement de ces différents certificats pour une ACR :



Chaque AC dispose donc de deux bi-clés et de deux certificats correspondants : un bi-clé pour la génération des certificats et un bi-clé pour la génération des listes de révocation (LAR ou LCR).

Dans la suite du présent document, ces différents certificats sont regroupés sous les dénominations suivantes :

- **Bi-clé et certificat d'ACR** - Il s'agit du bi-clé de l'ACR et du certificat autosigné correspondant utilisé par l'ACR pour générer les certificats des entités rattachées à l'ACR.
- **Bi-clés et certificats d'ACI** - Il s'agit de tous les certificats (et des bi-clés correspondants) signés par l'AC Racine (autre que son propre certificat autosigné),

à savoir : les certificats des ACI pour la génération des certificats porteurs, les certificats des ACI pour la génération des LCR, le certificat de l'ACR pour la génération des LAR. Lorsque du texte s'applique à la fois aux ACR et aux ACI, la dénomination "certificats d'AC" est également utilisée.

Sauf mention explicite contraire, les engagements et les exigences identifiés dans la suite du présent document s'appliquent à l'ensemble de ces types de bi-clés et de certificats.

1.4.2 Domaines d'utilisation interdits

Toute autre utilisation des bi-clés et des certificats objet des présentes PC que les utilisations prévues dans le cadre du présent document est interdite. En cas de non respect de cette interdiction par une entité extérieure à l'IGC "CPS", 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 des 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 la présente PC sont les suivants :

AC	Autorité de Certification
CC	Critères Communs
CDE	Carte de Directeur d'Etablissemement
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.
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
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 la présente 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 d'une des 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 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 et la mise en oeuvre des clés d'AC.

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.

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.

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 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.

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.

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 2.3 ci-dessous.

2.2 Informations devant être publiées

Au titre des présentes PC, 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 de la présente PC (cf. [CERT_CPS]) ;
- ☞ les certificats des AC Racines et les certificats des AC Intermédiaires.

Via l'annuaire du GIP "CPS" :

- ☞ les certificats valides (non révoqués, non expirés) des AC Racines et Intermédiaires ;
- ☞ les certificats valides (non révoqués, non expirés) de signature des LCR ;
- ☞ les LAR[1].

D'autres informations liées au certificats porteurs sont également diffusées (certificats des porteurs, LCR, 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 :

- o les certificats des AC (racines et intermédiaires) sont diffusés dans l'heure suivant leur génération ;
- o les LAR 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]).

[1] A noter que l'IGC "CPS" ne produit pas de delta-LAR

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 X.509 d'AC (racines et intermédiaires), le champ "issuer" (AC émettrice) et le champ "subject" (AC certifiée) correspondent à un Distinguished Name (DN). Ce DN est construit conformément au document [CERT_CPS].

3.1.2 Nécessité d'utilisation de noms explicites

Les noms utilisés dans les champs "issuer" et "subject" d'un certificat d'AC sont explicites dans le domaine santé-social.

3.1.3 Anonymisation ou pseudonymisation des porteurs

N/A pour des certificats d'AC.

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 d'ACR et d'ACI, le DN du champ "issuer" (AC émettrice) et du champ "subject" (AC certifiée) 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 d'AC et les certificats correspondants sont générés lors de cérémonies de clés (cf. chapitre 4).

3.2.2 Validation de l'identité d'un organisme

Pour les certificats d'ACR et d'ACI, l'identité est définie préalablement et validée par la Direction du GIP "CPS".

3.2.3 Validation de l'identité d'un individu

N/A.

3.2.4 Informations non vérifiées du porteur

N/A.

3.2.5 Validation de l'autorité du demandeur

Les cérémonies de génération des clés et certificats d'AC se font en présence d'au moins un membre de la Direction du GIP "CPS", seule apte à demander la génération de tels clés et certificats.

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

Le renouvellement courant des clés et certificats d'ACR et d'ACI s'effectue au cours de cérémonies de clés suite à validation préalable par la Direction du GIP "CPS".

3.3.2 Identification et validation pour un renouvellement des clés après révocation

Le renouvellement, suite à révocation, des clés et certificats d'ACR et d'ACI s'effectue au cours de cérémonies de clés suite à validation préalable par la Direction du GIP "CPS".

3.4 Identification et validation d'une demande de révocation

Pour les certificats d'ACR et d'ACI, toute révocation doit être préalablement et formellement validée par la Direction du GIP "CPS".

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Pour les certificats d'ACR et d'ACI, les demandes sont préalablement et formellement validées par la Direction du GIP "CPS", seule apte à le faire.

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

Pour les certificats d'ACR et d'ACI, l'enregistrement est sous la responsabilité de la Direction du GIP "CPS".

4.2 Traitement d'une demande de certificat

Suite à demande de génération formulée par la Direction du GIP "CPS", le service de génération organise la ou les cérémonies de clés correspondantes (scripts, convocation des témoins, préparation des matériels et logiciels, etc.).

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Les bi-clés et les certificats d'ACR et d'ACI sont générés au cours de cérémonies de clés, suivant des scripts pré-définis (cf. chapitre 4.2) et en présence de témoins, internes et externes au GIP "CPS", attestant du déroulement effectif de chaque cérémonie par rapport au script correspondant.

La cérémonie pendant laquelle sont générés et remis à leurs titulaires les "secrets d'IGC" est placée sous le contrôle d'un huissier de justice qui en dresse le constat.

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

N/A.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

N/A.

4.4.2 Publication du certificat

Les certificats d'ACR et d'ACI sont publiés dans un annuaire X500, qui peut être consulté en mode LDAP ou HTTP à l'adresse *annuaire.gip-cps.fr*, et sur le serveur Web du GIP "CPS" à l'adresse *www.gip-cps.fr*.

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

Le service de fourniture des boîtiers assure la gestion et la traçabilité de tous les boîtiers cryptographiques de l'IGC "CPS". Il tient informées les entités concernées, notamment le Responsable de la Sécurité des Systèmes d'Information du GIP "CPS".

4.5 Usages du bi-clés et du certificat

4.5.1 Utilisation de la clé privée et du certificat par l'ACI

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

L'utilisation par les ACI de leurs bi-clés et de leurs certificats de signature de certificats est réservée à la génération des certificats porteurs.
L'utilisation par les ACI de leurs bi-clés et de leurs certificats de signature de listes de révocation est réservée à la génération des LCR et LAR.

L'utilisation d'une clé privée n'est autorisée que pendant la période de validité du certificat associé.

Une clé privée d'AC ne se trouve sous forme déchiffrée et ne peut être mis en oeuvre qu'à l'intérieur d'un boîtier cryptographique sécurisé (cf. chapitre 6.2).

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 la présente PC (cf. § 1.4) et à l'usage prévu indiqué dans le certificat (attributs *key usage* et *extended key usage*).

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 d'ACR ou d'ACI sans renouvellement du bi-clé correspondant est impossible. Une demande de renouvellement entraîne donc automatiquement la génération d'un nouveau bi-clé (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

4.7.1 Causes possibles de changement d'un bi-clé

La durée de validité d'un bi-clé d'AC est égale à la durée de validité du certificat correspondant.

La cause principale de la génération d'un nouveau bi-clé et du certificat correspondant est l'arrivée à la date de fin de validité du certificat.

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 notamment la révocation d'un certificat d'AC (cf. chapitre 4.9).

4.7.2 Origine d'une demande d'un nouveau certificat

Pour les certificats d'ACR et d'ACI, les demandes de renouvellement sont préalablement et formellement validées par la Direction du GIP "CPS", seule apte à le faire.

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

Le traitement d'un renouvellement de bi-clés et de certificats d'AC est le même que pour une demande initiale : cf. chapitre 4.2).

4.7.4 Notification au porteur de l'établissement du nouveau certificat

Le service de fourniture des boîtiers se charge de mettre à jour les boîtiers opérationnels concernés par le nouveau bi-clé et le nouveau certificat.

4.7.5 Démarche d'acceptation du nouveau certificat

N/A.

4.7.6 Publication du nouveau certificat

L'annuaire de publication des certificats et le serveur Web du GIP "CPS" sont mis à jour avec le nouveau certificat.

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

Cf. chapitre 4.4.3.

4.8 Modification du certificat

Un certificat d'ACR ou d'ACI ne peut pas faire l'objet de modification.

4.9 Révocation et suspension des certificats

Il n'a pas de suspension possible de certificat. Seule la révocation définitive des certificats peut être réalisée.

4.9.1 Causes possibles d'une révocation

Certificat d'une AC racine de l'IGC "CPS" :

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

- compromission ou suspicion de compromission de la clé privée correspondante ou des éléments secrets protégeant cette clé hors des boîtiers cryptographiques ;
- perte ou vol d'un boîtier cryptographique contenant les éléments secrets mentionnés à l'alinéa précédent ;
- cessation d'activité de l'AC racine ;
- par anticipation par exemple : en cas de risque de mise en péril de l'IGC "CPS" suite à l'apparition d'une faiblesse au niveau des algorithmes ou des clés utilisés.

Certificat d'AC intermédiaire :

A chaque classe de certificats porteur correspond un certificat d'AC intermédiaire, lui-même signé par la clé privée d'une AC racine de l'IGC "CPS".

Les circonstances qui peuvent être à l'origine de la révocation d'un tel certificat sont les suivantes :

- révocation du certificat de l'ACR correspondante ;
- compromission ou suspicion de compromission de la clé privée de cette ACI ou des éléments secrets protégeant cette clé hors des boîtiers cryptographiques ;
- perte ou vol d'un boîtier cryptographique contenant les éléments secrets mentionnés à l'alinéa précédent ;
- par anticipation par exemple : en cas de risque de mise en péril de l'IGC "CPS" suite à l'apparition d'une faiblesse au niveau de l'algorithme ou des clés utilisés.

Les causes de révocation ne sont jamais publiées dans les LAR.

4.9.2 Origine d'une demande de révocation

Seule la Direction du GIP "CPS" peut demander la révocation d'un certificat d'ACR ou d'ACI.

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 :

- pour les certificats révoqués d'ACI, d'ajouter les n° de série de ces certificats dans les prochaines LAR à générer et publier,
- pour les certificats révoqués d'ACR et d'ACI, les retirer de l'annuaire et du serveur Web et informer explicitement sur le serveur Web de la révocation du ou des certificats concernés.

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 décision de révocation par la Direction du GIP "CPS", 7 jours / 7 (week-ends et jours fériés compris).

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 d'AC sur lesquels ils vont baser leur confiance. Cette vérification se fait en consultant, pour les certificats d'ACI, les LAR disponibles via l'annuaire (annuaire.gip-cps.fr) et, pour les certificats d'ACR, l'annuaire (présence des certificats dans l'annuaire) et/ou le site Web du GIP "CPS".

4.9.7 Fréquence d'établissement des LAR

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

Par mesure de sécurité, les LAR ont une durée de validité de 2 jours ouvrés.

4.9.8 Délai maximum de publication d'une LAR

Le délai maximum entre les publications de deux LAR 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 mécanisme de LAR 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

La révocation de certificats d'AC fait l'objet, en plus de la LAR, d'une information diffusée au moins sur le site Web du GIP "CPS" et éventuellement relayée par d'autres sites administratifs ou professionnels, ainsi que sur appel au numéro indigo du GIP "CPS" (cf. le numéro d'appel sur le serveur Web du GIP "CPS").

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

N/A.

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 LAR qui peuvent être téléchargées en mode LDAP à l'adresse :

ldap://annuaire.gip-cps.fr/c=fr,o=gip-cps,ou=gip-cps X

où X représente le nom de l'ACR (ANONYME, PROFESSIONNEL, STRUCTURE ou SERVEUR).

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

N/A.

4.12 Séquestre de clé et recouvrement

N/A.

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, 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,
- 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 ;

- 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 évènements qui la concernent.

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

Les évènements journalisés se décomposent en deux grandes catégories :

- les évènements relatifs aux services de l'IGC (génération des éléments cryptographiques, personnalisation des boîtiers, etc.) ;
- les évènements 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'évènements ;

La DPC précise les évènements 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'évènements 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'évènements

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

5.4.6 Système de collecte des journaux d'évènements

La collecte des journaux d'évènements 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'évènements 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, la DPC et les scripts de cérémonies de clés certifiés par les témoins.

Sont archivées les certificats et les LAR, ainsi que 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

Chaque PC et les scripts de cérémonies de clés correspondants sont conservés pendant trente ans à compter de la validation d'une nouvelle version, ou la fin de validité du dernier certificat produit au titre de la PC considérée.

La DPC est conservée pendant cinq ans après entrée en vigueur d'une nouvelle version ou expiration du dernier certificat émis au titre de la DPC.

Les certificats d'AC, ainsi que les LAR produites par les ACR, 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

Une ACR ne peut pas générer de certificat d'ACI dont la date de fin serait postérieure à la date d'expiration du bi-clé d'ACR.

De ce fait, la période de validité de ces derniers certificats est supérieure à celle des certificats des ACI, et la conséquence en est nécessairement un chevauchement des périodes de validité des certificats d'ACR.

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

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 stipulées dans les présentes PC.

En outre, le GIP "CPS" s'engage à :

- communiquer dans un délai de 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 LAR émises ;
- remettre ses archives ainsi que l'ensemble des données dont il dispose à une entité fiable.

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

Les bi-clés d'ACR et d'ACI sont générés dans des boîtiers cryptographiques sécurisés au cours de "cérémonies de clés" (cf. chapitre 4.3.1). Les boîtiers cryptographiques assurent également la génération des certificats correspondants.

Les clés privées sont conservées de manière sécurisée par le service de génération, afin d'en empêcher leur compromission.

6.1.2 Transmission de la clé privée à son propriétaire

Lorsqu'une composante de l'IGC "CPS" a besoin d'un boîtier cryptographique pour la mise en oeuvre de ses fonctions (par exemple, la génération des LCR), le service de fourniture des boîtiers prépare le boîtier, en y chargeant notamment, de manière sécurisée, les clés privées d'AC requises pour la fonction considérée (par exemple, les clés privées des ACI pour la génération des LCR), puis délivre le boîtier à la composante concernée, suivant une procédure sécurisée assurant la traçabilité.

6.1.3 Transmission de la clé publique à l'AC

N/A.

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

Les clés publiques des ACR et des ACI sont diffusées par le biais de leurs certificats respectifs. Ces certificats sont publiés dans l'annuaire "CPS" et également téléchargeables directement sur le site Internet du GIP "CPS" : http://www.gip-cps.fr.

Les empreintes numériques des clés publiques et des certificats autosignés des ACR sont également accessibles sur le même site.

6.1.5 Tailles des clés

Les bi-clés d'ACR et d'ACI utilisent des clés privées RSA de 2048 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

Les bi-clés de signature de certificats sont utilisés à des fins de génération de certificats.

Les bi-clés de signature de LCR sont utilisés à des fins de génération de LCR et LAR.

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 utilisées pour la génération des bi-clés et la fabrication des certificats sont des boîtiers cryptographiques sécurisés (cf. chapitre 6.2.11), conformes à la réglementation et autorisés par la DCSSI.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Dans l'environnement de l'IGC "CPS", l'initialisation d'un boîtier cryptographique et la gestion des clés privées d'ACR ou d'ACI (génération, sauvegarde,...) sont contrôlées via un processus où M parmi N porteurs des "secrets IGC" doivent s'authentifier.

6.2.3 Séquestre de la clé privée

Les clés privées d'AC ne sont en aucun cas séquestrées.

6.2.4 Copie de secours de la clé privée

Les clés privées d'ACR et d'ACI sont sauvegardées chiffrées hors des boîtiers cryptographiques. Elles ne peuvent être déchiffrées qu'à l'intérieur d'un boîtier cryptographique préalablement initialisé (cf. § 6.2.2 ci-dessus et DPC).

6.2.5 Archivage de la clé privée

Les clés privées d'ACR et d'ACI ne sont pas archivées.

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

Cf. chapitres 6.1.1 et 6.1.2.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC sont stockées chiffrées hors des boîtiers cryptographiques et mises en œuvre uniquement au sein des ces boîtiers, sans possibilité de les en faire sortir non chiffrées.

6.2.8 Méthode d'activation de la clé privée

L'activation d'une clé privée d'ACR autosignée n'est requise que lorsqu'il est nécessaire de signer un certificat d'ACI. Ceci nécessite la présence de plusieurs personnes et est réalisé au cours d'une cérémonie de clés en présence de plusieurs témoins.

Les clés privées d'ACI sont mises en oeuvre dans les boîtiers cryptographiques opérationnels des différents serveurs (unités de personnalisation des cartes CPS, serveurs de génération des certificats, serveurs de génération des LCR,...).

L'activation des clés privées d'ACI se fait au travers de l'activation de ces boîtiers cryptographiques. Cette activation requiert la présence de deux personnes distinctes simultanément, chacune ayant un rôle de confiance et étant détentrice d'une partie des données d'activation du boîtiers.

6.2.9 Méthode de désactivation de la clé privée

La désactivation des boîtiers cryptographiques dans lesquels sont mis en oeuvre les clés privées est automatique en fonction de différents évènements qui sont précisés dans la DPC.

6.2.10 Méthode de destruction des clés privées

Les boîtiers cryptographiques disposent de fonctions d'effacement des données sensibles, dont les clés privées.

6.2.11 Niveau d'évaluation sécurité du module cryptographique

Les boîtiers cryptographiques sont évalués au niveau FIPS 140-1 Level 3.

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

Les bi-clés et certificats d'ACR et d'ACI sont valides jusqu'au 31/12/2014.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Pour chaque boîtier cryptographique, les données d'activation sont générées lors de la personnalisation du boîtier et stockées sur cartes à puce protégées par des codes PIN. Ces cartes sont remises aux personnes chargées de l'activation et de la mise en oeuvre du boîtier au sein de la composante concernées de l'IGC (cf. chapitre 6.2.8).

6.4.2 Protection des données d'activation

Les codes PIN des cartes à puce contenant les données d'activation des boîtiers cryptographiques sont des données confidentielles. Chaque détenteur doit en protéger la confidentialité comme il doit également assurer la disponibilité et l'intégrité de sa carte.

6.4.3 Autres aspects liés aux données d'activation

N/A.

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.

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 LAR, les certificats ainsi que les journaux d'événements sont horodatés par les 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 OCSP ne sont pas mis en œuvre par l'IGC "CPS" au titre de la présente 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 la présente 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

N/A

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 secrètes[1] sont au minimum les clés privées des ACR et des ACI, les clés cryptographiques (clés privées et clés secrètes) de gestion des différentes entités de l'IGC "CPS" ainsi que les informations liées à la gestion des boîtiers cryptographiques (codes PIN protégeant les données d'activation, "secrets d'IGC" liés à l'initialisation des boîtiers, etc.).

Les informations considérées comme confidentielles[2] sont au minimum :

- la DPC de l'IGC "CPS" ;
- les journaux d'événements des composantes de l'IGC "CPS" ;
- certaines spécifications des systèmes de sécurité.

9.3.2 Informations hors du périmètre des informations classifiées

Les informations non classifiées sont dites "libres"[3] et peuvent être publiées sans restriction.

---

[1] 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.

[2] 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.

[3] Les informations classées libres sont destinées à une libre circulation.

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 d'AC qui ne sont sous forme déchiffrée qu'à l'intérieur des boîtiers cryptographiques), 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

S'agissant de clés et certificats d'AC, l'ensemble de ce chapitre est non applicable dans le cadre des présentes PC.

9.4.1 Politique de protection des données personnelles

N/A

9.4.2 Informations à caractère personnel

N/A

9.4.3 Informations non à caractère personnel

N/A

9.4.4 Responsabilité en termes de protection des données personnelles

N/A

9.4.5 Notification et consentement d'utilisation des données personnelles

N/A

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

N/A

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 donnée, 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 et ce, au fur et à mesure de leur réalisation.

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 les domaines 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.

9.6.2 Service d'enregistrement

N/A.

9.6.3 Porteurs de certificats

N/A

9.6.4 Accepteurs de certificats

Les accepteurs de certificats doivent :

- respecter les règles d'usage définies dans la présente 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 de la présente 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

N/A

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 au titre de ces PC.

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 d'une des 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 la 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

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 pratice 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

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 de la présente PC.]

Renvoi	Version	Date	Titre du document / Référence
[ACC_ANN]	1.6	16/10/2003	Charte d'accès à l'annuaire
[CERT_CPS]	1.4	17/09/2004	GIP "CPS" - Les certificats X.509 et les CRLs des cartes CPS2ter du système CPS
[PUC_CPS]		01/03/2004	GIP "CPS" - Protocole d'usage de la CPS - Formulaire d'attribution d'une carte CPS / CPF / CPA / CDE / CPE
[KEY_CEREM]		10/09/2004	Key Ceremony