POLITIQUE DE CERTIFICATION

DE

L'INFRASTRUCTURE DE GESTION DE CLÉS

« CARTE DE PROFESSIONNEL DE SANTÉ »

CERTIFICATS DE SERVEURS APPLICATIFS

VERSION 1.3 DU 19.03.2002

Groupement d'Intérêt Public
Carte de Professionnel de Santé
8 bis, rue de Chateaudun 75009 Paris
Tél. : 01.44.53.36.53
Fax : 01.40.16.90.15
e-mail : gip@gip-cps.fr
N° Siret : 180 030 009 00039

AVERTISSEMENT

DE LA VERSION 1.3

Le présent document(*) concerne la Politique de Certification (PC) de l'Infrastructure de Gestion de Clés « CPS » associée aux certificats délivrés à des serveurs applicatifs par le GIP « CPS ».

Le présent document ne concerne :

- ✓ ni les certificats de signature et d'authentification
- ✓ ni les certificats de confidentialité

délivrés à des personnes physiques, et qui font chacun l'objet d'une PC spécifique (cf. [PC_Sign] et [PC_Conf]).

(*) Document approuvé par une délibération du Conseil d'Administration du GIP « CPS » le 19 / 03 / 2002.

SOMMAIRE

1. INTRODUCTION 7

1.1. PRESENTATION GENERALE 7
1.1.1. Objectifs et domaine d'application de la PC 7
1.1.2. Rôle du GIP « CPS » 7
1.1.3. Le Système « CPS », clé de voûte de la sécurité du Système de Santé. 8
1.1.4. Garanties offertes par le GIP « CPS » 8
1.1.5. Types de certificats concernés par la présente PC 8
1.1.6. Classe de certificats concernés par la présente PC 8
1.2. IDENTIFICATION 9
1.3. AUTORITES, APPLICATIONS ET UTILISATEURS CONCERNES PAR LA PRESENTE PC 9
1.3.1. Autorité de Certification 9
1.3.2. Autorité d'Enregistrement 9
1.3.3. Service d'horodatage 10
1.3.4. Service de publication 10
1.3.5. Utilisateurs finaux 10
1.3.6. Types d'applications concernées par la présente PC 10
1.4. POINTS DE CONTACTS 10
1.4.1. Personne à contacter concernant ce document 10

2. DISPOSITIONS D'ORDRE GÉNÉRAL 11

2.1. OBLIGATIONS 11
2.1.1. Obligations communes à toutes les composantes de l'IGC « CPS » 11
2.1.2. Obligations incombant à l'AC 11
2.1.3. Obligations incombant à l'AE 12
2.1.4. Obligations incombant aux serveurs applicatifs 12
2.1.5. Obligations incombant aux accepteurs de certificats 12
2.2. RESPONSABILITES 12
2.2.1. Responsabilité de l'AC 12
2.2.2. Responsabilité de l'AE 12
2.2.3. Responsabilité du service de publication 12
2.2.4. Responsabilités du serveur applicatif 12
2.2.5. Responsabilité de l'accepteur de certificat 13
2.2.6. Limites de responsabilités du GIP « CPS » 13
2.3. INTERPRETATION DE LA LOI 13
2.3.1. Textes applicables 13
2.3.2. Arbitrage des litiges 13
2.4. PUBLICATION ET SERVICES ASSOCIES 13
2.4.1. Informations publiées au sein de l'IGC 13
2.4.2. Fréquence de mise à jour des certificats dans l'annuaire 14
2.4.3. Contrôle d'accès aux certificats dans l'annuaire 14
2.4.4. Responsabilité de la gestion de l'annuaire de l'IGC « CPS » 14
2.5. CONTROLES DE CONFORMITE 14
2.5.1. Fréquence des contrôles de conformité 14
2.5.2. Identité et qualification du contrôleur 14
2.5.3. Sujets couverts par le contrôle de conformité 14
2.5.4. Communication des résultats et mesures à prendre en cas de non-conformité 15
2.6. POLITIQUE DE CONFIDENTIALITE 15
2.6.1. Types d'informations secrètes ou confidentielles 15
2.6.2. Types d'informations sensibles 15
2.6.3. Types d'informations libres 15

2.6.4. Divulgation des causes de révocation *15*
2.7. DROITS SUR LA PROPRIETE INDUSTRIELLE 15

3. IDENTIFICATION ET AUTHENTIFICATION 17

3.1. ENREGISTREMENT INITIAL 17
3.1.1. Convention de noms *17*
3.1.2. Nécessité d'utilisation de noms explicites *18*
3.1.3. Règles d'interprétation des différentes formes de nom *18*
3.1.4. Unicité des noms *19*
3.1.5. Procédure de résolution de litige concernant un nom *19*
3.1.6. Preuve de la possession de la clé privée *19*
3.2. RE-GENERATION DE CERTIFICATS APRES EXPIRATION 19
3.3. RE-GENERATION DE CLES APRES REVOCATION 19
3.4. AUTHENTIFICATION D'UNE DEMANDE DE REVOCATION 19

4. BESOINS OPÉRATIONNELS 20

4.1. DEMANDE DE CERTIFICAT 20
4.1.1. Demande administrative *20*
4.1.2. Demande de certification *20*
4.2. GENERATION DE CERTIFICAT 21
4.3. ACCEPTATION DE CERTIFICAT 22
4.4. REVOCATION ET EXPIRATION DE CERTIFICAT 22
4.4.1. Causes possibles d'une révocation *22*
4.4.2. Origine d'une demande de révocation *23*
4.4.3. Procédure de demande de révocation *23*
4.4.4. Délai de traitement d'une révocation *23*
4.4.5. Fréquence de mise à jour des CRL *23*
4.4.6. Exigences de contrôle des CRL *23*
4.4.7. Publication des causes de révocation *24*
4.4.8. Accès en ligne des CRL *24*
4.4.9. Expiration des certificats *24*
4.5. JOURNALISATION DES EVENEMENTS 24
4.6. ARCHIVES 24
4.6.1. Types de données archivées *24*
4.6.2. Période de rétention des archives *24*
4.6.3. Protection des archives *25*
4.6.4. Procédures de copie / backup des archives *25*
4.6.5. Besoin d'horodatage des enregistrements d'archives *25*
4.6.6. Système de collecte des archives (interne ou externe) *25*
4.6.7. Procédures d'accès / de récupération des archives *25*
4.7. CHANGEMENT DE CLE D'UNE COMPOSANTE 25
4.8. COMPROMISSION ET PLAN ANTI-SINISTRE 25
4.8.1. En cas de corruption des ressources informatiques (logiciels ou données) *25*
4.8.2. En cas de révocation du certificat d'une composante de l'IGC *25*
4.8.3. Mesures de sécurité après un sinistre *26*
4.9. FIN DE VIE DE L'AC « CPS » 26

5. CONTRÔLES DE SÉCURITÉ PHYSIQUE, DES PROCÉDURES ET DU PERSONNEL 27

5.1. CONTROLES DE SECURITE PHYSIQUE 27
5.1.1. Situation géographique et construction des sites *27*
5.1.2. Accès physique *27*
5.1.3. Alimentation électrique et climatisation *27*
5.1.4. Vulnérabilité aux dégâts des eaux *27*
5.1.5. Prévention et protection contre le feu *27*

5.1.6. Conservation des médias *27*
5.1.7. Destruction des données *27*
5.1.8. Site(s) de secours *27*
5.2. CONTROLES DES PROCEDURES 28
5.2.1. Rôles de confiance *28*
5.2.2. Nombre de personnes requises par tâche *28*
5.2.3. Identification et authentification pour chaque rôle *28*
5.3. CONTROLES DU PERSONNEL 28
5.3.1. Compétences, qualification et antécédents requis *28*
5.3.2. Exigences et fréquence en matière de formation *29*
5.3.3. Gestion des métiers *29*
5.3.4. Sanctions appliquées en cas d'actions non autorisées *29*
5.3.5. Contrôle du personnel contractant *29*
5.3.6. Documentation fournie au personnel *29*

6. CONTRÔLES TECHNIQUES DE SÉCURITÉ 30

6.1. GENERATION ET INSTALLATION DE BI-CLES 30
6.1.1. Génération de bi-clés *30*
6.1.2. Transmission de la clé privée à son propriétaire *30*
6.1.3. Transmission de la clé publique à l'AC *30*
6.1.4. Transmission de clé publique de l'AC aux utilisateurs *30*
6.1.5. Algorithme et tailles des clés *30*
6.1.6. Génération des paramètres de clé publique *30*
6.1.7. Contrôle de qualité des paramètres de clés *30*
6.1.8. Mode de génération de clé (matérielle ou logiciel) *30*
6.1.9. Usage de la clé *31*
6.2. PROTECTION DE CLES PRIVEES 31
6.3. AUTRES ASPECTS DE GESTION DES BI-CLES 31
6.3.1. Archive des clés publiques *31*
6.3.2. Durée de vie des clés publiques et privées *31*
6.4. DONNEES D'ACTIVATION 31
6.5. CONTROLES DE SECURITE DES POSTES DE TRAVAIL 31
6.5.1. Besoins de sécurité spécifiques sur les postes de travail *31*
6.5.2. Niveau de sécurité du poste de travail *32*
6.6. CONTROLES TECHNIQUES DU SYSTEME DURANT SON CYCLE DE VIE 32
6.6.1. Contrôles des développements des systèmes *32*
6.6.2. Contrôles de la gestion de la sécurité *32*
6.7. CONTROLES DE SECURITE DU RESEAU 32
6.8. CONTROLES TECHNIQUES DU MODULE CRYPTOGRAPHIQUE 32

7. PROFILS DES CERTIFICATS ET DES CRL 33

7.1. PROFIL DU CERTIFICAT 33
7.1.1. Champs de base *34*
7.1.2. Extensions *34*
7.2. PROFIL DE CRL 35
7.2.1. Champs de base *35*
7.2.2. Extensions *36*

8. ADMINISTRATION DES SPÉCIFICATIONS 37

8.1. PROCEDURE DE MODIFICATION DE CES SPECIFICATIONS 37
8.2. PROCEDURE DE PUBLICATION ET NOTIFICATION 37
8.3. PROCEDURES D'APPROBATION DE LA DPC 37

ANNEXE 1 38

DOCUMENTS DE RÉFÉRENCE **38**

DOCUMENTS DE NATURE JURIDIQUE 39
DOCUMENTS DE NATURE NORMATIVE 40
DOCUMENTS INTERNES GIP « CPS » 40

ANNEXE 2 **41**

GLOSSAIRE ET ACRONYMES **41**

GLOSSAIRE 42
ACRONYMES 45

1. INTRODUCTION

1.1. PRESENTATION GENERALE

1.1.1. Objectifs et domaine d'application de la PC

Une PC est un ensemble de règles, qui indique les conditions d'applicabilité d'un certificat pour une communauté donnée ou pour des applications ayant des besoins de sécurité communs : elle est définie indépendamment des détails concernant l'environnement de mise en œuvre de l'IGC à laquelle elle s'applique.

Une PC décrit quelles sont les modalités de gestion et d'usage des certificats. Les pratiques mises en œuvre pour atteindre les garanties offertes sur ces certificats sont présentées dans un autre document : la « Déclaration relative aux Pratiques de Certification », ci-après nommée DPC (cf.[DPC]).

La gestion d'un certificat comprend toutes les phases du cycle de vie d'un certificat, de la demande d'attribution à la fin de vie de ce certificat (expiration, révocation). Le but de la présente PC est de fournir aux utilisateurs de certificats de serveurs applicatifs émis par l'IGC « CPS » les informations relatives aux garanties offertes par ces certificats ainsi qu'à leurs conditions d'utilisation.

Cette PC est cohérente avec le document « Procédures et Politiques de Certification de Clés » (PC² version 2.2), émis par la Commission Interministérielle pour la Sécurité des Systèmes d'Information (CISSI) et dont elle suit la structuration.

1.1.2. Rôle du GIP « CPS »

« 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) (...) » (Extrait 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 » 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. 161-54 du [Décret 98-271]).

Le rôle du GIP « CPS » est articulé autour de trois axes fondamentaux :

1. **Spécification et développement du système « CPS » et des services associés :**
   1.1 carte et masque « CPS » ;
   1.2 services logiciels « CPS » (API) ;

1.3 secrets et systèmes de signature et de chiffrement.

2. Exploitation du système « CPS » et des services associés :

2.1 gestion des dossiers de demande et des habilitations correspondantes ;

2.2 émission, distribution et renouvellement des cartes de la famille CPS ;

2.3 génération , distribution, renouvellement et publication des certificats ;

2.3 garantie de contrôle et de validation des données contenues dans les cartes, conformément aux procédures en vigueur ;

2.4 constitution et publication des listes de certificats révoqués (CRL) ;

2.5 délivrance d'une datation de confiance concernant notamment les certificats et les révocations.

3. Promotion du système « CPS » en vue de son intégration :

3.1 promotion de la carte et des services « CPS » ;

3.2 examen des demandes d'utilisation des cartes de la famille « CPS » par des promoteurs d'application, dans le cadre d'avis rendus par le « Collège de Déontologie » (CODEON) du GIP « CPS » ;

3.2 spécification des mécanismes et protocoles à respecter par les tiers.

1.1.3. Le Système « CPS », clé de voûte de la sécurité du Système de Santé.

« 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.161-3 sont opposables à leur signataire. » (Art. R. 161-58 de [Décret 98-271])

1.1.4. Garanties offertes par le GIP « CPS »

Le GIP « CPS » garantit à ses utilisateurs (dans la limite du niveau de sécurité des technologies employées, tel qu'évalué au sens ITSEC ou Critères Communs (CC)) :

1. que tout détenteur légitime (porteur) de carte « CPS » est une personne autorisée :

chaque porteur de carte « CPS » a ainsi été clairement authentifié et sa qualité vérifiée, conformément aux procédures en vigueur ;

2. que les cartes utilisées sont valides :

le système mis en œuvre permet de vérifier qu'aucune carte périmée n'est utilisée.

1.1.5. Types de certificats concernés par la présente PC

En tant qu'Autorité de Certification (AC), le GIP « CPS » gère dans le cadre de cette PC les certificats destinés à la sécurisation de sessions de serveurs applicatifs.

1.1.6. Classe de certificats concernés par la présente PC

Une classe de certificats a été définie au sein de l'IGC « CPS » pour distinguer les certificats de serveurs applicatifs des certificats attribués à des personnes physiques (de signature et d'authentification ou de confidentialité)**.**

L'accepteur d'un certificat de serveur applicatif de l'IGC « CPS » peut connaître sa classe en affichant le contenu du certificat et en contrôlant le champ *Emetteur (Issuer)* :

C=FR, O=GIP-CPS, OU=AC-CLASSE-4

1.2. IDENTIFICATION

La présente PC est identifiée, à partir de l'Identifiant d'Objet (OID) déposé pour le GIP « CPS » auprès de l'AFNOR, comme suit :

{iso(1) member-body(2) france(250) type-org(1) gip-cps(71) icp(3) doc(7) cp(5)}

1.3. AUTORITES, APPLICATIONS ET UTILISATEURS CONCERNES PAR LA PRESENTE PC

1.3.1. Autorité de Certification

Le GIP « CPS » est l'AC de l'IGC « CPS », dont il doit être considéré comme le Maître d'Ouvrage. A ce titre et dans le cadre de cette PC, il exerce les responsabilités suivantes :

- ✓ la définition des PC et leur mise en œuvre formalisée à travers une DPC ;
- ✓ la génération et la gestion des secrets maîtres de l'IGC « CPS » : certificats d'AC racines et certificats d'AC intermédiaires ;
- ✓ la génération et la gestion des certificats délivrés aux serveurs applicatifs ;
- ✓ la publication dans un annuaire des certificats valides et des CRL signées ;
- ✓ la journalisation et l'archivage des événements et informations relatifs au fonctionnement de l'IGC « CPS ».

Pour assurer les fonctions opérationnelles qui en découlent, l'AC « CPS » peut s'organiser de la façon qui lui convient le mieux :

- ✓ soit en les prenant directement en charge,
- ✓ soit en les sous-traitant sous son contrôle à un ou plusieurs Opérateur(s) de Certification.

1.3.2. Autorité d'Enregistrement

Le GIP « CPS », AC de l'IGC « CPS », exerce également le rôle d'Autorité d'Enregistrement (AE) vis-à-vis des utilisateurs-serveurs applicatifs, ainsi que des diverses Autorités Compétentes pour le compte desquelles il assure la cohérence des informations validées ou fournies par celles-ci :

- ✓ contrôle, validation des demandes de certificats ;
- ✓ contrôle, validation des demandes de révocation ;
- ✓ transmission des demandes validées à l' AC « CPS » pour exécution ;
- ✓ délivrance des certificats aux demandeurs ;
- ✓ journalisation et archivage des demandes.

1.3.3. Service d'horodatage

Le service d'horodatage est assuré par l'AC « CPS ».

1.3.4. Service de publication

Ce service est rendu par un annuaire de type X.500, accessible par des requêtes LDAP ou HTTP, exploité par l'AC « CPS ».

1.3.5. Utilisateurs finaux

Les utilisateurs finaux de l'IGC « CPS » sont :

- ✓ les serveurs applicatifs ;
- ✓ les accepteurs des certificats de serveurs applicatifs.

Les utilisateurs doivent respecter les règles d'usage définies dans la présente PC.

1.3.6. Types d'applications concernées par la présente PC

Les applications concernées par cette PC sont toutes celles utilisant les certificats de l'IGC « CPS » pour la sécurisation de sessions de serveurs applicatifs Internet.

1.4. POINTS DE CONTACTS

1.4.1. Personne à contacter concernant ce document

La personne à contacter concernant la présente PC est le Responsable Sécurité du GIP «CPS».

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

2. DISPOSITIONS D'ORDRE GÉNÉRAL

2.1. OBLIGATIONS

2.1.1. Obligations communes à toutes les composantes de l'IGC « CPS »

Le GIP « CPS » s'engage, pour chacune des composantes de l'IGC « CPS », au respect des obligations suivantes :

- ✓ protéger et garantir la confidentialité et l'intégrité de ses clés privées ;
- ✓ n'utiliser ses clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, selon la présente PC ;
- ✓ respecter le résultat d'un contrôle de conformité et remédier aux non-conformités qu'il révélerait ;
- ✓ respecter le contrat qui le lie aux utilisateur finaux ;
- ✓ documenter ses procédures internes de fonctionnement ;
- ✓ mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles l'entité s'engage ;
- ✓ respecter et appliquer les PC et DPC associées de l'IGC « CPS ».

2.1.2. Obligations incombant à l'AC

Le GIP « CPS », en tant qu'AC :

- ✓ assure l'élaboration des différentes PC et DPC associées de l'IGC « CPS » ;
- ✓ soumet ces documents à l'approbation de son Conseil d'Administration ou de son Assemblée Générale ;
- ✓ détient et gère les clés de l'AC racine et certifie la clé publique d'AC intermédiaire de l'Opérateur de Certification ;
- ✓ prend toutes les mesures raisonnables pour s'assurer que les utilisateurs sont au courant de leurs droits et obligations respectifs en ce qui concerne l'utilisation et la gestion des clés et des certificats (notamment en publiant la présente PC sur son site Internet).

Dans le cadre de ses fonctions opérationnelles, qu'il assume directement ou qu'il délègue sous son contrôle à l'Opérateur de Certification, le GIP « CPS » :

- ✓ génère les certificats, les stocke et les renouvelle ;
- ✓ est responsable de la mise en œuvre et de l'exploitation du service de publication ;
- ✓ révoque les certificats ;
- ✓ signe et transmet les CRL au service de publication (annuaire « CPS ») ;
- ✓ dispose d'un moyen de reconstruction de ses propres clés privées ;
- ✓ met en œuvre tout ce qui est en son pouvoir pour garantir la fiabilité des mécanismes techniques de sécurité utilisés ainsi que la cohérence entre les différentes composantes, notamment à travers la vérification du chemin de confiance ;
- ✓ garantit l'intégrité des informations manipulées, notamment :
  - les informations contenues dans le certificat,

- les informations publiées,
- les informations fournies par le service d'horodatage.

2.1.3. Obligations incombant à l'AE

Le GIP « CPS », en tant qu'AE :

- ✓ vérifie la signature du demandeur (nouveau certificat, révocation) ;
- ✓ vérifie dans l'annuaire « CPS » le niveau d'habilitation du demandeur.

2.1.4. Obligations incombant aux serveurs applicatifs

Les serveurs applicatifs sont tenus de respecter les exigences et recommandations de la présente PC.

2.1.5. Obligations incombant aux accepteurs de certificats

Les accepteurs de certificats doivent :

- ✓ vérifier l'authenticité du certificat traité ;
- ✓ vérifier que le certificat n'est pas expiré ;
- ✓ vérifier la validité du certificat par rapport à la CRL (statut du certificat dans la CRL et validité de la CRL) avec la fréquence qu'ils jugent adaptée aux garanties qu'ils souhaitent ;
- ✓ respecter les exigences et recommandations de la PC.

2.2. RESPONSABILITES

2.2.1. Responsabilité de l'AC

Le GIP « CPS », en tant qu'AC, est responsable de la conformité des certificats qu'il émet vis à vis de la présente PC.

2.2.2. Responsabilité de l'AE

Le GIP « CPS », en tant qu'AE, est responsable des contrôles de complétude et de cohérence effectués lors de la réception du formulaire de la demande de certificat de serveur applicatif.

2.2.3. Responsabilité du service de publication

Ce service est responsable du contrôle des accès à son annuaire, conformément à la charte d'accès à l'annuaire [Accès_Annuaire] qui lui est propre et qui ne fait pas partie des spécifications de la PC de l'IGC « CPS ».

Il garantit les conditions de mise à jour et de disponibilité explicitées au sous-chapitre 2.4.

2.2.4. Responsabilités du serveur applicatif

Le serveur applicatif est responsable d'utiliser les certificats et bi-clés aux fins pour lesquels ils sont générés.

2.2.5. Responsabilité de l'accepteur de certificat

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

2.2.6. Limites de responsabilités du GIP « CPS »

Le GIP « CPS », en tant qu'AC, décline toute responsabilité vis à vis de l'utilisation, dans des conditions autres que celles prévues par la présente PC, des certificats qu'il émet. Il décline notamment sa responsabilité pour tout dommage résultant d'un emploi de ces certificats pour un usage autre que ceux prévus, comme pour tout dommage résultant d'actes délictueux dans la commission desquels serait intervenue l'utilisation de ces certificats.

Le GIP « CPS », en tant qu'AC, décline également sa responsabilité pour tout dommage résultant des erreurs ou inexactitudes entachant les informations contenues dans le certificat, lorsque ces erreurs ou inexactitudes résultent directement du caractère erroné des informations qui lui ont été transmises.

2.3. INTERPRETATION DE LA LOI

2.3.1. Textes applicables

Les dispositions de nature juridique (législatifs ou réglementaires) ou normative applicables sont indiquées en Annexe 1.

2.3.2. Arbitrage des litiges

La juridiction compétente est chargée de la résolution des litiges. Dans le cas où le litige relève de la juridiction administrative, il est fait attribution de compétence au Tribunal Administratif de Paris.

2.4. PUBLICATION ET SERVICES ASSOCIES

2.4.1. Informations publiées au sein de l'IGC

Les documents suivants sont publics et rendus disponibles dès leur publication sur le site Internet du GIP « CPS » à l'adresse www.gip-cps.fr :

- ✓ PC de l'IGC « CPS » relatives aux différentes catégories de certificats ;
- ✓ Charte d'accès à l'Annuaire « CPS » (cf. [Accès_Annuaire]) ;
- ✓ Certificats et CRL du système « CPS » ;
- ✓ Procédures de distribution des cartes « CPS ».

Les informations suivantes sont publiées par le service de publication de l'AC « CPS » sur son annuaire accessible par Internet :

- ✓ les CRL ;
- ✓ les certificats valides ;
- ✓ le certificat racine de l'AC ;
- ✓ l'empreinte de la clé publique du certificat racine de l'AC « CPS » ;

- ✓ les certificats d'AC intermédiaires.

2.4.2. Fréquence de mise à jour des certificats dans l'annuaire

Les certificats applicatifs sont rendus disponibles dans l'annuaire de l'IGC « CPS » après certification de la clé publique associée.

2.4.3. Contrôle d'accès aux certificats dans l'annuaire

L'accès en consultation aux certificats de serveurs applicatifs est libre.

L'accès en écriture à l'annuaire est réservé aux fonctions internes à l'IGC « CPS » : aucun accès en écriture d'origine externe à l'IGC « CPS » n'est possible.

2.4.4. Responsabilité de la gestion de l'annuaire de l'IGC « CPS »

L'AC de l'IGC « CPS » est responsable de la mise en œuvre et de l'exploitation de l'annuaire « CPS », par son service de publication.

2.5. CONTROLES DE CONFORMITE

2.5.1. Fréquence des contrôles de conformité

Un contrôle de conformité est réalisé de manière régulière, au moins tous les deux ans, afin de vérifier la conformité des pratiques effectives de sécurité par rapport à la DPC.

2.5.2. Identité et qualification du contrôleur

Le GIP « CPS », en tant que « maître d'ouvrage » 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 sera choisie par le GIP « CPS », en accord avec l'Opérateur de Certification, en fonction de ses compétences en sécurité des systèmes d'information. Les composantes de l'IGC « CPS » n'auront aucun lien structurel avec cette entité.

2.5.3. Sujets couverts par le contrôle de conformité

Le contrôle de conformité porte principalement sur les points suivants :

- ✓ identification et authentification ;
- ✓ besoins opérationnels ;
- ✓ contrôle de sécurité physique, contrôle des procédures, contrôle du personnel ;
- ✓ contrôles techniques de sécurité ;
- ✓ profil des certificats et CRL ;
- ✓ spécifications d'administration.

2.5.4. Communication des résultats et mesures à prendre en cas de non-conformité

Les résultats du contrôle de conformité sont intégralement communiqués par l'entité d'audit au GIP « CPS », maître d'ouvrage pour l'IGC « CPS », qui a la responsabilité de faire mettre en œuvre les mesures correctrices éventuellement nécessaires.

2.6. POLITIQUE DE CONFIDENTIALITE

2.6.1. Types d'informations secrètes ou confidentielles

Les informations secrètes[1] sont les clés privées des entités propriétaires de certificats (AC et serveurs applicatifs).
Les informations confidentielles[2] sont :

- ✓ les journaux d'événements des composantes de l'IGC « CPS » ainsi que leurs archives ;
- ✓ certaines spécifications des systèmes de sécurité.

2.6.2. Types d'informations sensibles

Dans le cadre de cette PC, il n'y a pas d'informations sensibles[3].

2.6.3. Types d'informations libres

Les informations libres[4] sont les informations publiées (cf. paragraphe 2.4.1).

2.6.4. Divulgation des causes de révocation

Les causes de révocation ne sont jamais divulguées par l'IGC « CPS ».

2.7. DROITS SUR LA PROPRIETE 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

[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 sensibles sont des informations dont la divulgation entraînerait 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.
[4] Les informations classées libres sont destinées à une libre circulation.

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.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1. ENREGISTREMENT INITIAL

3.1.1. Convention de noms

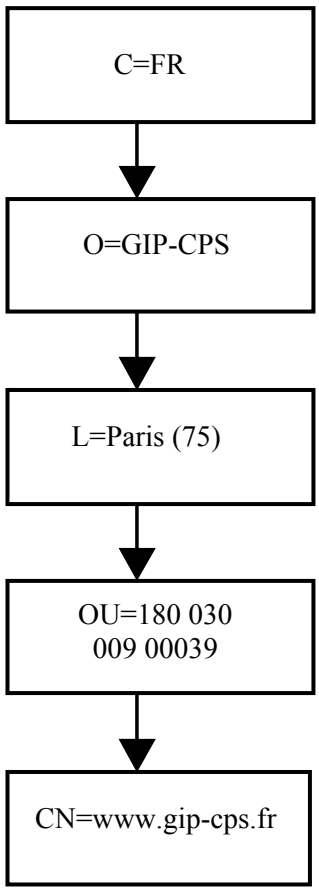
Les noms utilisés dans un certificat émis par l'IGC «CPS» sont décrits selon la norme X.500.
Dans chaque certificat X.509 le fournisseur (issuer) et le porteur (subject) sont identifiés par un Distinguished Name (DN) qui doit être unique sur le domaine de certification de l'AC « CPS ».

Chaque DN est hiérarchiquement construit par la concaténation des Relative Distinguished Names (RDN) suivants :

- Country (France),
- Organisation (GIP-CPS),
- Locality (département),
- Organisational Unit (Identification nationale de la structure),
- Common name (FQDN du serveur).

Le FQDN (*Fully Qualified Domain Name*) est de la forme : XXX.YYY où XXX est le nom d'hôte du serveur et YYY est le nom de domaine.

Exemple : *DN d'un serveur appartenant au domaine « gip-cps.fr »*

Arbre de nommage	Relative Distinguished Name	Distinguished Name
	Racine	{ }
	Country = France	{ C=FR }
	Organisation =GIP-CPS	{ C=FR O=GIP-CPS }
	Locality = Paris (75)	{ C=FR O=GIP-CPS L=Paris (75) }
	Organisational Unit = 180 030 009 00039	{ C=FR O=GIP-CPS L=Paris (75) OU= 180 030 009 00039 }
	Common name = www.gip-cps.fr	{ C=FR O=GIP-CPS L=Paris (75) OU= 180 030 009 00039 CN= www.gip-cps.fr }

Note : Les DN des certificats de test auront « GIP-CPS-TEST » au lieu de « GIP-CPS » comme valeur pour le RDN Organisation.

3.1.2. Nécessité d'utilisation de noms explicites

Les noms pour désigner le porteur d'un certificat sont explicites. Le CommonName d'un serveur est unique.

3.1.3. Règles d'interprétation des différentes formes de nom

Sans objet.

3.1.4. Unicité des noms

Les noms pour désigner un porteur de certificat sont uniques sur le domaine de certification de l'AC « CPS » (Cf. paragraphe 3.1.1).

3.1.5. Procédure de résolution de litige concernant un nom

Sans objet.

3.1.6. Preuve de la possession de la clé privée

La preuve est faite que le porteur dispose bien de la clé privée de confidentialité associée à la clé publique à certifier par l'AC « CPS » puisque la demande est signée par cette clé privée.

3.2. RE-GENERATION DE CERTIFICATS APRES EXPIRATION

Les certificats de serveur applicatif émis par le GIP « CPS » ont une durée de vie de un an.

La demande de génération d'un nouveau certificat après expiration est de la responsabilité de l'administrateur du serveur.

3.3. RE-GENERATION DE CLES APRES REVOCATION

La génération de nouvelles clés applicatives est de la responsabilité de l'administrateur du serveur.

3.4. AUTHENTIFICATION D'UNE DEMANDE DE REVOCATION

Les demandes de révocation sont signées par l'administrateur du serveur ou par un opérateur de l'AC. Elles peuvent être formulées :

- par téléphone, mais doivent faire dans ce cas l'objet d'une confirmation écrite papier à posteriori ou, éventuellement, d'une confirmation électronique sécurisée ;
- par messagerie, en envoyant un message signé par l'administrateur du serveur ou l'opérateur d'AC dont le corps de message est de la forme : `revoque <FQDN du serveur>.`

La demande de révocation doit contenir explicitement les informations d'identification du certificat du serveur (cf. § 4.4.3).

4. BESOINS OPÉRATIONNELS

4.1. DEMANDE DE CERTIFICAT

Une demande de certificat se fait en deux étapes :

- demande administrative d'enregistrement ;
- demande de certification.

4.1.1. Demande administrative

La demande administrative est un formulaire papier signé par le représentant légal de l'organisme ou de l'établissement demandeur. Ce document comporte obligatoirement :

- le(s) nom(s) de domaine rattaché(s) à son établissement (par exemple : gip-cps.fr) ;
- l'identité des personnes qui ont le rôle d'"administrateur" des bi-clés et des certificats : les administrateurs sont les seuls habilités à demander ou révoquer les certificats serveurs.

Ce formulaire peut être obtenu auprès du **Service Relations Extérieures** du GIP « CPS », auquel il devra être retourné par courrier une fois rempli.

Le traitement du formulaire par l'AE « CPS » comporte :

- la vérification du (ou des) nom(s) de domaine(s) ;
- la vérification du signataire de la demande, obligatoirement porteur d'une carte valide de la famille CPS (types « CPS », « CDE » ou « CPA responsable » - c'est-à-dire avec certificats de classes 1 ou 2)
- la vérification de l'identité et de la qualité des administrateurs désignés, obligatoirement porteurs d'une carte valide de la famille CPS (types « CPE » ou « CPA » - c'est-à-dire avec certificats de classe 3) ;
- la mise à jour et l'enregistrement des habilitations dans l'annuaire CPS.

4.1.2. Demande de certification

Pour obtenir un certificat, l'administrateur, une fois habilité par l'AE « CPS, réalise les opérations suivantes :

4.1.2.1. Génération de la Requête de Certificat Serveur (CSR)

La CSR est l'élément nécessaire à la fabrication du Certificat Serveur. Elle est générée sur la machine qui sert de serveur.

Le "Distinguished Name" (DN) du serveur doit être conforme à la convention de noms spécifiée au § 3.1.1.

La CSR peut comporter éventuellement les extensions suivantes :

- l'extension "netscapeCertype" qui indique le type de certificat demandé :
  - 0xC0 pour les certificat SSL (assumé par défaut)

- 0x20 pour les certificats S/MIME

- l'extension "subjectAltName" qui indique le nom alternatif du serveur :
  - le FQDN *(Fully Qualified Domain Name)* du serveur, identique au CN du DN, pour les certificat de type SSL (assumé par défaut)
  - l'adresse e-mail du serveur, pour les certificat de type S/MIME.

4.1.2.2. Signature de la CSR par la carte de l'administrateur

L'administrateur envoie la CSR dans un message S/MIME signé (par sa clé privée de signature CPS) et chiffré à l'adresse de messagerie de l'autorité d'enregistrement (par exemple : certification@certificats.gip-cps.fr).

4.2. GENERATION DE CERTIFICAT

Un message contenant une CSR est accepté par l'Opérateur de Certification si les conditions suivantes sont remplies :

1. le message peut être déchiffré par le serveur d'AE ;
2. le certificat public du signataire est un certificat de signature CPS de classe 3 ;
3. la signature du message est valide : contrôle cryptographique, contrôle du chemin de certification et de non-révocation ;
4. le signataire détient les habilitations suffisantes : droits d'administration des clés et des certificats ;
5. la preuve de possession de la clé privée est faite ;
6. la structure de la CSR est conforme ;
7. la structure est référencée dans l'annuaire (OU=idnatstruct, L=département, O=GIP-CPS, C=FR) ;
8. la cohérence du DN est établie ; cas possibles :
   - il existe dans l'annuaire un autre DN composé d'un CN identique : rejet de la demande ;
   - le DN est absent de l'annuaire : la demande est une demande initiale ;
   - le DN est présent dans l'annuaire : il s'agit d'un renouvellement (révocation implicite de l'ancien certificat) ;
9. le type de certificat demandé est déterminé.

Le tableau suivant indique le type de certificat en fonction des valeurs croisées des deux extensions netscapeCertype et subAltName présentes ou non dans la CSR (X = rejet de la demande) :

subAltName / **netscapeCertype**	Non présente	Valeur RFC822	Valeur FQDN	Valeur autre
Non présente	SSL	S/MIME	SSL	X
Valeur 0xC0	SSL	X	SSL	X
Valeur 0x20	X	S/MIME	X	X
Valeur autre	X	X	X	X

La génération des certificats se fait par un « Boîtier de Sécurité » qui est soumis à une évaluation sécuritaire.

Le certificat fabriqué par l'Opérateur de Certification est retourné à l'adresse de messagerie de l'émetteur du message CSR.

4.3. ACCEPTATION DE CERTIFICAT

La réception par le demandeur de son certificat dans sa boîte de messagerie vaut acceptation.

4.4. REVOCATION ET EXPIRATION DE CERTIFICAT

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

4.4.1. Causes possibles d'une révocation

Certificat « racine » de l'AC « CPS » :

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat « racine » :

- ✓ compromission ou suspicion de compromission, perte ou vol de la clé privée correspondante ;
- ✓ cessation d'activité de l'AC ;
- ✓ 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.

Certificat d'AC intermédiaire de classe 4 :

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

- ✓ révocation du certificat racine de l'AC « CPS » ;
- ✓ compromission ou suspicion de compromission, perte ou vol de la clé privée correspondante ;
- ✓ 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.

Certificat applicatif :

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

- ✓ la clé privée du serveur applicatif est détruite, perdue, volée, compromise ou suspectée de compromission ;
- ✓ les informations ou les attributs du serveur applicatif 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 serveur applicatif 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).

4.4.2. Origine d'une demande de révocation

Les entités qui peuvent demander la révocation d'un certificat applicatif sont les suivantes :

- ✓ le propriétaire du certificat,
- ✓ le GIP « CPS » en tant qu'AC.

4.4.3. Procédure de demande de révocation

La demande de révocation doit contenir explicitement les informations d'identification du certificat et du serveur applicatif propriétaire. Elle peut être transmise directement à l'AE par l'intermédiaire de sa « hot-line », mais doit faire dans ce cas l'objet d'une confirmation écrite papier à posteriori

A la réception de la demande de révocation, l'AE authentifie le demandeur, vérifie son habilitation, vérifie, s'il y a lieu, la cause de révocation et transmet la demande, si elle est justifiée, à l'AC.

La demande de révocation doit contenir explicitement les informations d'identification du certificat du serveur.

Une demande de révocation est acceptée et traitée si :
- la signature apposée est valide,
- le signataire possède les habilitations suffisantes (administrateur ou opérateur),
- le FQDN du serveur est enregistré dans l'annuaire CPS.

L'AC révoque le certificat en introduisant le numéro de série du certificat dans la CRL. Le certificat est en outre supprimé de l'annuaire « CPS ».

La révocation de son certificat est confirmée par messagerie à son propriétaire.

L'opération de révocation est journalisée avec l'origine de la demande ayant entraîné la révocation du certificat.

4.4.4. Délai de traitement d'une révocation

Le délai maximum de traitement d'une demande de révocation est de 2 jours ouvrés *(c'est à dire hors samedis, dimanches et jours de fermeture réglementaires du GIP « CPS », ces derniers comprenant les jours fériés ainsi que deux jours supplémentaires accordés par la Direction selon accord d'entreprise portant sur la réduction du temps de travail signé le 30 décembre 1999)* à réception de la demande.

4.4.5. Fréquence de mise à jour des CRL

L'AC "CPS" publie une mise à jour des CRL et des DeltaCRL chaque jour ouvré *(cf.définition §4.4.4)*. Chaque CRL (ou DeltaCRL) contient la date et l'heure prévisionnelles de publication de la CRL (ou DeltaCRL) suivante.

4.4.6. Exigences de contrôle des CRL

Il appartient à l'utilisateur « accepteur » d'un certificat « CPS » de contrôler le statut de ce certificat ainsi

que la validité de la CRL publiée sur l'annuaire de l'IGC « CPS ».

4.4.7. Publication des causes de révocation

Les causes de révocation ne sont pas publiées dans les CRL ou DeltaCRL.

4.4.8. Accès en ligne des CRL

Les CRL et DeltaCRL sont en accès libre sur l'annuaire « CPS » pour téléchargement en ligne.

4.4.9. Expiration des certificats

Les certificats expirés ne sont pas révoqués ; ils sont supprimés de l'annuaire mais ne sont pas inclus en CRL ou DeltaCRL. Ces deux dernières listes ne contiennent que des certificats révoqués mais non expirés.

Les certificats expirés ne doivent plus être utilisés.

4.5. JOURNALISATION DES EVENEMENTS

Les types d'évênements enregistrés, ainsi que les modalités de traitement et de conservation des journaux d'évênements, sont spécifiés dans la DPC.

4.6. ARCHIVES

4.6.1. Types de données archivées

Sont archivées les informations concernant les porteurs, c'est à dire :

- ✓ les demandes de certificats ;
- ✓ les listes de certificats et CRL ;
- ✓ les certificats et les informations les concernant ;
- ✓ les documents contractuels et conventions.

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

4.6.2. Période de rétention des archives

Les demandes de certificats applicatifs sont conservés pendant cinq ans.

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

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

4.6.3. 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.

4.6.4. Procédures de copie / backup des archives

Les procédures correspondantes sont décrites dans la DPC.

4.6.5. Besoin d'horodatage des enregistrements d'archives

Les enregistrements d'archives sont horodatés conformément à la DPC.

4.6.6. Système de collecte des archives (interne ou externe)

Pas de spécifications particulières.

4.6.7. Procédures d'accès / de récupération 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.

4.7. CHANGEMENT DE CLE D'UNE COMPOSANTE

L'AC « CPS » ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du bi-clé d'AC intermédiaire correspondant à la classe de ce certificat ou du bi-clé racine de l'AC « CPS ».

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

4.8. COMPROMISSION ET PLAN ANTI-SINISTRE

4.8.1. En cas de corruption des ressources informatiques (logiciels ou données)

Les composantes de l'IGC « CPS » font l'objet d'un plan de continuité décrit dans la DPC, garantissant, en cas de sinistre majeur, une reprise dans des délais compatibles avec les exigences de sécurité requises par l'IGC.

4.8.2. En cas de révocation du certificat d'une composante de l'IGC

En cas de révocation d'une composante de l'IGC (AC ou autre), la composante est mise hors service, jusqu'à ce qu'un contrôle de conformité ou une éventuelle nouvelle accréditation soit effectuée.

4.8.3. Mesures de sécurité après un sinistre

Ces mesures sont spécifiées dans la DPC.

4.9. FIN DE VIE DE L'AC « CPS »

En cas d'interruption de ses activités, l'AC « CPS » s'engage à en aviser immédiatement les porteurs et à prendre des dispositions pour que les clés et les informations de l'AC continuent d'être archivées selon les indications et la période stipulées dans la PC.

En outre, l'AC en fin de vie 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 elle dispose pour informer ses partenaires de ses intentions ;
- ✓ révoquer son certificat (sauf en cas de transfert) ;
- ✓ révoquer tous les certificats valides qu'elle a signés (sauf en cas de transfert) ;
- ✓ assurer la pérennité des CRL émises ;
- ✓ remettre ses archives ainsi que l'ensemble des données dont elle dispose à une entité fiable.

En cas de transfert des activités de l'AC « CPS » à une autre AC, cette dernière devra offrir le même niveau d'assurance (niveau de confiance dans la sécurité des processus mis en œuvre).

5. CONTRÔLES DE SÉCURITÉ PHYSIQUE, DES PROCÉDURES ET DU PERSONNEL

5.1. CONTROLES DE SECURITE PHYSIQUE

Le GIP « CPS » s'engage à mettre en œuvre et à maintenir un niveau de sécurité physique conforme aux règles de bonne pratique concernant les locaux d'exploitation des composantes de son IGC (les procédures correspondantes sont détaillées dans la DPC).

5.1.1. Situation géographique et construction des sites

Les sites d'exploitation des composantes de l'IGC « CPS » sont implantés sur le territoire national

5.1.2. Accès physique

Le GIP « CPS » a mis en œuvre des contrôles d'accès physiques aux sites et locaux renfermant des composantes de son IGC, permettant de se protéger contre tout accès non autorisé.

5.1.3. Alimentation électrique et climatisation

L'environnement électrique et de climatisation des locaux d'exploitation des composantes de l'IGC « CPS » est conforme aux recommandations des fournisseurs de matériels.

5.1.4. Vulnérabilité aux dégâts des eaux

Les locaux d'exploitation des composantes de l'IGC « CPS » sont équipés de systèmes de protection contre les accidents de type dégâts des eaux adaptés à leur environnement physique.

5.1.5. Prévention et protection contre le feu

Les locaux d'exploitation des composantes de l'IGC « CPS » sont équipés de systèmes de protection contre les accidents de type incendie adaptés à leur environnement physique.

5.1.6. Conservation des médias

Les supports d'information manipulés au sein des composantes de l'IGC « CPS » sont protégés en confidentialité et en intégrité selon des règles formelles présentées dans la DPC.

5.1.7. Destruction des données

Tous les supports servant au stockage de l'information sensible doivent être effacés ou détruits avant leur mise au rebut.

5.1.8. Site(s) de secours

L'existence et la gestion de ce(s) site(s) sont définies dans le cadre du plan de continuité référencé au § 4.8.1.

5.2. CONTROLES DES PROCEDURES

Ces contrôles s'appliquent à l'ensemble de l'IGC « CPS ». Ils peuvent concerner les composantes du GIP « CPS » ou d'autres entités sous-traitantes exploitant certaines composantes de l'IGC « CPS ». L'obligation pour ces sous-traitants de respecter les contrôles définis dans la présente PC figure explicitement dans les contrats les liant au GIP « CPS ».

5.2.1. Rôles de confiance

On distingue au sein de l'IGC « CPS » les quatre rôles suivants . :

- ✓ ingénieur sécurité,
- ✓ directeur d'exploitation,
- ✓ opérateur,
- ✓ responsable sécurité.

Les attributions détaillées associées à chaque rôle sont décrites dans la DPC.

5.2.2. Nombre de personnes requises par tâche

Selon le type 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 exigés 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 d'AC et d'AE de l'IGC ;
- ✓ que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement aux systèmes d'AC ou d'AE 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.

5.3. CONTROLES DU PERSONNEL

Les contrôles de personnel s'appliquent à l'ensemble du personnel du GIP « CPS », qu'il s'agisse du personnel interne au GIP « CPS » ou du personnel d'entités sous-traitantes exploitant certaines composantes de l'IGC. L'obligation pour ces sous-traitants de respecter les contrôles définis dans la présente PC figure explicitement dans les contrats les liant au GIP « CPS ».

5.3.1. Compétences, qualification et antécédents requis

Le recrutement du personnel impliqué dans l'exploitation de l'IGC « CPS » fait l'objet d'une procédure de contrôle et de suivi particulière, permettant de valider les compétences professionnelles et l'intégrité

des candidats. Le contrat de travail doit mentionner explicitement le rôle de la personne embauchée et comporter une clause de confidentialité.

5.3.2. Exigences et fréquence en matière de formation

Le personnel exécutant de l'IGC « CPS » reçoit une formation initiale à l'utilisation des logiciels, matériels et procédures mis à sa disposition, dans le cadre de la composante pour laquelle il opère.

Sa formation se trouve complétée à chaque mise à jour de l'organisation, des outils ou des procédures.

5.3.3. Gestion des métiers

Les règles de gestion des métiers au sein des composantes de l'IGC « CPS » sont celles des organismes employeurs.

5.3.4. Sanctions appliquées en cas d'actions non autorisées

Les organismes employeurs décident des sanctions à appliquer lorsqu'un collaborateur de l'IGC « CPS » a abusé de ses droits ou effectué une opération non conforme à ses attributions, et ce, dans le cadre des textes législatifs et réglementaires en vigueur.

5.3.5. Contrôle du personnel contractant

Les personnels contractants respectent les mêmes conditions que celles applicables au personnel interne (Cf. § 5.3.1 à 5.3.4).

5.3.6. Documentation fournie au personnel

Le personnel dispose de l'ensemble des informations et documents impliquant des éléments de sécurité dans ses activités, notamment la DPC, la PC, les procédures internes de fonctionnement, ainsi que les documentations des matériels et logiciels utilisés.

6. CONTRÔLES TECHNIQUES DE SÉCURITÉ

6.1. GENERATION ET INSTALLATION DE BI-CLES

6.1.1. Génération de bi-clés

La génération des bi-clés du serveur applicatif est effectuée par celui-ci.

6.1.2. Transmission de la clé privée à son propriétaire

Sans objet.

6.1.3. Transmission de la clé publique à l'AC

La clé publique du serveur applicatif est transmise à l'Opérateur de Certification selon la procédure d'enregistrement protégée en intégrité de bout en bout décrite en § 4.1.

6.1.4. Transmission de clé publique de l'AC aux utilisateurs

Les certificats des clés publiques de l'AC (« racine » et « intermédiaires ») sont transmis aux utilisateurs par publication dans l'annuaire « CPS ».

La clé publique racine de l'AC « CPS » fait l'objet de la plus large diffusion, notamment sur le site Internet du GIP « CPS »

.

6.1.5. Algorithme et tailles des clés

Les bi-clés « racines » de l'AC « CPS » sont des clés RSA de 2048 bits.

Les bi-clés de signature des certificats des AC intermédiaires « CPS » sont des clés RSA de 1024 bits.

Les bi-clés de serveurs applicatifs sont des clés RSA de 1024 bits.

6.1.6. Génération des paramètres de clé publique

Sans objet. L'entité qui génère son bi-clé génère également les paramètres de clé publique.

6.1.7. Contrôle de qualité des paramètres de clés

Sans objet.

6.1.8. Mode de génération de clé (matérielle ou logiciel)

Sans objet.

6.1.9. Usage de la clé

Les bi-clés de serveurs applicatifs sont utilisés à des fins de sécurisation de sessions de ces serveurs ou de signature de messages émis par ces derniers (deux certificats distincts).

Les différents usages possibles des clés sont définis et contraints par l'utilisation d'une extension de certificat X.509v3 (cf. chapitre 7.1.2).

6.2. PROTECTION DE CLES PRIVEES

Pas de spécifications. L'utilisateur est entièrement responsable de la protection de ses clés privées.

6.3. AUTRES ASPECTS DE GESTION DES BI-CLES

6.3.1. Archive des clés publiques

Les clés publiques sont archivées dans le cadre de l'archivage des certificats (cf. paragraphe 4.6.).

6.3.2. Durée de vie des clés publiques et privées

Elle est égale à la durée de vie du certificat correspondant. Cette dernière est définie contractuellement entre le GIP « CPS » et l'entité propriétaire du serveur applicatif.

6.4. DONNEES D'ACTIVATION

Sans objet.

6.5. CONTROLES DE SECURITE DES POSTES DE TRAVAIL

Il s'agit ici des postes de travail des systèmes informatiques de l'IGC « CPS » et en aucun cas des postes utilisateurs.

6.5.1. Besoins de sécurité spécifiques sur les postes de travail

Les postes de travail appartenant au système d'information de l'IGC « CPS » répondent aux exigences suivantes :

- ✓ identification et authentification des utilisateurs du poste de travail ;
- ✓ gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlés par rôle et nom d'utilisateur) ;

- ✓ protection contre les virus informatiques ;
- ✓ fonctions d'audits (imputabilité et nature des actions effectuées) ;
- ✓ éventuellement gestion des reprises sur erreurs.

En outre, les postes recensés comme habilités à recevoir des informations sensibles font l'objet de mesures de sécurité complémentaire (authentification renforcée, utilisation de cartes de type « CPA »…).

6.5.2. Niveau de sécurité du poste de travail

Le niveau minimal d'assurance offert est défini dans la DPC.

6.6. CONTROLES TECHNIQUES DU SYSTEME DURANT SON CYCLE DE VIE

6.6.1. Contrôles des développements des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes 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.

Les composantes du système d'information de l'IGC « CPS » pourront être évaluées suivant un schéma d'évaluation et de certification.

6.6.2. Contrôles de la gestion de la sécurité

Toute évolution du système doit être autorisée par l'AC « CPS », documentée et doit apparaître dans les procédures de fonctionnement interne de l'IGC « CPS ».

6.7. CONTROLES DE SECURITE DU RESEAU

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC «CPS».

6.8. CONTROLES TECHNIQUES DU MODULE CRYPTOGRAPHIQUE

Les contrôles techniques du module cryptographique suivent les recommandations émises par la DCSSI.

7. PROFILS DES CERTIFICATS ET DES CRL

7.1. PROFIL DU CERTIFICAT

CERTIFICAT

Contenu du certificat

Version		
Numéro de série		
Informations sur la signature du certificat par l'AC (algorithmes et paramètres)		
Nom du fournisseur du certificat		
Période de validité du certificat		
Nom du porteur de certificat		
Informations sur la clé publique (valeur de la clé publique, algorithme et paramètres)		
Nom unique du fournisseur de certificat		
Nom unique du porteur de certificat		
Identifiant du type de l'extension	Criticité (oui / non)	Valeur
Identifiant du type de l'extension	Criticité (oui / non)	Valeur
Identifiant du type de l'extension	Criticité (oui / non)	Valeur
…		

Algorithme de signature du certificat par l'AC *

Algorithme
Paramètres

Signature numérique du contenu du certificat

Valeur de la signature numérique du certificat par l'AC

Le profil d'un certificat est la description complète de ce certificat. Cette description comprend les champs du certificat, les extensions présentes sur ce certificat ainsi que les extensions propres au GIP « CPS ».
Ces spécifications techniques sont décrites dans le document [X509_CRL_CPS].

7.1.1. Champs de base

Les champs de base d'un certificat renseignent les informations suivantes :

- ✓ Version
- ✓ Numéro de série
- ✓ Informations sur la signature du certificat par l'AC (algorithmes et paramètres)
- ✓ Nom du fournisseur du certificat
- ✓ Période de validité du certificat
- ✓ Nom du porteur de certificat
- ✓ Informations sur la clé publique (valeur de la clé publique, algorithme et paramètres).

7.1.2. Extensions

La possibilité d'ajouter des extensions à un certificat a été apportée par la version 3 de la norme ISO 9594-8.

Une implémentation de la norme choisit parmi les extensions proposées dans cette norme celles qui sont pertinentes à son application et ajoute aux champs de base du certificat les extensions choisies.

La séquence contenue d'extension(s) adjointe aux champs de base du certificat est une collection ordonnée d'éléments dont le cardinal peut être nul. Par conséquent, un certificat X.509v3 peut ne contenir aucune extension.

Si la norme définit plusieurs types d'extensions, d'autres extensions, dites « privées » peuvent être ajoutées pour correspondre aux besoins d'une implémentation particulière.

Chacune de ces extensions est caractérisée par trois informations :

- ✓ l'identifiant de l'extension considérée, donnée par la norme,
- ✓ le fait qu'elle soit critique ou non,
- ✓ la valeur de l'extension, propre à un certificat.

Il peut être noté que le profil d'un certificat est une caractéristique de la politique de certification. Par conséquent, si l'extension précisant la politique de certification utilisée pour générer le certificat est critique, aucun problème d'interopérabilité ni de reconnaissance de certificat ne se pose. En effet, si le système vérificateur connaît et pratique cette même politique de certification, alors il connaît également le format du certificat reçu.

Les extensions de certificat permettent de spécifier plus précisément les caractéristiques suivantes :

- ✓ Informations sur les clés,
- ✓ Informations sur les politiques,
- ✓ Fournisseur et porteur de certificat,
- ✓ Contraintes sur le chemin de certification.

Le fait qu'une extension soit critique rend obligatoire la conformité du certificat aux informations contenues dans l'extension.

7.2. PROFIL DE CRL

Contenu de la LCR

Version					
Informations sur la signature de la LCR par l'AC (algorithmes et paramètres)					
Nom du fournisseur de la LCR					
Date d'émission de la LCR					
Date d'émission de la prochaine LCR					
Nom du porteur de certificat					
Liste des certificats révoqués					
	Numéro de série du certificat révoqué	Date de révocation	**Extensions d'entrée de LCR**		
			Identifiant du type de l'extension	Criticité (oui / non)	Valeur
			Identifiant du type de l'extension	Criticité (oui / non)	Valeur
			…		
	Numéro de série du certificat révoqué	Date de révocation	**Extensions d'entrée de LCR**		
			Identifiant du type de l'extension	Criticité (oui / non)	Valeur
			Identifiant du type de l'extension	Criticité (oui / non)	Valeur
			…		
	…				
Extensions de LCR					
Identifiant du type de l'extension		Criticité (oui / non)		Valeur	
Identifiant du type de l'extension		Criticité (oui / non)		Valeur	
…					

Le profil d'une CRL est la description de cette CRL en terme de champs et d'extensions propres à la CRL.

Ces spécifications techniques sont décrites dans le document [X509_CRL_CPS].

7.2.1. Champs de base

Les champs de base d'une CRL renseignent les informations suivantes :

- ✓ Version.
- ✓ Informations sur la signature de la CRL par l'AC (algorithmes et paramètres).
- ✓ Nom du fournisseur de la CRL.

- ✓ Date de l'émission de la CRL.
- ✓ Date de l'émission de la prochaine CRL.
- ✓ Liste de certificats révoqués composée de :
  - Date de révocation.
  - Numéro de série du certificat révoqué.

Remarque : La date inclut le jour et l'heure.

7.2.2. Extensions

Une implémentation de la norme X.509 choisit parmi les extensions proposées dans cette norme celles qui sont pertinentes à son application et les ajoute aux champs de base.

La version 2 du profil des CRL admet deux types d'extensions : des extensions d'entrée de CRL et des extensions de CRL.

7.2.2.1. Extensions d'entrée de CRL

Une extension d'entrée de CRL qualifie un certificat révoqué, c'est-à-dire une entrée de la CRL. Une extension d'entrée de CRL ne qualifie que l'entrée à laquelle elle est associée et ne doit affecter que le certificat identifié dans cette entrée.

Lorsqu'une implémentation traite une CRL qui ne reconnaît pas une extension d'entrée de CRL critique, elle doit supposer, au minimum, que le certificat identifié a été révoqué, qu'il n'est plus valide et les mesures conséquentes édictées dans la PC doivent être prises.

7.2.2.2. Extensions de CRL

Une extension de CRL qualifie la CRL dans son ensemble.

Lors de la vérification d'une CRL, aucune supposition ne doit être faite sur le fait que la liste des certificats est ordonnée ou non, sauf si cela est une clause de la PC. Le fait d'imposer le tri des certificats inclus dans une CRL peut réduire le temps de parcours de ces listes.

8. ADMINISTRATION DES SPÉCIFICATIONS

8.1. PROCEDURE DE MODIFICATION DE CES SPECIFICATIONS

Cette PC est revue régulièrement pour assurer sa conformité aux normes de sécurité et à l'évolution des mises en œuvre du marché.

Toute évolution est validée par le Comité de Direction du GIP « CPS » puis approuvée par son Conseil d'Administration ou par son Assemblée Générale.

8.2. PROCEDURE DE PUBLICATION ET NOTIFICATION

Ce document est disponible en version électronique sur le site Internet de l'AC « CPS », à l'adresse URL suivante :

http ://www.gip-cps.fr

8.3. PROCEDURES D'APPROBATION DE LA DPC

La validation de la DPC correspondante ainsi que la vérification de sa conformité avec la présente PC sont de la responsabilité du Comité de Direction (CODIR) du GIP « CPS ».

ANNEXE 1

DOCUMENTS DE RÉFÉRENCE

DOCUMENTS DE NATURE JURIDIQUE

Renvoi	Titre du document / Référence
[Arrêté CC GIP « CPS »]	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 ».
[Arrêté CPS]	Arrêté du 9 avril 1998 relatif aux spécifications physiques et logiques de la Carte de Professionnel de Santé.
[Arrêté 17031999]	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.
[Article28 Loi 90-1170]	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.
[Décret 98-102]	Décret définissant les conditions dans lesquelles sont agréés les organismes gérant, pour le compte d'autrui, des conventions secrètes de cryptologie en application de l'article 28 de la loi n° 90-1170 du 29 décembre 1990 modifiée, sur la réglementation des télécommunications, n° 98-102 du 24 février 1998.
[Décret 98-271]	Décret 98-271 du 9 avril 1998 relatif à la carte de professionnel de santé et modifiant le code de la sécurité sociale et de la santé publique.
[Décret 99-200]	Décret n° 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable.
[Décret 99-999]	Décret n° 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.
[Décret 2001-272]	Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, J.O. Numéro 77 du 31 mars 2001 page 5070
[Directives 95/46/CE – 97/66/CE]	Directives du Parlement Européen et du Conseil concernant : - la protection des données à caractère personnel ; - le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications..
[Directive 1999/93/CE]	Directive 1999/93/CE du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques.
[Loi 2000-230]	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.
[Ordonnance 96-345]	Ordonnance 96-345 du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins.
[PRMX9802730A]	Arrêté définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fournitures d'un moyen ou d'une prestation de cryptologie, n° PRMX9802730A du 13 mars 1998.
[PRMX9802731A]	Arrêté définissant la forme et le contenu du dossier de demande d'agrément, n° PRMX9802731A du 13 mars 1998.
[PRMX9802732A]	Arrêté définissant le modèle de notification préalable par le fournisseur des identités des intermédiaires utilisés pour la fourniture des moyens ou prestations de cryptologie soumis à autorisation, n° PRMX9802732A du 13 mars 1998.
[PRMX9802733A]	Arrêté fixant la liste des organismes agréés pouvant recevoir dépôt des conventions

	secrètes à l'issue de la période de quatre ans, suite à la cessation d'activité ou suite au retrait de l'agrément, n° PRMX9802733A du 13 mars 1998.
[PRMX9802734A]	Arrêté fixant la base du tarif forfaitaire définissant les frais de mise en œuvre des conventions secrètes, n° PRMX9802734A du 13 mars 1998.

DOCUMENTS DE NATURE NORMATIVE

Renvoi	Version	Date	Titre du document / Référence
[PC²]	2.2	Janvier 2001	Procédures et Politiques de Certification de Clés – PC^2 – Commission Interministérielle pour la Sécurité des Systèmes d'Information.
[PC-Type]	2.0	Décembre 1999	Politique de Certification type émise par le MINEFI
[RFC2527]		Mars 1999	Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework
[RFC2459]		Janvier 1999	Internet X.509 Public Key Infrastructure Certificate and CRL Profile
[Rôles_IGC]	1.0	Mars 1999	Rôle des exploitants d'une Infrastructure de Gestion de clés (origine : CISSI)
[X.509]		Juillet 1996	ISO / IEC 9594-8 / ITU-T. Recommandation X.509.

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
[PUC]			Protocole d'usage de la carte des professionnels de santé
[Tables]		Juillet 2000	Tables de validation des informations par les Autorités Compétentes.
[Distr_Cartes_CPS2]		Novembre 2000	Groupe de Travail « Procédures de Distribution des cartes de la famille CPS »
[X.509_CRL_CPS]	2.1	Septembre 2001	Les certificats X.509 et les CRL du système CPS.
[Accès_Annuaire]	1.5	Octobre 2001	Charte d'Accès à l'annuaire.
[DPC]	1.0	Novembre 2001	Déclaration des Pratiques de Certification

ANNEXE 2

GLOSSAIRE ET ACRONYMES

Glossaire

A - LES DIFFÉRENTS ACTEURS D'UNE INFRASTRUCTURE DE GESTION DE CLÉS

Accepteur : toute entité (personne physique, personne morale ou process) 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 un certificat d'AC intermédiaire, lui-même signé par la clé privée du certificat racine de l'AC « 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 d'Enregistrement (AE) : composante de l'IGC qui vérifie les données propres au demandeur ou porteur de certificat, ainsi que les contraintes liées à l'usage d'un certificat, conformément à la politique de certification. L'utilisation d'une AE dans une IGC n'est pas obligatoire. Ses services peuvent être directement fournis par une AC [PC²].

Autorité Compétente : 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 ».

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.

Opérateur de Certification : entité sous traitant, pour le compte de l'AC et sous son contrôle, les fonctions opérationnelles de création et d'attribution des certificats. Cette autorité peut, facultativement, créer les clés d'utilisateur.

Partenaire : promoteur d'application ou Opérateur de réseau

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

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 CRL, sur la période de validité d'un certificat ou la date d'émission d'une CRL. 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 (CRL). 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.

Utilisateur Final : porteur ou accepteur de certificat.

B - OBJETS

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 intermédiaire, dont la clé privée est utilisée par l'AC 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 utilisateur, 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 utilisateur, servant à l'établissement de sessions sécurisées entre deux utilisateurs.

Boîtier de sécurité : boîtier cryptographique ayant subi une évaluation sécuritaire, 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.

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.

DeltaCRL : CRL particulière ne contenant que les changements intervenus depuis la publication de la dernière CRL 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 du hach [PC²].

Famille de cartes CPS : elle est composée des types de cartes suivants :

- ✓ CPS : Carte de Professionnel de Santé, réservée aux Professionnels de Santé réglementés par le code de la santé publique.
- ✓ CPF : Carte de Professionnel de Santé en Formation.
- ✓ CDE : Carte de Directeur d'Etablissement.
- ✓ CPE : Carte de Personnel d'Etablissement pour les personnes employées par :
  - ✗ un établissement de santé répertorié par son n° FINESS,

- ✗ une société d'exercice libéral répertorié par son n° SIREN ou SIRET,
- ✗ un Professionnel de Santé (exemple : secrétaire médicale, ..) répertorié par son n° d'identification cabinet.

✓ CPA : Carte de Personnel Autorisé pour les personnes employées par des établissements qui ne rentrent pas dans la catégorie d'établissements pouvant déployer des CPE. L'autorisation des établissements est sous la responsabilité du Ministère de l'Emploi et de la Solidarité.

Infrastructure de gestion de clés (IGC) : ensemble organisé de composantes fournissant divers types de prestations, dans le but de permettre d'effectuer des opérations au moyen de clés publiques au profit d'utilisateurs.

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

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.

C - ACTIONS

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.

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

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.

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.

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.

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.

Acronymes

AC	Autorité de Certification
AE	Autorité d'Enregistrement
CC	Critères Communs
CDE	Carte de Directeur d'Etablissemement
CISSI	Commission Interministérielle pour la Sécurité des Systèmes d'Information
CODIR	Comité de Direction du GIP « CPS »
CPA	Carte de Personnel Administratif
CPE	Carte de Personnel d'Etablissement
CPF	Carte de Personnel en Formation
CPS	Carte de Professionnel de Santé
CRL	Certificats Revocation List (Liste des Certificats Révoqués)
CSR	Requête de Certificat Serveur
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DPC	Déclaration relative aux Pratiques de Certification
FQDN	Fully Qualified Domain Name
GIP «CPS»	Groupement d'Intérêt Public « Carte de Professionnel de Santé »
IGC	Infrastructure de Gestion de Clés.
OID	Object Identifier
PC	Politique de Certification
PC²	Procédures et Politiques de Certification de Clés
PP	Profil de Protection
PS	Professionnel de Santé
RSA	Rivest Shamir Adelman
URL	Unique Resource Locator