Politique de Certification de l'IGC-Santé

ACI Gamme ELEMENTAIRE / Domaine ORGANISATIONS

1.2.250.1.213.1.7.1.1.2.8.1 (EL-ORG-CL-SMIME)

Identification du document	
Référence	PC-EL-ORG-CL-SMIME-V1.1
Date de création	13/10/2015
Date de dernière mise à jour	25/06/2018
Etat	Validé
Version	1.1
Classification	Non sensible public
Nombre de pages	67

Historique du document			
Version	Date	Auteur	Commentaires
V 1.0	19/02/2016	ASIP Santé	Première version publiée
V 1.1	25/06/2018	ASIP Santé	Mise à jour mineure (précisions et corrections).

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
T.+33 (0)1 58 45 32 50
esante.gouv.fr

Agir ensemble pour soigner mieux

Sommaire

1 Introduction

1.1 Présentation générale

La création de l'ASIP Santé (Agence des Systèmes d'Information Partagés de Santé) en 2009 témoigne de la volonté des pouvoirs publics de renforcer la maîtrise d'ouvrage publique des systèmes d'information qui se développent dans le secteur de la santé et d'accompagner l'émergence de technologies numériques afin d'améliorer l'accès aux soins tout en veillant au respect des droits des patients.

L'ASIP Santé est notamment en charge de la gestion de la Carte de Professionnel de Santé (CPS) et contribue au développement de la télésanté.

L'ASIP Santé offre des services de certification ayant pour objectif la mise en œuvre de fonctions de sécurité (authentification, signature, chiffrement) pour les échanges dématérialisés entre les différents acteurs des domaines de la santé et du médico-social.

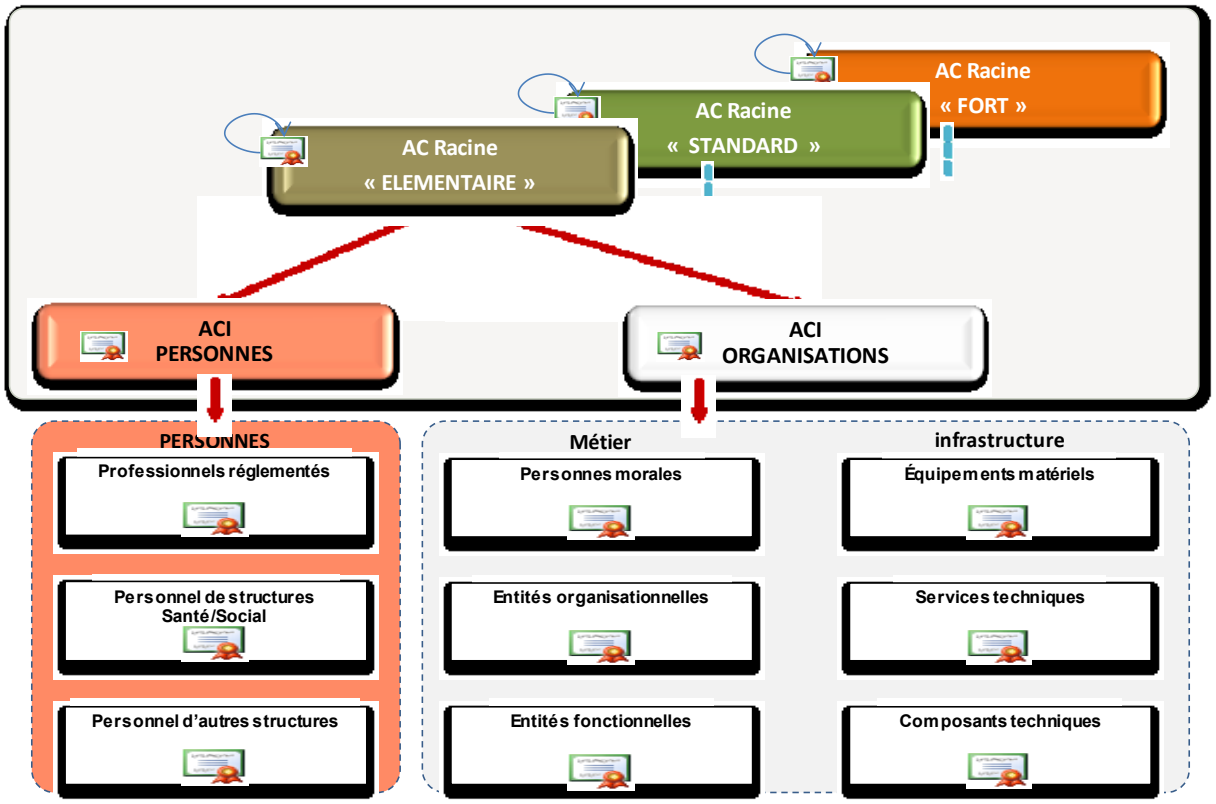
L'ASIP Santé met en œuvre une Infrastructure de Gestion de Clés (IGC), appelée IGC-Santé, afin de gérer les certificats présents sur les Cartes de Professionnels de Santé ainsi qu'une offre de certificats logiciels. Les services offerts par l'IGC-Santé offrent ainsi des moyens pour sécuriser les échanges dématérialisés de données de santé, et participent ainsi à la mise en application de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) élaborée par l'Etat.

Les certificats finaux des porteurs ou services applicatifs sont gérés par des Autorités de Certification Intermédiaires (ACI)[1] « en ligne » structurées en fonction des domaines adressés (Personnes et Organisations). Ces ACI sont signées par des Autorités de Certification Racines (ACR) « hors ligne » qui représentent le niveau de confiance des certificats regroupés en gammes (Elémentaire, Standard et Fort).

La hiérarchie d'Autorités de Certification (AC) est la suivante :

- 3 ACR (une gamme par niveau de confiance).
- 2 ACI pour chaque ACR (un domaine pour les certificats destinés à des porteurs, et un domaine pour des certificats destinés à des services applicatifs).

[1] Le terme Autorité de Certification Fille (ACF) peut également être utilisé. Pour des raisons de compatibilité avec le corpus documentaire de l'ASIP Santé, le terme ACI est utilisé dans la suite du document.



Hiérarchie d'AC de l'IGC-Santé

La structure de cette PC est conforme au [RFC3647].

1.2 Identification du document

Ce document constitue l'une des Politiques de Certification (PC) de l'ACI « gamme ELEMENTAIRE / domaine ORGANISATIONS » de l'IGC-Santé. Il est la propriété de l'ASIP Santé.

Cette PC couvre les exigences de sécurité relatives à la gestion du cycle de vie de certificats logiciels et bi-clés associés émis à des fins de cachet et de chiffrement pour des serveurs, dans le cadre d'échange de données par messagerie sécurisée.

Lorsque la précision est nécessaire dans ce document, ce type de certificat est désigné sous la référence EL-ORG-CL-SMIME.

Le numéro d'OID[2] correspondant à cette PC est 1.2.250.1.213.1.7.1.1.2.8.1.

[2] La structure des OID des PC de l'IGC-Santé est « 1.2.250.1.213.1.7.1.g.d.t.v » où : 1.2.250.1.213.1.7.1 désigne les PC de l'IGC-Santé, « g » désigne la gamme (1 = Elémentaire, 2 = Standard, 3 = Fort), « d » désigne le domaine (1 = Personnes, 2 = Organisations), « t » désigne le type de certificat, et « v » désigne le numéro de version majeure de la PC.

1.3 Définitions et acronymes

Ce chapitre détaille des acronymes et donne des définitions valables pour toute l'IGC. Si certains ne sont pas utilisés dans la présente Politique de Certification, ils le sont dans d'autres.

1.3.1 Acronymes

Les acronymes utilisés dans la présente Politique de Certification sont les suivants :

AC	Autorité de Certification
ACI	Autorité de Certification Intermédiaire
ACR	Autorité de Certification Racine
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CPS	Carte de Professionnel de Santé
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
LDAP	Lightweight Directory Access Protocol
MC	Mandataire de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OSC	Opérateur de Services de Certification
PC	Politique de Certification
PSCE	Prestataire de Services de Certification Electronique
RC	Responsable du Certificat du service applicatif
RSA	Rivest Shamir Adelman
SHA-256	Secure Hash Algorithm 256
SP	Service de Publication
UC	Utilisateur de certificat

1.3.2 Définitions

Agence : Dans ce document, le terme Agence désigne l'ASIP Santé.

Applications utilisatrices : Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat, ou des besoins d'authentification, de cachet ou de chiffrement du service applicatif auquel le certificat est rattaché.

Audit : Contrôle indépendant des enregistrements et activités d'un système afin d'évaluer la pertinence et l'efficacité des contrôles du système, de vérifier sa conformité avec les politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures.

Autorité de Certification : Autorité à qui un ou plusieurs utilisateurs se fient pour créer et attribuer des certificats. [ISO/IEC 9594-8; ITU-T X.509].

Autorité d'Enregistrement : Autorité chargée de vérifier et valider les informations d'identité nécessaire à l'établissement d'un certificat.

Autorité d'Enregistrement Déléguée : Unité de proximité à laquelle l'AE délègue tout ou partie de ses fonctions.

Bi-clé : Paire de clés asymétriques, constituée d'une clé publique et de la clé privée correspondante.

Cachet serveur : Signature numérique effectuée par un serveur applicatif sur des données dans le but de pouvoir être utilisée soit dans le cadre d'un service d'authentification de l'origine des données, soit dans le cadre d'un service de non répudiation dans le cadre d'échanges dématérialisés.

Cérémonie de clés : Une procédure par laquelle une bi-clé d'AC est générée et/ou sa clé publique certifiée. Le terme est aussi utilisé pour toutes les procédures ultérieures où des parts de secrets d'IGC doivent être utilisées pour gérer ou manipulée la clé privée d'AC.

Certificat : Clé publique d'une entité (personne physique ou service applicatif), ainsi que d'autres informations, rendues impossibles à contrefaire grâce au chiffrement par la clé privée de l'autorité de certification qui l'a émis [ISO/IEC 9594-8; ITU-T X.509].

Certificat autosigné : Certificat d'AC signé par la clé privée de cette même AC.

Chemin de certification (ou chaîne de confiance, ou chaîne de certification) : Chaîne constituée de multiples certificats nécessaires pour valider un certificat.

Clé privée : Clé de la bi-clé asymétrique d'une entité qui doit être uniquement utilisée par cette entité [ISO/IEC 9798-1].

Clé publique : Clé de la bi-clé asymétrique d'une entité qui peut être rendue publique. [ISO/IEC 9798-1].

Compromission : Violation, avérée ou soupçonnée, d'une politique de sécurité, au cours de laquelle la divulgation non autorisée, ou la perte de contrôle d'informations sensibles, a pu se produire. En ce qui concerne les clés privées, une compromission est constituée par la perte, le vol, la divulgation, la modification, l'utilisation non autorisée, ou d'autres compromissions de la sécurité de cette clé privée.

Confidentialité : La propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus [ISO/IEC 13335-1:2004].

Déclaration des Pratiques de Certification : Une déclaration des pratiques qu'une entité (agissant en tant qu'Autorité de Certification) utilise pour approuver ou rejeter des demandes de certificat (émission, gestion, renouvellement et révocation de certificats). [RFC 3647].

Disponibilité : La propriété d'être accessible sur demande, à une entité autorisée [ISO/IEC 13335-1:2004].

Données d'activation : Des valeurs de données, autres que des clés, qui sont nécessaires pour exploiter les modules cryptographiques ou les éléments qu'ils protègent et qui doivent être protégées (par ex. un PIN, une phrase secrète, …).

Fonction de hachage : Fonction qui lie des chaînes de bits à des chaînes de bits de longueur fixe, satisfaisant ainsi aux trois propriétés suivantes :

- Il est impossible, par un moyen de calcul, de trouver, pour une sortie donnée, une entrée qui corresponde à cette sortie.
- Il est impossible, par un moyen de calcul, de trouver, pour une entrée donnée, une seconde entrée qui corresponde à la même sortie [ISO/IEC 10118-1].
- Il est impossible par calcul, de trouver deux données d'entrées différentes qui correspondent à la même sortie.

Infrastructure de Gestion de Clés : Egalement appelée Infrastructure à Clé Publique (ICP), c'est l'infrastructure requise pour produire, distribuer, gérer et archiver des clés, des certificats et des Listes de Certificats Révoqués ainsi que la base dans laquelle les certificats et les LCR/LAR doivent être publiés. [2nd DIS ISO/IEC 11770-3].

Intégrité : Fait référence à l'exactitude de l'information, de la source de l'information, et au fonctionnement du système qui la traite.

Liste de Certificats Révoqués : Liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus valables ou qui ne sont plus dignes de confiance. La liste contient l'identité de la LCR d'AC, la date de publication, la date de publication de la prochaine LCR et les numéros de série des certificats révoqués. Quand la liste contient uniquement des certificats d'AC, le terme Liste des Autorités Révoquées (LAR) est utilisé.

Modules cryptographiques : Un ensemble de composants logiciels et matériels utilisés pour mettre en œuvre une clé privée afin de permettre des opérations cryptographiques (signature, chiffrement, authentification, génération de clé…). Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée (FIPS ou critères communs), utilisée pour conserver et mettre en œuvre la clé privée d'AC.

Période de validité d'un certificat : La période de validité d'un certificat est la période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat. [RFC 2459].

Plan de secours (après sinistre) : Plan défini par une AC pour remettre en place tout ou partie de ses services d'IGC après qu'ils aient été endommagés ou détruits à la suite d'un sinistre, ceci dans un délai défini dans l'ensemble PC/DPC.

Point de distribution de LCR/LAR : Entrée de répertoire ou une autre source de diffusion des LCR. Une LCR diffusée via un point de distribution de LCR peut inclure des entrées de révocation pour un sous-ensemble seulement de l'ensemble des certificats émis par une AC, ou peut contenir des entrées de révocations pour de multiples AC. [ISO/IEC 9594-8; ITU-T X.509].

Politique de Certification : Ensemble de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou une classe d'applications possédant des exigences de sécurité communes. [ISO/IEC 9594-8; ITU-T X.509].

Politique de sécurité : Ensemble de règles édictées par une autorité de sécurité et relatives à l'utilisation, la fourniture de services et d'installations de sécurité [ISO/IEC 9594-8; ITU-T X.509].

Porteur de certificat : Personne physique identifiée dans le certificat et qui est la détentrice de la clé privée correspondant à la clé publique.

Porteur de secret : Personne qui détient une donnée d'activation liée à la mise en œuvre de la clé privée d'une AC à l'aide d'un module cryptographique.

Prestataire de Services de Certification Electronique : Un PSCE se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs, RC et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondants à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Intermédiaires). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ « issuer » du certificat.

Qualificateur de politique : Des informations concernant la politique qui accompagnent un identifiant de politique de certification (OID) dans un certificat X.509. [RFC 3647]

Responsable du Certificat : Personne en charge et responsable du certificat électronique de service applicatif.

RSA : Algorithme cryptographique à clé publique inventé par Rivest, Shamir et Adleman.

Structure : Personne morale pouvant être identifiée dans les certificats de l'IGC (établissements de santé, structures « autorisées » par l'AC…)

Structure de rattachement : structure dont dépend une personne physique (via un contrat de travail, au travers d'une sous-traitance, au travers d'une déclaration d'activité pour un PS…).

Validation de certificat électronique : Opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de certification (AC) et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC et la vérification de la signature électronique de l'ensemble des AC contenues dans le chemin de certification. La validation d'un certificat électronique nécessite au préalable de choisir le certificat racine autosigné qui sera pris comme référence de confiance.

1.4 Entités intervenant dans l'IGC

1.4.1 Autorités de certification

Remarque :

Ce chapitre est commun à toutes les PC de l'IGC-Santé. C'est pourquoi il mentionne des fonctions, des entités ou des personnes physiques qui peuvent par la suite ne pas être évoquées dans cette PC particulière. Typiquement, la notion de « porteur » ne s'applique qu'aux PC des domaines PERSONNES, et les notions de « responsable du certificat » et de « service applicatif identifié dans le certificat » ne s'appliquent qu'aux PC des domaines ORGANISATIONS.

L'ASIP Santé, en tant que Prestataire de Services de Certification Electronique, a en charge la fourniture des prestations de gestion des certificats d'ACR, d'ACI et de porteurs ou services applicatifs finaux, tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation, ...) et s'appuie pour cela sur une infrastructure technique : l'Infrastructure de Gestion de Clés.

Les prestations d'une AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats.

La décomposition fonctionnelle d'une IGC qui est retenue dans cette PC est la suivante[3] :

- Autorité d'enregistrement (AE)[4] - Cette fonction vérifie les informations d'identification du futur porteur d'un certificat, ou du futur responsable du certificat (RC) et du service applicatif auquel le certificat doit être rattaché, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. L'AE a également en charge, lorsque cela est nécessaire, la revérification des informations du porteur, ou du RC et du service applicatif lors du renouvellement du certificat. Dans le cadre de l'IGC-Santé, la notion d'autorité d'enregistrement déléguée (AED) est aussi utilisée (cf. chapitre 1.4.2).
- Fonction de génération des certificats - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'AE et de la clé publique du porteur provenant du porteur, ou de la clé publique du service applicatif provenant du RC.
- Fonction de génération des éléments secrets du porteur ou du service applicatif - Cette fonction génère les éléments secrets à destination du porteur ou du RC, lorsque l'AC a en charge une telle génération, et les prépare en vue de leur remise au porteur ou au RC. Ces éléments secrets sont par exemple la bi-clé du porteur ou du service applicatif et les données d'activation.
- Fonction de remise au porteur ou au RC - Cette fonction remet au porteur son certificat, ou au RC le certificat du service applicatif.
- Fonction de publication - Cette fonction met à disposition des différentes parties concernées les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs, aux RC et/ou utilisateurs de certificats, hors informations d'état des certificats. Elle met également à disposition les certificats valides des porteurs et des services applicatifs.
- Fonction de gestion des révocations - Cette fonction traite les demandes de révocation (notamment l'identification et l'authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
- Fonction d'information sur l'état des certificats - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqué, valide, etc.). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, deltaLCR) et également selon un mode requête / réponse temps réel (OCSP).

Un certain nombre d'entités ou de personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

[3] Cette décomposition fonctionnelle est celle proposée dans les « PC type » du RGS, mais seules les fonctions applicables aux PC de l'IGC-Santé sont listées.

[4] Les documents de l'ETSI utilisent le terme Service d'Enregistrement. Le [RFC3647] utilise le terme Autorité d'Enregistrement. Dans ce document, le terme Autorité d'Enregistrement est retenu ; il doit être compris en tant que fonction et non pas en tant que composante technique de l'IGC.

- Porteur – La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est contenue dans le certificat.
- Responsable du certificat (RC) – La personne physique responsable du certificat électronique de service applicatif, notamment de l'utilisation du certificat et de la bi-clé correspondante, pour le compte de l'entité dont dépend le service applicatif identifié dans le certificat.
- Mandataire de certification (MC) – Le mandataire de certification est désigné par une structure cliente de l'IGC-Santé (pour laquelle des demandes de certificats sont effectuées). Il effectue les démarches auprès de l'AC pour le compte du porteur rattaché à la structure. Il s'assure de la remise au porteur de son certificat, et d'éventuels autres éléments associés au certificat.
- Utilisateur de certificat – L'entité ou la personne physique qui reçoit un certificat et qui s'y fie – selon le type de certificat – pour :
  - Vérifier une signature électronique ou une valeur d'authentification provenant du porteur du certificat.
  - Chiffrer des données à destination du porteur du certificat.
  - Vérifier une valeur de cachet ou d'authentification serveur provenant du service applicatif auquel le certificat est rattaché, ou pour établir une clé de session.
  - Chiffrer des données à destination du service applicatif auquel le certificat est rattaché.

La présente PC définit les exigences de sécurité pour toutes les fonctions de l'IGC décrites ci-dessus afin de délivrer des certificats à des porteurs ou à des services applicatifs.

La Déclaration des Pratiques de Certification (DPC) décrit l'organisation opérationnelle de l'IGC et la répartition des rôles en fonction des exigences décrites dans cette PC.

La mise en œuvre opérationnelle des différentes fonctions est effectuée par plusieurs composantes de l'IGC.

Le service de publication (SP) est la composante de l'IGC qui rend disponible les certificats de clés publiques, les LCR et les deltaLCR émis par l'AC, aux utilisateurs finaux et aux utilisateurs de certificat conformément à la PC. Le SP est donc une composante qui participe à la mise en œuvre des fonctions de publication et d'information sur l'état des certificats.

Dans le cadre de cette PC, certaines composantes de l'IGC ne sont pas opérées par l'AC.

Composantes de l'IGC opérées par l'AC

L'AC est l'autorité chargée de créer et d'attribuer les certificats. Dans le cadre de l'IGC-Santé, l'AC est toujours l'ASIP Santé.

La Direction Générale de l'ASIP Santé porte la responsabilité de l'AC de l'IGC-Santé et possède un pouvoir décisionnaire au sein de l'IGC-Santé. Dans ce document, la Direction Générale de l'ASIP Santé – lorsqu'elle agit dans ce rôle de responsable et décisionnaire – est désignée sous le terme « Responsable de l'IGC ». Pour l'assister dans ce rôle, elle met en place une organisation interne spécifique.

Le Responsable de l'IGC est le responsable de la mise en œuvre opérationnelle de l'AC. Il définit le référentiel de sécurité, garantit sa cohérence et sa gestion, ainsi que sa mise en application.

Le référentiel de sécurité de l'AC est composé de la présente PC, de la DPC associée et des procédures mises en œuvre par les composantes de l'IGC.

Le Responsable de l'IGC valide le référentiel de sécurité composé de la présente PC et de la DPC associée. Il suit les audits et/ou contrôles de conformité effectués sur les composantes de l'IGC, décide des actions à mener et veille à leur mise en application.

La DPC précise l'organisation interne mise en place pour assister le Responsable de l'IGC dans son rôle.

Composantes de l'IGC opérées par une entité externe : OSC

L'Imprimerie Nationale a le rôle d'Opérateur de Services de Certification (OSC), en application du décret n° 2012-1117 du 2 octobre 2012 relatif à l'intégration de la carte de professionnel de santé dans le monopole de l'Imprimerie Nationale.

L'OSC assure les fonctions dont la mise en œuvre opérationnelle lui a été confiée par le Responsable de l'IGC, ainsi que les prestations techniques associées à ces fonctions, en particulier cryptographiques, nécessaires au processus de certification, conformément à la présente PC et à la DPC associée.

Il s'agit des fonctions suivantes :

- Fonction de génération des certificats.
- Fonction de génération des éléments secrets du porteur ou du service applicatif (uniquement pour les certificats délivrés par l'AC avec un dispositif de protection des éléments secrets[5]).
- Fonction de remise au porteur ou au RC.
- Fonction de gestion des révocations :
    - Pour ce qui concerne les certificats logiciels[6], entièrement
    - Pour ce qui concerne les certificats délivrés par l'AC avec un dispositif de protection des éléments secrets, partiellement (l'AC reçoit les demandes de révocation et commence à les traiter, seules les demandes acceptées par l'AC sont ensuite transmises à l'OSC).
- Fonction d'information sur l'état des certificats, uniquement pour le mode requête / réponse temps réel (OCSP)[7].

Le Responsable de l'IGC reste in fine responsable vis-à-vis de toute partie externe à l'IGC (utilisateurs, autorités publiques, etc.) des prestations fournies et garantit le respect des engagements, pris dans cette PC et la DPC correspondante, relatifs à son activité de certification.

Dans la présente PC, le rôle et les obligations de l'OSC ne sont pas distingués de ceux de l'AC. La distinction est faite dans la DPC.

Composantes de l'IGC opérées par une entité externe : AE

[5] Dans les PC de l'IGC-Santé, les types de certificats correspondants aux certificats délivrés par l'AC avec un dispositif de protection des éléments secrets sont ceux pour lesquels une partie de la référence est « CPx ».

[6] Dans les PC de l'IGC-Santé, les types de certificats correspondants aux certificats logiciels sont ceux pour lesquels une partie de la référence est « CL ».

[7] L'ASIP Santé assure elle-même la fonction d'information sur les certificats via LCR et/ou deltaLCR, sur la base des éléments transmis par l'OSC.

L'AE peut parfois être une entité externe à l'ASIP Santé (cf. chapitre 1.4.2 qui apportera des précisions si les certificats émis au titre de cette PC sont concernés).

1.4.2 Autorité d'Enregistrement

L'AE a pour rôle de vérifier l'identité du futur RC et les informations liées au service applicatif. Pour cela, l'AE assure les tâches suivantes :

- L'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC suivant l'organisation de cette dernière et les prestations offertes.
- L'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage).
- La conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du RC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).
- La prise en compte et la vérification des informations du futur RC, du service applicatif et de leur structure de rattachement et la constitution du dossier d'enregistrement correspondant.

L'AE est toujours l'ASIP Santé.

L'ASIP Santé délègue certaines de ses fonctions d'AE à des unités de proximité dans les structures clientes. Ces unités de proximité sont désignées sous le nom d'autorités d'enregistrement déléguées (AED). L'AED est le directeur ou responsable de la structure concernée, et toute autre personne qu'il pourrait avoir désigné à l'AE pour l'assister dans ce rôle.

Les fonctions que l'AE de l'ASIP Santé délègue aux AED sont celles liées :

- A l'enregistrement des RC et des services applicatifs.
- Au rattachement de ces RC et services applicatifs à la structure.

1.4.3 Porteurs de certificats

Sans objet.

1.4.4 Responsables de certificats électroniques de services applicatifs

Un RC est une personne physique qui est responsable de l'utilisation du certificat électronique et de la clé privée correspondant à ce certificat, pour le compte de la structure également identifiée dans ce certificat. Le RC a un lien contractuel, hiérarchique ou réglementaire avec cette entité.

Le RC doit respecter les conditions qui lui incombent définies dans cette PC.

Le certificat étant attaché au service applicatif et non au RC, ce dernier peut être amené à changer en cours de validité du certificat. L'entité doit signaler préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RC et lui désigner un successeur.

1.4.5 Utilisateurs de certificats

L'utilisateur d'un certificat peut-être notamment :

- Un usager destinataire de données signées par un service applicatif de cachet et qui utilise le certificat électronique du cachet ainsi qu'un module de vérification de cachet afin d'authentifier l'origine de ces données transmises.
- Un service applicatif destinataire de données provenant d'un autre service applicatif et qui utilise le certificat électronique de cachet et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises.
- Un service en ligne qui utilise un dispositif de chiffrement pour chiffrer des données ou un message à destination du service applicatif identifié dans le certificat.
- Une personne qui émet un message chiffré à l'intention du service applicatif identifié dans le certificat électronique.

1.4.6 Mandataire de certification

Sans objet.

1.5 Usage des certificats

1.5.1 Domaines d'utilisation applicables

Les certificats émis par l'IGC-Santé ont vocation à être utilisé pour répondre à des besoins de sécurité dans les domaines de la santé et du médico-social.

Toutefois l'usage des certificats émis par l'IGC-Santé est également autorisé pour d'autres domaines d'activité mais la responsabilité de l'ASIP Santé ne saurait être engagée dans ce cadre particulier (voir chapitre 9.8).

Usages des certificats électroniques des services applicatifs

Les usages sont ceux de la messagerie électronique sécurisée :

- La signature électronique de messages électroniques.
- Le déchiffrement : à l'aide de sa clé privée, un service applicatif déchiffre les messages électroniques qui lui ont été transmis dans le cadre d'échanges dématérialisés, chiffrés à partie de sa clé publique.
- Le chiffrement : à l'aide de la clé publique du service applicatif destinataire, une personne ou un service applicatif chiffre des messages électroniques.

Cela couvre notamment le cas de chiffrement par une clé symétrique de fichiers ou de messages, clé elle-même protégée par un mécanisme cryptographique asymétrique, type RSA (chiffrement de la clé symétrique par la clé publique du service applicatif et déchiffrement par sa clé privée) ou de type Diffie-Hellman (obtention de la clé symétrique, par l'émetteur d'un message, via un algorithme combinant la clé privée de l'émetteur et la clé publique du destinataire, et inversement pour l'obtention de cette clé symétrique par le destinataire du message).

Niveaux de sécurité

Les certificats électroniques objets de la présente PC sont utilisés par des applications pour lesquelles les besoins de sécurité sont moyens eu égard aux risques qui les menacent.

1.5.2 Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.5. L'AC respecte ces restrictions et impose leur respect par les RC auxquels elle délivre des certificats de service applicatif et les utilisateurs de ces certificats.

À cette fin elle communique à tous les RC et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

1.6 Gestion de la PC

1.6.1 Entité gérant la PC

Le Responsable de l'IGC est responsable de la validation et de la gestion de la présente PC.

1.6.2 Point de contact

Le point de contact est :

ASIP Santé

Responsable de l'IGC-Santé

9 rue Georges Pitard 75015 Paris

e-mail : Responsable-IGC-Sante@asipsante.fr

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

Le Responsable de l'IGC a l'autorité et la responsabilité finale pour déterminer la conformité de la DPC avec la PC.

1.6.4 Procédures d'approbation de la conformité de la DPC

Le Responsable de l'IGC définit le processus d'approbation de la conformité de la DPC avec la PC.

Le Responsable de l'IGC est responsable de la gestion (mises à jour, révisions) de la DPC. Toute demande de mise à jour de la DPC suit le processus d'approbation mis en place.

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 RC et des utilisateurs de certificats, l'AC met en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats (cf. chapitre 1.4).

La fonction de publication s'appuie sur :

- Une architecture web, accessible au travers de requêtes HTTP (certificats et autres informations).

- Un service d'annuaire accessible au travers de requêtes LDAP (certificats uniquement).

La fonction d'information sur l'état des certificats s'appuie sur :

- Une architecture web, accessible au travers de requêtes HTTP (LCR et serveur OCSP).
- Un service d'annuaire accessible au travers de requêtes LDAP (LCR et deltaLCR).

2.2 Informations devant être publiées

L'AC publie les informations du tableau suivantes à destination des RC et utilisateurs de certificats :

Informa-tion	Fonction de l'IGC concernée	Moyen de diffusion	Commentaires
La présente PC	Publication	Serveur WEB : ➢ A l'adresse http://igc-sante.esante.gouv.fr/PC, via un lien de téléchargement.	Cette adresse figure dans les certificats émis.
LCR	Information sur l'état des certificats	Serveur WEB : ➢ A l'adresse http://igc-sante.esante.gouv.fr/PC, via un lien de téléchargement manuel. Service d'annuaire LDAP : ➢ En interrogeant le serveur annuaire-igc.esante.gouv.fr	Les adresses HTTP et LDAP permettant un accès direct aux LCR figurent dans les certificats émis.
deltaLCR	Information sur l'état des certificats	Service d'annuaire LDAP : ➢ En interrogeant le serveur annuaire-igc.esante.gouv.fr	L'adresse LDAP permettant un accès direct aux deltaLCR figure dans les certificats émis.
Certificat de l'AC en cours de validité	Publication	Serveur WEB : ➢ A l'adresse http://igc-sante.esante.gouv.fr/PC, via un lien de téléchargement manuel.	L'adresse HTTP permettant un accès direct au certificat de l'AC figure dans les certificats émis.

Informa-tion	Fonction de l'IGC concernée	Moyen de diffusion	Commentaires
Informations concernant le reste de la hiérarchie d'AC	Publication	Serveur WEB : ➢ A l'adresse http://igc-sante.esante.gouv.fr/PC. Cette page web est commune à toutes les AC de l'IGC-Santé et présente pour l'AC Racine ayant signé l'AC : le certificat en cours de validité (et, s'agissant d'un certificat autosigné, les informations permettant aux utilisateurs de s'assurer de son origine et de son état), la PC correspondante et d'éventuels documents complémentaires.	Pour plus de précisions, cf. chapitre équivalent de la PC des AC Racines de l'IGC-Santé.
Certificats en cours de validité	Publication	Serveur WEB : ➢ A l'adresse http://annuaire-igc.esante.gouv.fr/ en utilisant des formulaires de recherche Service d'annuaire LDAP : ➢ En interrogeant le serveur annuaire-igc.esante.gouv.fr	Cf. chapitre 4.4.2 sur la publication des certificats.

La page web http://igc-sante.esante.gouv.fr/PC référence aussi divers documents administratifs (dont les conditions générales d'utilisation des certificats de l'IGC-Santé) et techniques.

Les URL permettant un accès direct à la LCR sont :

- http://igc-sante.esante.gouv.fr/CRL/ACI-EL-ORG.crl
- ldap://annuaire-igc.esante.gouv.fr/cn=AC%20IGC-SANTE%20ELEMENTAIRE%20ORGANISATIONS,ou=AC%20RACINE%20IGC-SANTE%20ELEMENTAIRE,ou=IGC-SANTE,ou=0002%20187512751,o=ASIP-SANTE,c=FR?certificaterevocationlist;binary?base?objectClass=pkiCA

L'URL permettant un accès direct à la deltaLCR est :

- ldap://annuaire-igc.esante.gouv.fr/cn=AC%20IGC-SANTE%20ELEMENTAIRE%20ORGANISATIONS,ou=AC%20RACINE%20IGC-SANTE%20ELEMENTAIRE,ou=IGC-SANTE,ou=0002%20187512751,o=ASIP-SANTE,c=FR?deltarevocationlist;binary?base?objectClass=pkiCA
- L'attribut est multivalué et présente les 7 dernières deltaLCR correspondantes aux 7 dernières LCR.

L'URL permettant un accès direct au certificat de l'AC est :

- http://igc-sante.esante.gouv.fr/AC/ACI-EL-ORG.cer

L'URL permettant un accès direct au certificat de l'AC est :

- http://igc-sante.esante.gouv.fr/AC/ACR-EL.cer

2.3 Délais et fréquences de publication

Les informations liées à l'IGC (nouvelle version de la PC, etc.) sont publiées dès que nécessaire afin d'assurer à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC. Toute nouvelle version est communiquée aux AE, et est mise à disposition sur le Service de Publication. Les systèmes publiant ces informations sont au moins disponibles les jours ouvrés.

Les certificats d'AC sont diffusés préalablement à toute diffusion de certificats finaux et/ou de LCR correspondants et les systèmes les publiant ont une disponibilité de 24 heures / 24 et 7 jours / 7.

Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux chapitres 4.9 et 4.10.

La perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une indisponibilité de cette information.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès de type mot de passe basé sur une politique de gestion stricte des mots de passe, ou d'un niveau de sécurité supérieur.

3 Identification et authentification

3.1 Nommage

3.1.1 Types de noms

Les noms utilisés dans les certificats sont conformes aux spécifications de la norme X.500.

Dans chaque certificat (conforme à la norme X.509), l'AC émettrice (« issuer ») et le service applicatif (« subject ») sont identifiés par un « Distinguished Name » (DN) répondant aux exigences de la norme X.501.

La construction du DN de ces champs est précisée dans le document [GAB_ET1_ET2].

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les services applicatifs dans les certificats sont explicites. L'application de cette politique est de la responsabilité des RC lors de la demande de certificat.

Le DN contient les éléments nécessaires pour identifier l'entité à laquelle est rattaché le service applicatif.

Remarque : Le certificat est associé au service applicatif et pas au serveur physique sur lequel la bi-clé est déployée. Autrement dit, une bi-clé peut être déployée sur plusieurs machines physiques rattachées au service applicatif, ou vice-versa plusieurs bi-clés peuvent être déployées sur un même serveur hébergeant plusieurs services applicatifs.

3.1.3 Anonymisation ou pseudonymisation des services applicatifs

Sans objet.

3.1.4 Règles d'interprétation des différentes formes de nom

Les noms utilisés dans les certificats sont conformes aux spécifications de la norme X.500.

3.1.5 Unicité des noms

Le DN du champ « subject » de chaque certificat de service applicatif permet d'identifier le service applicatif de façon unique au sein du domaine de l'AC.

L'unicité est assurée par la présence dans le DN :

- De « l'identifiant national » de la structure à laquelle appartient le service applicatif, dont les règles de gestion permettent de garantir l'unicité.
- Du nom du service applicatif au niveau du CN, qui doit être identifié d'une manière évitant toute ambiguïté. L'application de cette politique est de la responsabilité des RC lors de la demande de certificat.

3.1.6 Identification, authentification et rôle des marques déposées

Le Responsable de l'IGC est responsable de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

3.2 Validation initiale de l'identité

Les données recueillies lors des processus d'enregistrement alimentent un référentiel d'identité, qui est utilisé par l'AC. La gestion des identités est gérée indépendamment de la gestion des certificats. Il n'est pas possible de garantir que l'identité présente dans le référentiel d'identité est revérifiée régulièrement.

Tous les acteurs intervenant dans le cycle de vie du certificat ont été préalablement enregistrés dans le référentiel d'identité utilisé par l'AC. Les certificats émis au titre de cette PC ne peuvent l'être que pour des RC dont l'identité a été préalablement enregistrée dans le référentiel d'identité.

3.2.1 Méthode pour prouver la possession de la clé privée

Le RC génère lui-même la bi-clé. Il fournit à l'AC une preuve de possession de sa clé privée correspondant à la clé publique contenue dans la demande de certificat.

Cette preuve est fournie via une opération technique de signature[8] à l'aide de la clé privée, que l'AC vérifie avec la clé publique transmise dans la demande.

3.2.2 Validation de l'identité d'un organisme

La validation de l'identité d'une structure (personne morale) est décrite dans le document [AE-PROCESS]. Elle est effectuée par l'ASIP Santé, agissant en tant qu'AE.

[8] Le terme « opération technique de signature » plutôt que « signature » est utilisé car il ne s'agit pas d'une réelle signature électronique. Les mêmes mécanismes cryptographiques sont utilisés, mais avec une clé publique qui n'est pas encore certifiée et sans tenir compte de l'usage final de la bi-clé.

3.2.3 Validation de l'identité d'un individu

La validation de l'identité d'un RC est décrite dans le document [AE-PROCESS]. Elle est effectuée par une AE ou une AED.

La validation d'un éventuel rattachement de ce RC à une structure est décrite dans le document [AE-PROCESS]. Elle est effectuée au sein de la structure de rattachement, par l'AED (à laquelle l'ASIP Santé délègue ces fonctions d'AE).

3.2.4 Informations non vérifiées du RC et du service applicatif

Toutes les informations d'identité des RC sont validées par les AE ou AED.

Toutes les informations relatives au service applicatif sont validées par le RC.

3.2.5 Validation de l'autorité du demandeur

Les droits d'une personne physique sont déterminés d'après les données fournies lors de l'enregistrement de ces personnes par les AE ou AED. Ces données permettent de lui attribuer des habilitations dans le référentiel d'identités.

L'autorité du demandeur est vérifiée lors du traitement de la demande de certificat en s'appuyant sur ses habilitations présentes dans le référentiel d'identités.

3.2.6 Critères d'interopérabilité

Sans objet.

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

Le renouvellement de la bi-clé d'un service applicatif entraine automatiquement la génération et la fourniture d'un nouveau certificat. De plus un nouveau certificat de service applicatif ne peut pas être fourni au RC sans renouvellement de la bi-clé correspondante (cf. chapitre 4.6).

3.3.1 Identification et validation pour un renouvellement courant

La gestion des identités est gérée indépendamment de la gestion des certificats (cf. chapitre 3.2). Il n'est pas possible de garantir que l'identité présente dans le référentiel d'identité est revérifiée régulièrement.

Dans le cadre du traitement d'un renouvellement courant de certificat, les mêmes vérifications sont effectuées que lors d'une demande initiale de certificat.

3.3.2 Identification et validation pour un renouvellement après révocation

La gestion des identités est gérée indépendamment de la gestion des certificats (cf. chapitre 3.2). Il n'est pas possible de garantir que l'identité présente dans le référentiel d'identité est revérifiée régulièrement.

Dans le cadre du traitement d'un renouvellement de certificat après révocation, les mêmes vérifications sont effectuées que lors d'une demande initiale de certificat.

3.4 Identification et validation d'une demande de révocation

La demande de révocation peut être effectuée en ligne de deux manières différentes :

- Dans un mode authentifié. L'authentification du demandeur est réalisée à l'aide d'une carte CPx.
- Dans un mode non authentifié. Le demandeur doit préciser l'AC émettrice du certificat, le numéro de série du certificat et le code de révocation (qui a été choisi par le demandeur de certificat au moment au retrait du certificat). Ce mode n'est disponible que pour les demandes de révocation effectuées via le **canal IHM**.

La demande de révocation peut aussi être demandée à l'AC via un service téléphonique. Dans ce cas, certains personnels du support de l'AC ayant des habilitations particulières réaliseront effectivement la révocation en ligne, en mode authentifié, via une fonction « agir pour un tiers ». Le personnel de l'AC effectue une authentification du demandeur en utilisant une « procédure d'authentification du déclarant » existante au sein de l'ASIP Santé. L'autorité du demandeur par rapport au certificat à révoquer est vérifiée par l'AC au moment de l'utilisation de la fonction « agir pour un tiers ».

La manière dont est récupérée l'identité du demandeur de la révocation, lorsqu'elle est effectuée en ligne et en mode authentifié, dépend du canal utilisé pour effectuer la demande.

Canal MAIL :

La personne qui effectue la demande de révocation (cf. chapitre 4.9.2) doit disposer d'une carte CPx. Il utilise cette carte pour signer la demande effectuée par mail. L'identité du demandeur est récupérée dans la signature.

Canal WEB SERVICES :

La personne qui effectue la demande de révocation (cf. chapitre 4.9.2) doit disposer d'une carte CPx. Il utilise cette carte pour signer la demande effectuée par appel web service. L'identité du demandeur est récupérée dans la signature.

Canal IHM :

La personne qui effectue la demande de révocation (cf. chapitre 4.9.2) doit disposer d'une carte CPx. Il utilise cette carte pour s'identifier et s'authentifier auprès de l'application qui permet d'effectuer la demande. L'identité du demandeur est récupérée au travers du mécanisme d'authentification.

Dans le cas particulier des demandes effectuées par le **canal MAIL**, un mail est envoyé au demandeur (adresse récupérée dans l'expéditeur du mail de demande) :

- Si la demande est mal formée, il s'agit d'un mail d'information expliquant l'origine du problème, et la demande n'est pas transmise à l'AC.
- Si la demande est correctement formée, il s'agit d'un mail d'information expliquant que la demande est « prise en compte », et la demande est transmise à l'AC.

Les certificats initialement demandés via le **canal MAIL** ne peuvent pas être révoqué en mode non authentifié via le canal IHM. En effet, aucun code de révocation ne peut être fixé par le demandeur de certificat au moment du retrait via le canal MAIL.

Les demandes correctement formées effectuées par l'un des canaux possibles sont automatiquement validées par l'AC (dans le sens où elles sont prises en compte par l'AC pour être acceptées ou rejetées).

4 Exigences opérationnelles sur le cycle de vie des certificats

Le cycle de vie des certificats est géré au travers de trois canaux :

- Le canal MAIL.
- Le canal WEB SERVICES.
- Le canal IHM.

Le principe d'utilisation de ces canaux est le suivant :

- Un certificat ne peut être retiré qu'au travers du canal au travers duquel il a été demandé.
- Un certificat peut être révoqué au travers de n'importe quel canal (quel que soit celui au travers duquel il avait été commandé).
- La délivrance d'un nouveau certificat peut être faite au travers de n'importe quel canal (quel que soit le canal au travers duquel le certificat initial avait été commandé).

Les chapitres qui suivent expliquent lorsque cela est nécessaire les particularités de chaque canal, à chaque étape du cycle de vie d'un certificat.

Le **canal MAIL** est mis en place pour l'IGC-Santé afin de limiter les impacts terrain de la migration depuis l'IGC CPS-2bis (les mécanismes mis en place par ces outils n'ont pas à évoluer, seuls quelques paramètres doivent être modifiés). Il n'est utilisable que pour les trois types de certificats de la gamme ELEMENTAIRE répondant à des besoins déjà couverts par l'IGC CPS-2bis[9].

Le canal **WEB SERVICES** et le **canal IHM** sont mis en place avec l'IGC-Santé :

- Les outils déployés sur le terrain pour automatiser les demandes devront à terme évoluer pour utiliser le canal WEB SERVICES. En effet, le canal MAIL sera à terme abandonné.
- Le canal IHM peut être utilisé pour effectuer manuellement des demandes.

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Seul le RC peut effectuer une demande de certificat.

[9] Il s'agit des types EL-PP-CL-CONF (besoin couvert dans l'IGC CPS-2bis par les certificats de CLASSE 5), et EL-ORG-CL-SSL_SERV et EL-ORG-CL-SMIME (besoin couvert dans l'IGC CPS-2bis par les certificats de CLASSE 4).

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

Une demande de certificat ne peut être effectuée que pour un service applicatif rattaché à une structure déjà enregistrée dans le référentiel d'identités tenu à jour par l'AC en fonction des données communiquées par les AED.

Techniquement, la demande de certificat est effectuée au travers de l'un des trois canaux disponibles : MAIL, WEB SERVICES ou IHM.

Le demandeur indique quel est le type de certificat souhaité.

Le demandeur est un RC effectuant une demande pour obtenir un certificat de service applicatif rattaché à une structure :

- L'Identifiant National du RC est récupéré au travers du processus d'identification décrit au chapitre 4.2.1 et qui dépend du canal utilisé pour la demande. Cet Identifiant National est utilisé comme clé pour récupérer dans le référentiel d'identités la liste des structures pour lesquelles il est RC. Ces droits ont été communiqués à l'ASIP Santé et enregistrés dans le référentiel d'identité en fonction des données communiquées par les AED des structures concernées.
- Il précise dans la demande l'Identifiant National de la structure de rattachement du service applicatif. Cet identifiant est utilisé comme clé pour récupérer dans le référentiel d'identités certaines autres informations nécessaires à l'établissement du certificat.

4.2 Traitement d'une demande de certificat

4.2.1 Exécution des processus d'identification et de validation de la demande

La manière dont est récupérée l'identité du demandeur dépend du canal utilisé pour effectuer la demande.

Canal MAIL :

La personne qui effectue la demande de certificat (cf. chapitre 4.1.1) doit disposer d'une carte CPx. Il utilise cette carte pour signer la demande effectuée par mail. L'identité du demandeur est récupérée dans la signature.

Canal WEB SERVICES :

La personne qui effectue la demande de certificat (cf. chapitre 4.1.1) doit disposer d'une carte CPx. Il utilise cette carte pour signer la demande effectuée par appel web service. L'identité du demandeur est récupérée dans la signature.

Canal IHM :

La personne qui effectue la demande de certificat (cf. chapitre 4.1.1) doit disposer d'une carte CPx. Il utilise cette carte pour s'identifier et s'authentifier auprès de l'application qui permet d'effectuer la demande. L'identité du demandeur est récupérée au travers du mécanisme d'authentification.

Dans le cas particulier des demandes effectuées par le **canal MAIL**, un mail est envoyé au demandeur (adresse récupérée dans l'expéditeur du mail de demande) :

- Si la demande est mal formée, il s'agit d'un mail d'information expliquant l'origine du problème, et la demande n'est pas transmise à l'AC.
- Si la demande est correctement formée, il s'agit d'un mail d'information expliquant que la demande est « prise en compte », et la demande est transmise à l'AC.

Les demandes correctement formées effectuées par l'un des canaux possibles sont automatiquement traitées par l'AC (dans le sens où elles sont prises en compte par l'AC pour être acceptées ou rejetées).

4.2.2 Acceptation ou rejet de la demande

La demande de certificat est acceptée :

- Après avoir vérifié dans le référentiel d'identité de l'ASIP Santé que le demandeur a bien le droit d'effectuer la demande pour la structure d'appartenance du service applicatif concerné. Il s'agit des contrôles dans le référentiel d'identité indiqués au chapitre 4.1.2.
- Après avoir contrôlé le contenu de la CSR :
  - Vérification de la preuve de possession de la clé privée.
  - Vérification que la clé publique (et donc la bi-clé) n'a jamais été utilisée dans une précédente demande.
  - Remarque : l'AC est susceptible de modifier ou compléter certains éléments de la CSR (à l'exception des clés).
- Après avoir effectué les contrôles sur les adresses mail (voir plus bas).
- Après avoir contrôlé la présence des attributs obligatoires (dépend du type de certificat).
- Après avoir contrôlé la syntaxe des différents attributs.

2 adresses mails peuvent être présentes dans la demande : l'adresse mail du demandeur et l'adresse mail de la personne à informer.

La récupération de ces adresses mail dans la demande dépend du canal de demande utilisé :

Canal de demande	**Adresse mail**	
	Du demandeur	**De la personne à informer**
Canal MAIL :	Obligatoire. L'adresse de l'expéditeur du mail est utilisée.	Non utilisée.

Canal de demande	Adresse mail	
	Du demandeur	De la personne à informer
Canal WEB SERVICES :	Obligatoire.	Facultatif.
Canal IHM :	Obligatoire.	Facultatif.

Le contrôle des adresses mail dépend de l'adresse mail concernée et du type de certificat demandé :

- Adresse mail du demandeur : pas de contrôle.
- Adresse mail de la personne à informer : pas de contrôle.
- Adresse mail éventuellement présente en tant que « nom alternatif du sujet » : l'adresse mail ne doit pas déjà être utilisée dans un certificat valide avec un DN « sujet » différent (quelle que soit l'AC de l'IGC-Santé ayant émis le certificat).

La demande est rejetée si un contrôle présente un résultat négatif. Dans ce cas, un mail d'information expliquant l'origine du problème est envoyé aux adresses mail :

- Du demandeur.
- De la personne à informer (si présente).

Le rejet est aussi notifié par un autre moyen par le canal WEB SERVICES ou le canal IHM :

Canal WEB SERVICES :

L'erreur est renvoyée dans la réponse à l'appel web service de demande.

Canal IHM :

Un message d'erreur est affiché une fois la demande soumise.

Par ailleurs, un certain nombre de contrôles ont déjà été effectués dès la saisie de la demande, avant soumission de la demande.

4.2.3 Durée d'établissement du certificat

Lorsque la demande de certificat est acceptée, l'AC est en mesure d'établir le certificat immédiatement.

Canal MAIL :

Le certificat est généré immédiatement, avant d'être envoyé par mail dans les minutes qui suivent.

Canal WEB SERVICES :

Un jeton de retrait est renvoyé dans la réponse à l'appel web service de demande. Le certificat ne sera généré qu'au moment de l'utilisation de ce jeton de retrait dans l'appel web service de retrait.

La demande de certificat est annulée par l'AC si le retrait n'est pas effectué dans les 10 jours. Dans un tel cas, le certificat demandé n'est donc jamais généré.

Canal IHM :

Un lien de retrait est envoyé par mail au demandeur dans les minutes qui suivent. Il est aussi possible pour le demandeur de procéder au retrait en se connectant à l'application. Le certificat ne sera généré qu'au moment du retrait.

La demande de certificat est annulée par l'AC si le retrait n'est pas effectué dans les 10 jours. Dans un tel cas, le certificat demandé n'est donc jamais généré.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Voir le chapitre 4.2.3 qui précise à quel moment l'AC génère le certificat.

Les conditions de génération des certificats et les mesures de sécurités respectées sont précisées aux chapitres 5 et 6.

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

Le RC est systématiquement notifié par l'AC de la délivrance des certificats, et cette notification dépend du canal utilisé pour la demande.

Canal MAIL :

Un mail contenant le certificat est envoyé à l'adresse mail du demandeur (donc du RC).

Canal WEB SERVICES et canal IHM :

Un mail d'information indiquant que le certificat a été retiré est envoyé à l'adresse mail du demandeur (donc du RC).

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Canal MAIL :

L'acceptation du certificat est tacite à compter de la date d'envoi du certificat.

Canal WEB SERVICES :

L'acceptation du certificat est tacite à compter de la date d'envoi du certificat dans la réponse à l'appel Web Service de retrait.

Canal IHM :

L'acceptation du certificat est tacite à compter de la date de téléchargement du certificat.

4.4.2 Publication du certificat

Tous les certificats émis par l'AC sont envoyés au Service de Publication qui peut y donner accès :

- En LDAP, sans authentification client.
- Via un serveur HTTP, accessible sans authentification client, ou avec authentification client à l'aide d'un certificat de type ST-PP-CPx-AUTH ou FO-PP-CPx-AUTH[10].

Les certificats de services applicatifs publiés sont visibles en accès anonyme comme en accès authentifié.

Seule l'AC a accès à tous les certificats publiés dans le Service de Publication, au travers de l'accès HTTP en mode authentifié. Cet accès est réservé à certains personnels de l'AC qui disposent pour cela d'autorisations spéciales.

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

Le RC est systématiquement notifié par l'AC de la délivrance des certificats de services applicatifs, et cette notification dépend du canal utilisé pour la demande.

Canal MAIL :

Aucune autre entité n'est informée de la délivrance du certificat.

[10] C'est-à-dire une authentification avec une carte CPx de type « CPE/CPA » (ST-PP-CPx-AUTH) ou « CPS/CPF » (FO-PP-CPx-AUTH), mais pas de type « CPE/CPA de service » (EL-PP-CPx-AUTH).

Canal WEB SERVICES et canal IHM :

Un mail d'information indiquant que le certificat a été retiré est envoyé à l'adresse mail de la personne à informer (si présente dans la demande).

4.5 Usage de la bi-clé et du certificat

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

L'utilisation de la clé privée du service applicatif et du certificat associé est strictement limitée à la fonction de sécurité concernée (cf. chapitre 1.5.1). Les RC doivent respecter strictement les usages autorisés des bi-clés et certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé du service applicatif et du certificat associé est par ailleurs :

- Indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.
- Clairement explicité dans la présente PC.

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

Cf. chapitre précédent et chapitre 1.5.

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6 Renouvellement d'un certificat

Conformément au [RFC3647], la notion de « renouvellement de certificat » correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique du service applicatif). Le renouvellement de certificat n'est pas autorisé.

L'AC contrôle que la clé publique présentée pour certification n'a jamais été utilisée (et donc que la bi-clé est différente).

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

Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat liée à la génération d'une nouvelle bi-clé.

4.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés sont périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des services applicatifs, et les certificats correspondants, sont renouvelés au minimum tous les 3 ans et 1 mois.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, à la suite de la révocation du certificat (cf. chapitre 4.9, notamment 4.9.1 pour les différentes causes possibles de révocation).

Remarque – Dans la suite du présent chapitre, le terme utilisé est « fourniture d'un nouveau certificat ».

4.7.2 Origine d'une demande d'un nouveau certificat

La demande d'un nouveau certificat n'est jamais automatique.

Des mails de notification sont envoyés quelque temps avant l'échéance d'un certificat. La demande d'un nouveau certificat doit ensuite être effectuée selon le même processus que la demande de certificat initiale.

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

La demande d'un nouveau certificat est effectuée selon le même processus que la demande de certificat initiale. La procédure de traitement de la demande est donc identique.

4.7.4 Notification au RC de l'établissement du nouveau certificat

La demande d'un nouveau certificat est effectuée selon le même processus que la demande de certificat initiale. La notification au RC de l'établissement du nouveau certificat est donc identique.

4.7.5 Démarche d'acceptation du nouveau certificat

La demande d'un nouveau certificat est effectuée selon le même processus que la demande de certificat initiale. La démarche d'acceptation du nouveau certificat est donc identique.

4.7.6 Publication du nouveau certificat

La demande d'un nouveau certificat est effectuée selon le même processus que la demande de certificat initiale. La publication du nouveau certificat est donc identique.

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

La demande d'un nouveau certificat est effectuée selon le même processus que la demande de certificat initiale. La notification par l'AC aux autres entités de la délivrance du nouveau certificat est donc identique.

4.8 Modification du certificat

Conformément au [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique et autres qu'uniquement la modification des dates de validité.

La modification de certificat n'est pas autorisée.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

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

- Les informations du service figurant dans le certificat ne sont plus en conformité avec l'identité du service ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat.
- Le RC n'a pas respecté les modalités applicables d'utilisation du certificat.
- Le RC et/ou le cas échéant l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC.
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement.
- La clé privée du service applicatif est suspectée de compromission, est compromise, est perdue ou est volée.

- Le RC ou une entité autorisée (représentant légal de la structure) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du service applicatif).
- L'arrêt définitif du service applicatif ou la cessation d'activité de l'entité du RC de rattachement du service applicatif.

Lorsque l'une des circonstances ci-dessus se réalise et que l'AC en a connaissance, le certificat concerné est révoqué.

Par ailleurs, l'AC effectue une révocation automatique des anciens certificats de chiffrement pour lesquels l'adresse mail du service applicatif (celle présente dans le certificat) est identique. Cette révocation automatique est effectuée dans un délai calculé par l'AC à partir du moment du retrait du nouveau certificat. Ce délai permet de s'assurer que le nouveau certificat a bien été publié.

Cette révocation automatique permet aux utilisateurs de certificats envoyant des messages électroniques chiffrés de pouvoir connaitre le dernier certificat valide du service applicatif.

4.9.2 Origine d'une demande de révocation

Les personnes / entités qui peuvent demander la révocation d'un certificat électronique sont les suivantes :

- Le RC pour le service applicatif considéré.
- L'AC émettrice du certificat ou l'une de ses composantes.
- Un représentant légal de la structure.

4.9.3 Procédure de traitement d'une demande de révocation

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre 3.4.

Les informations suivantes figurent dans la demande de révocation de certificat :

- Des éléments permettant d'identifier clairement le certificat à révoquer.
  - En mode authentifié :
    - Canal IHM : le demandeur à la possibilité de faire une recherche de certificat.
    - Autre canaux : AC émettrice et numéro de série du certificat
  - En mode non authentifié par le canal IHM : AC émettrice, numéro de série du certificat et code de révocation (qui a été choisi par le demandeur de certificat au moment au retrait du certificat).
- L'identité du demandeur de la révocation.
- La cause de révocation.

Le demandeur de la révocation peut indiquer dans sa demande :

- Si la révocation doit être immédiate
- Si la révocation doit être différée (il précise alors la date). La révocation différée est interdite lorsque la raison de révocation correspond à une compromission de la clé ou à un cas de perte ou de vol de la clé.

Le **canal MAIL** ne permet pas d'effectuer une révocation différée.

En mode authentifié, la demande de révocation est acceptée après avoir vérifié dans le référentiel d'identité de l'ASIP Santé que le demandeur a bien le droit d'effectuer la demande pour le service applicatif désigné dans le certificat.

Le demandeur est un RC. L'Identifiant National du demandeur est récupéré au travers du processus d'identification et d'authentification. Cet Identifiant National est utilisé comme clé pour récupérer dans le référentiel d'identités la liste des structures pour lesquelles il est RC. Ces droits ont été communiqués à l'ASIP Santé et enregistrés dans le référentiel d'identité en fonction des données communiquées par les AED les structures concernées.

En mode non authentifié par le canal IHM, le demandeur de la révocation fournit les trois informations suivantes :

- AC émettrice.
- Numéro de série du certificat.
- Code de révocation.

Le code de révocation permet de s'assurer que le demandeur a bien le droit d'effectuer la demande de révocation.

Une fois la demande acceptée, la fonction de gestion des révocations peut révoquer le certificat correspondant en changeant son statut, puis communiquer ce nouveau statut à la fonction d'information sur l'état des certificats. Cette opération est effectuée immédiatement dans le cas d'une demande de révocation immédiate, et à la date demandée dans le cas d'une demande révocation différée.

L'opération est enregistrée dans les journaux d'événements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entrainé la révocation du certificat.

Le demandeur de la révocation peut préciser dans la demande 2 adresses mail : une pour lui-même et une pour la « personne à informer » (sauf pour une demande de révocation effectuée via le canal MAIL pour laquelle il ne peut pas préciser de « personne à informer »).

L'AC envoie un mail du type « le certificat a été révoqué » à ces deux adresses lorsque la révocation a été effectuée.

Dans le cas particulier de la révocation automatique par l'AC d'anciens certificats de chiffrement (cf. chapitre 4.9.1), les adresses mail utilisées sont l'adresse du demandeur et l'adresse de la « personne à informer » renseignées lors de la demande initiale des certificats.

Un mail d'information expliquant l'origine du problème est envoyé par l'AC à ces deux adresses si la demande est rejetée parce qu'un contrôle présente un résultat négatif (par exemple si les droits du demandeur ne lui permettent pas de demander la révocation du certificat, ou si le certificat renseigné dans la demande n'est pas trouvé).

Le rejet d'une demande de révocation effectuée par le canal WEB SERVICES ou le canal IHM est aussi notifié par un autre moyen :

Canal WEB SERVICES :

L'erreur est renvoyée dans la réponse à l'appel web service de demande de révocation.

Canal IHM :

Un message d'erreur est affiché une fois la demande de révocation soumise.

Par ailleurs, un certain nombre de contrôles ont déjà été effectués dès la saisie de la demande, avant soumission de la demande.

4.9.4 Délai accordé au RC pour formuler la demande de révocation

Dès que le RC (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

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

4.9.5.1 Révocation d'un certificat électronique

Par nature une demande de révocation immédiate est traitée en urgence. Les demandes effectuées en ligne sont traitées immédiatement.

Une demande de révocation différée est traitée à la date renseignée dans la demande de révocation.

4.9.5.2 Disponibilité du système de traitement des demandes de révocation

La fonction de gestion des révocations :

- Est disponible aux heures ouvrées.
- A une durée maximale d'indisponibilité par interruption (panne ou maintenance) de 2 heures (jours ouvrés).
- A une durée maximale d'indisponibilité par mois de 16 heures (jours ouvrés).

Toute demande de révocation d'un certificat est traitée dans un délai inférieur à 72 heures. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

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

L'utilisateur d'un certificat délivré au titre de cette PC est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification. La méthode utilisée (LCR, deltaLCR, OCSP…) est à l'appréciation de l'utilisateur selon les contraintes liées à son emploi.

4.9.7 Fréquence d'établissement et durée de validité des LCR

Les LCR et deltaLCR sont émises une fois toutes les 24 heures et ont une durée de validité de 6 jours.

4.9.8 Délai maximum de publication d'une LCR

Les LCR et deltaLCR sont publiées et disponibles pour le téléchargement au maximum 30 minutes après leur génération.

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

Un service OCSP est mis en œuvre. Il respecte les exigences d'intégrité, de disponibilité et de délai de publication décrites dans cette PC concernant la fonction d'information sur l'état des certificats.

4.9.10 Exigence de la vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Cf. chapitre 4.9.6.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

4.9.13 Causes possibles d'une suspension

La suspension de certificat n'est pas autorisée. Les chapitres suivants sont donc sans objet.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

L'AC fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'ACR), c'est-à-dire de vérifier également les signatures de certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR, deltaLCR, jetons OCSP, LAR et l'état du certificat de l'ACR.

Pour ce qui concerne les certificats émis par l'AC

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR et de deltaLCR. Ces LCR sont des LCR au format V2, publiées sur le site de l'ASIP Santé.

Les URL d'accès aux LCR et deltaLCR sont indiquées au chapitre 2.2.

La fonction d'information sur l'état des certificats met aussi à la disposition des utilisateurs de certificats un service de vérification en ligne du statut du certificat via le protocole OCSP. Ce service est disponible en HTTP à l'adresse : http://ocsp.esante.gouv.fr.

Pour ce qui concerne le reste de la chaîne de certification

La fonction d'information sur l'état des certificats émis par les AC Racines de l'IGC-Santé repose sur un mécanisme de publication de LAR disponibles en HTTP.

Se référer à la PC des AC Racines de l'IGC-Santé pour plus de précisions.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24 7j/7.

Cette fonction :

- A une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4 heures (jours ouvrés).
- A une durée maximale totale d'indisponibilité par mois de 32 heures (jours ouvrés).

Le temps de réponse du serveur OCSP à une requête reçue[11] est au maximum de 10 secondes.

4.10.3 Dispositifs optionnels

Sans objet.

4.11 Fin de la relation entre le RC et l'AC

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et l'entité de rattachement du service applicatif avant la fin de validité de l'un de ses certificats, pour une raison ou pour une autre, l'AC doit révoquer tous les certificats du service applicatif en cours de validité.

4.12 Séquestre de clé et recouvrement

Les clés privées des services applicatifs ne sont pas séquestrées. Ce chapitre ainsi que ses sous-chapitres sont donc sans objet.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

4.12.1.1 Demande de séquestre

Sans objet.

4.12.1.2 Traitement d'une demande de séquestre

Sans objet.

4.12.1.3 Origine d'une demande de recouvrement

Sans objet.

[11] Durée mesurée au niveau du serveur (requête reçue par le serveur et réponse au départ du serveur).

4.12.1.4 Identification et validation d'une demande de recouvrement

Sans objet.

4.12.1.5 Traitement d'une demande de recouvrement

Sans objet.

4.12.1.6 Destruction des clés séquestrées

Sans objet.

4.12.1.7 Disponibilité des fonctions liées au séquestre et au recouvrement

Sans objet.

4.12.2 Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physique

Les exigences de ce chapitre concernent aussi bien le site d'exploitation principal que le(les) site(s) utilisé(s) pour la reprise d'activité.

Les exigences de ce chapitre pouvant s'appliquer à d'autres composantes de l'IGC que l'OSC sont :

- Celles où cela est mentionné explicitement.
- Celles concernant les fonctions d'information sur l'état des certificats.

Les mesures permettant de répondre à ces exigences sont explicitées dans la DPC.

5.1.1 Situation géographique et construction des sites

Les sites d'exploitation de l'IGC sont installés dans des locaux situés sur le territoire national.

La construction des sites respecte les règlements et les normes en vigueur.

5.1.2 Accès physique

Afin d'éviter toute perte, dommage ou compromission des ressources de l'IGC et l'interruption des services de l'AC, les accès aux locaux des différentes composantes de l'IGC sont contrôlés.

En outre, aucune personne entrant dans ces zones physiquement sécurisées n'est laissée, pendant une période de temps significative, sans la surveillance d'une personne autorisée.

5.1.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.

Elles permettent également de respecter les engagements pris par l'AC dans cette PC en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.4 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les engagements pris par l'AC dans cette PC en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les engagements pris par l'AC dans cette PC en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.6 Conservation des supports

Les différentes informations intervenant dans les activités de l'IGC sont identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).

Le Responsable de l'IGC maintient un inventaire de ces informations.

L'AC met en place des mesures pour éviter la compromission et le vol de ces informations.

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils sont manipulés de manière sécurisée afin de les protéger contre les dommages, le vol et les accès non autorisés.

Des procédures de gestion protègent ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

5.1.7 Mise hors service des supports

En fin de vie, les supports sont soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

Les procédures et moyens de destruction et de réinitialisation sont conformes à ce niveau de confidentialité.

5.1.8 Sauvegardes hors site

Les composantes de l'IGC mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes sont organisées de manière à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conforme aux engagements de l'AC dans la présente PC en matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des certificats (cf. chapitres 4.9.5.1 et 4.10.2).

Les informations sauvegardées hors site respectent les exigences de la présente PC en matière de protection en confidentialité et en intégrité de ces informations.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Chaque composante de l'IGC distingue les cinq rôles fonctionnels de confiance suivants :

- Responsable de sécurité - Le responsable de sécurité est chargé de la mise en œuvre et du contrôle de la politique de sécurité d'une ou plusieurs composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et des journaux

d'évènements. Il est responsable des opérations de génération et de révocation des certificats.

- Responsable d'application - Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
- Ingénieur système - Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
- Opérateur - Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation au quotidien des applications pour les fonctions mises en œuvre par la composante.
- Contrôleur - Personne autorisée à accéder et en charge de l'analyse régulière des archives et de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

En plus de ces rôles de confiance au sein de chaque composante de l'IGC, la mise en œuvre de l'AC nécessite également le rôle de confiance de porteur de parts de secrets d'IGC.

Ces porteurs de parts de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiés.

Des procédures sont établies et appliquées pour tous les rôles administratifs et les rôles de confiance ayant trait à la fourniture de service de certification.

Ces rôles sont décrits et définis dans la description des postes propre à chaque entité opérant une des composantes de l'IGC sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles déterminent la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilisation des employés.

Lorsqu'appropriées, ces descriptions font la différence entre les fonctions générales et les fonctions spécifiques à l'AC. L'AC implémente techniquement le principe de moindre privilège via les mécanismes de contrôle d'accès qu'elle met en œuvre.

De plus, les opérations de sécurité de l'AC sont séparées des opérations normales. Les responsabilités des opérations de sécurité incluent :

- Les procédures et responsabilités opérationnelles.
- La planification et la validation des systèmes sécurisés.
- La protection contre les logiciels malicieux.
- L'entretien.
- La gestion de réseaux.
- La surveillance active des journaux d'audit, l'analyse des évènements et les suites.
- La manipulation et la sécurité des supports.
- L'échange de données et de logiciels.

Ces responsabilités sont gérées par les opérations de sécurité de l'AC, mais peuvent être effectivement réalisées par du personnel opérationnel non spécialiste (en étant supervisé), tel que défini dans la politique de sécurité appropriée et les documents relatifs aux rôles et responsabilités.

Des mesures sont mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux services de l'AC soient sortis du site sans autorisation.

5.2.2 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, les fonctions sensibles sont réparties sur plusieurs personnes. La présente PC définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC (cf. chapitre 6).

La DPC précise quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.).

5.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC vérifie l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

- Que son nom est ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle.
- Que son nom est ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes.
- Le cas échéant et en fonction du rôle, qu'un compte est ouvert à son nom dans ces systèmes.
- Eventuellement, que des clés cryptographiques et/ou un certificat lui sont délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.

Ces contrôles sont décrits dans la DPC et sont conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'IGC est notifiée par écrit. Ce rôle est clairement mentionné et décrit dans sa fiche de poste.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul sont respectées.

Les attributions associées à chaque rôle sont décrites dans la DPC et sont conformes à la politique de sécurité de la composante de l'IGC concernée.

Concernant les rôles de confiance, le cumul suivant est interdit :

- Responsable de sécurité et ingénieur système.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont soumis à une clause de confidentialité vis-à-vis de leur employeur.

Chaque entité opérant une composante de l'IGC s'assure que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier des procédures de sécurité en vigueur au sein de l'IGC.

L'AC informe toute personne intervenant dans des rôles de confiance de l'IGC :

- De ses responsabilités relatives aux services de l'IGC.
- Des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.

En particulier, les personnes intervenant dans des rôles de confiance y sont formellement affectées par l'encadrement supérieur chargé de la sécurité.

5.3.2 Procédures de vérification des antécédents

Chaque entité opérant une composante de l'IGC met en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions.

A ce titre, l'employeur peut demander à ces personnels la communication d'une copie du bulletin n°3 de leur casier judiciaire.

L'employeur peut décider en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les trois ans).

5.3.3 Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondants à la composante de l'IGC au sein de laquelle il opère.

Les personnels ont connaissance et comprennent les implications des opérations dont ils ont la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

La présente PC ne formule pas d'exigence spécifique sur le sujet.

5.3.6 Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont précisées dans la DPC.

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC respecte également les exigences du présent chapitre 5.3. Ceci est traduit en clauses adéquates dans les contrats avec ces prestataires.

5.3.8 Documentation fournie au personnel

Chaque personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante de l'IGC au sein de laquelle il travaille. En particulier, il lui est remis la ou les politique(s) de sécurité l'impactant.

5.4 Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer de façon manuelle ou automatique. Les fichiers résultants, sous forme papier ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Type d'évènements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre de l'IGC, chaque entité opérant une composante de l'IGC journalise au minimum les évènements tels que décrits ci-dessous, sous forme électronique. La journalisation est automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.).
- Démarrage et arrêt des systèmes informatiques et des applications.
- Evènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises à la suite d'une défaillance de la fonction de journalisation.
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements sont aussi recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- Les accès physiques.
- Les actions de maintenance et de changements de la configuration des systèmes.
- Les changements apportés au personnel.
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, ...).

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC sont également journalisés, notamment :

- Réception d'une demande de certificat (initiale et renouvellement).
- Validation / Rejet d'une demande de certificat.
- Evènements liés aux clés de signature et aux certificats d'AC : génération (cérémonie de clés), sauvegarde / récupération, révocation, renouvellement, destruction, ...
- Génération des certificats des services applicatifs.
- Transmission des certificats aux RC.
- Publication et mise à jour des informations liées à l'AC (PC, certificats d'ACR, conditions générales d'utilisation, etc.).
- Réception d'une demande de révocation.

- Validation / rejet d'une demande de révocation.
- Génération puis publication des LCR (et deltaLCR).

Chaque enregistrement d'un évènement dans un journal contient au minimum les champs suivants :

- Type de l'évènement.
- Nom de l'exécutant ou référence du système déclenchant l'évènement.
- Date et heure de l'évènement (l'heure exacte des évènements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat est enregistrée).
- Résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement contient également les champs suivants :

- Destinataire de l'opération.
- Nom du demandeur de l'opération ou référence du système effectuant la demande.
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes).
- Cause de l'évènement.
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Les opérations de journalisation sont effectuées au cours du processus.

En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'évènement.

Les évènements et données spécifiques à journaliser sont documentés par l'AC dans la DPC.

5.4.2 Fréquence de traitement des journaux d'évènements

Cf. chapitre 5.4.8.

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant au moins 1 mois.

Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous 1 mois (recouvrement possible entre la période de conservation sur site et la période d'archivage).

5.4.4 Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des

mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Le système de datation des évènements respecte les exigences du chapitre 6.8.

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.5 Procédure de sauvegarde des journaux d'évènements

Chaque entité opérant une composante de l'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC.

5.4.6 Système de collecte des journaux d'évènements

Des précisions sur le système de collecte des journaux d'événements sont apportées dans la DPC.

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

La présente PC ne formule pas d'exigence spécifique sur le sujet.

5.4.8 Evaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements sont contrôlés une fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité au moins une fois toutes les deux semaines et dès la détection d'une anomalie.

Cette analyse donne lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les des différents journaux d'évènements de fonctions qui interagissent entre elles est effectué au moins une fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à relever toute anomalie.

5.5 Archivage des données

5.5.1 Types de données à archiver

Des dispositions en matière d'archivage sont également prises par l'AC. Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

Il permet également la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données archivées sont au moins les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques.

- La PC.
- La DPC.
- Les conditions générales d'utilisation.
- Les accords contractuels avec d'autres AC.
- Les certificats d'AC, les LCR et deltaLCR tels qu'émis ou publiés.
- Les récépissés ou notifications (à titre informatif).
- Les journaux d'évènements des différentes entités de l'IGC.
- Les justificatifs d'identité des RC et, le cas échéant de leur structure de rattachement.
- Les justificatifs de possession des services applicatifs ainsi que leurs noms.

5.5.2 Période de conservation des archives

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé aussi longtemps que nécessaire, et pendant au moins sept ans, pour les besoins de fourniture de la preuve de certification dans des procédures légales, conformément à la loi applicable sur le territoire français.

La durée de conservation des dossiers d'enregistrement est portée à la connaissance du RC.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat peut être présenté par l'AC lors de toute sollicitation par les autorités habilitées.

Ce dossier, complété par les mentions consignées par l'AE permet de retrouver l'identité réelle du RC responsable, à un instant « t » du service applicatif désigné dans le certificat émis par l'AC.

Certificats, LCR et deltaLCR émis par l'AC

Les certificats de clés de services applicatifs et d'AC, ainsi que les LCR et deltaLCR produites, sont archivés pendant au moins cinq années après leur expiration.

Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 sont archivés pendant sept ans après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage offrent le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements est assurée tout au long de leur cycle de vie.

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes :

- Sont protégées en intégrité.
- Sont accessibles uniquement aux personnes autorisées.
- Peuvent être relues et exploitées.

L'AC précise dans sa DPC les moyens mis en œuvre pour archiver les pièces en toute sécurité.

5.5.4 Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes d'archives est au moins équivalent au niveau de protection des archives.

5.5.5 Exigences d'horodatage des données

Cf. chapitre 5.4.4 pour la datation des journaux d'évènements.

Le chapitre 6.8 précise les exigences en matière de datation / horodatage.

5.5.6 Système de collecte des archives

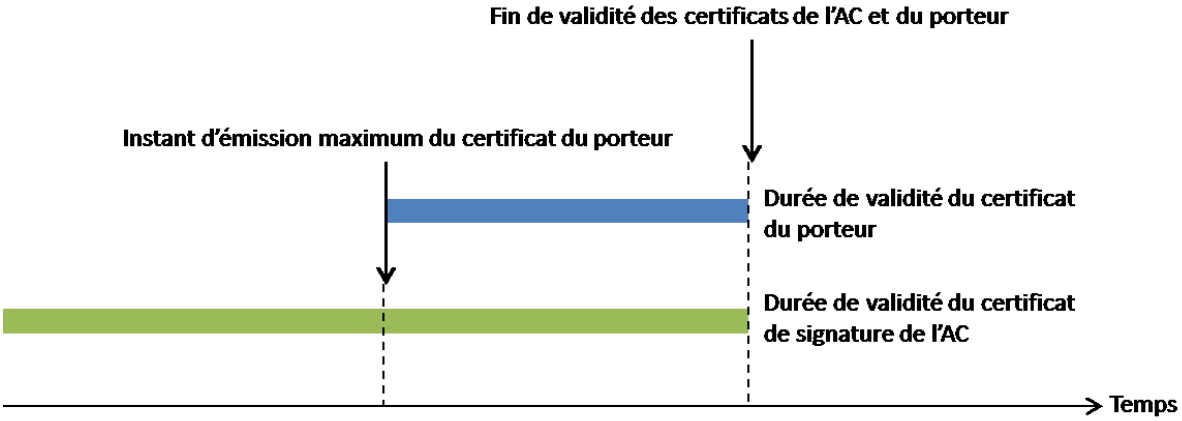
Le système de collecte des archives respecte les exigences de protection des archives concernées.

5.5.7 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) peuvent être récupérées dans un délai inférieur à deux jours ouvrés, sachant que seul le Responsable de l'IGC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

5.6 Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin est postérieure à la date d'expiration de son propre certificat. Pour cela la période de validité du certificat d'une ACR est supérieure à celles des certificats d'ACI qu'elle signe.



Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats.

Le certificat précédent de l'AC reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7 Reprise suite à compromission et sinistre

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

Chaque entité opérant une composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements. Ces procédures et moyens permettent de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident par l'entité opérant la composante concernée. Cette dernière en informe immédiatement le Responsable de l'IGC. Le cas de l'incident majeur est impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, est faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses serveurs devient insuffisant pour son utilisation prévue restante, alors le Responsable de l'IGC :

- Informe tous les RC et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information est mise à disposition des autres utilisateurs de certificats.
- Fait révoquer tout certificat concerné.

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

Chaque composante de l'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant des engagements de l'AC dans la présente PC, notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

Ce plan est testé au minimum une fois tous les trois ans.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante de l'IGC est traité dans le plan de continuité de la composante en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué : cf. chapitre 4.9 de la PC des AC Racines de l'IGC-Santé. De même, tous les certificats émis par cette AC doivent être révoqués.

En outre, le Responsable de l'IGC respecte au minimum les engagements suivants :

- Informer les entités suivantes de la compromission : tous les RC et les autres entités avec lesquelles l'AC a passé des accords ou a d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autres AC. En complément, cette information est mise à disposition des autres tiers utilisateurs.
- Indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC.

5.8 Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'Agence prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'Agence serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'Agence en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'Agence, entre autres obligations :

1. Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des services applicatifs et des informations relatives aux certificats, archivage de séquestre le cas échéant).
2. Assure la continuité de la fonction de révocation (prise en compte d'une demande de révocation et publication de l'état des certificats), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC.
3. Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des RC ou des utilisateurs de certificats, l'Agence les avise aussitôt que nécessaire et, au moins un mois avant les changements.

Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats seulement). La cessation partielle d'activité est progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) ci-dessous sont à exécuter par l'Agence, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'Agence ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention conclue avec cette entité, assurera la révocation des certificats et la publication des LCR conformément aux engagements pris dans la PC.

L'AC décrit dans ses pratiques les dispositions prises en cas de cessation d'activité. Elles prévoient :

- La notification des entités affectées.
- Le transfert de ses obligations à d'autres parties.

- La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'Agence :

1. S'interdit de transmettre les clés privées des AC lui ayant permis d'émettre des certificats.
2. Prend toutes les mesures nécessaires pour les détruire ou les rendre inopérante.
3. Révoque les certificats d'AC (ACR ou ACI).
4. Révoque tous les certificats signés par les ACI et qui seraient encore en cours de validité.
5. Informe tous les RC des certificats révoqués ou à révoquer, ainsi que leur structure de rattachement le cas échéant (cf. chapitre 3.2.3).

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

La bi-clé est générée au niveau du service applicatif. Cette génération doit être effectuée dans un dispositif répondant aux exigences du chapitre 12.

6.1.2 Transmission de la clé privée au service applicatif

Sans objet (l'AC ne génère pas la bi-clé du service applicatif).

6.1.3 Transmission de la clé publique à l'AC

La bi-clé est générée par le demandeur de certificat. La demande de certificat est effectuée auprès de l'AC au format PKCS#10.

Cette demande de certificat contient la clé publique à certifier. Le mécanisme permettant de prouver la possession de la clé privée (cf. chapitre 3.2.1), et la sécurisation des canaux de demande (cf. chapitre 4.2.1), permettent de protéger l'intégrité de la clé publique et d'authentifier son origine.

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

La clé publique de l'AC est diffusée dans un certificat qui est émis par une AC Racine, ce qui permet d'en assurer l'intégrité et d'en authentifier l'origine.

La clé publique de l'AC, ainsi que les informations correspondantes (certificats, empreintes numériques, déclarations d'appartenance) peuvent être récupérées aisément par les utilisateurs de certificats sur un serveur Web, tel que mentionné au chapitre 2.2.

6.1.5 Tailles des clés

Les certificats de services applicatifs émis par l'AC utilisent l'algorithme RSA avec la fonction de hachage SHA-256. La taille de la bi-clé est de 2048 bits.

6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité

L'équipement de génération des bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé. Les paramètres et les algorithmes utilisés sont indiqués dans cette PC et dans [GAB_ET1_ET2].

6.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée et du certificat associé est strictement limitée à la fonction de sécurité concernée (cf. chapitres 1.5.1 et 4.5).

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 dispositifs de protection des éléments secrets des services applicatifs, pour la mise en œuvre de leurs clés privées, doivent respecter les exigences du chapitre 12.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Sans objet.

6.2.3 Séquestre de la clé privée

Les clés privées ne sont pas séquestrées.

6.2.4 Copie de secours de la clé privée

Les clés privées des services applicatifs peuvent faire l'objet de copie de secours.

Ces copies peuvent être effectuées, soit dans un module cryptographique conforme aux exigences du chapitre 11, soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuyer sur un algorithme, une longueur de clé, et un mode opératoire capable de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les règles à respecter sont définies dans le document [RGS_B_1].

6.2.5 Archivage de la clé privée

Les clés privées ne sont pas archivées (ni par l'AC, ni par aucune des composantes de l'IGC).

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

Sans objet.

6.2.7 Stockage de la clé privée dans un module cryptographique

Sans objet.

6.2.8 Méthode d'activation de la clé privée

Sans objet.

6.2.9 Méthode de désactivation de la clé privée

Sans objet.

6.2.10 Méthode de destruction des clés privées

Sans objet.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs de protection des éléments secrets

Sans objet (le dispositif de protection des éléments secrets n'est pas délivré par l'AC).

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 correspondants.

6.3.2 Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats ont une durée de vie maximale de 3 ans et 1 mois.

Plus précisément, une extension de certificat indique que la période d'usage de la clé privée est au maximum de 3 ans, et la période de validité du certificat s'étend sur un mois supplémentaire. De cette manière, les signatures effectuées à la fin de la période d'usage de la clé privée pourront encore être considérées comme valide lors de l'opération de vérification de la signature pendant un mois.

Dans tous les cas, la fin de validité du certificat d'AC est postérieure à la fin de vie des certificats qu'elle émet.

6.4 Données d'activation

L'AC ne génère pas la clé privée. Ce chapitre ainsi que ses sous-chapitres sont donc sans objet.

6.4.1 Génération et installation des données d'activation

Sans objet.

6.4.2 Protection des données d'activation

Sans objet.

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Le niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est défini dans la DPC. Il répond au moins aux objectifs de sécurité suivants :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique).
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par le Responsable de l'IGC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles).

- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur).
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels.
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès.
- Protection du réseau contre toute intrusion d'une personne non autorisée.
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent.
- Fonctions d'audits (non-répudiation et nature des actions effectuées).
- Eventuellement, gestion des reprises sur erreur.

Les applications utilisant les services des composantes de l'IGC peuvent requérir des besoins de sécurité complémentaires.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle fait l'objet de mesures particulières.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) sont mis en place.

6.5.2 Niveau de qualification des systèmes informatiques

L'IGC utilise des modules cryptographiques répondants aux exigences sur la qualification décrites au chapitre 11.2.

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau est documentée et contrôlée. Les composantes de l'IGC utilisent des systèmes et des produits fiables qui sont protégés contre toute modification.

Le Responsable de l'IGC garantit que les objectifs de sécurité sont définis lors des phases de spécification et de conception.

6.6.2 Mesures liées à la gestion de la sécurité

Le Responsable de l'IGC est consulté pour la validation de toute évolution significative d'un système d'une composante de l'IGC. Cette évolution est documentée et apparaît dans les procédures de fonctionnement interne de la composante concernée et est conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

6.7 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires à leur fonctionnement au sein de l'IGC.

L'AC garantit que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'AC.

De plus, certains échanges entre composantes au sein de l'IGC nécessitent la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle…).

6.8 Horodatage / Système de datation

Les différentes composantes de l'IGC utilisent « l'heure système de l'IGC » en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près.

Pour la synchronisation par rapport au temps UTC, l'OSC se réfère à un système comprenant deux sources indépendantes de temps.

7 Profils des certificats, OCSP et des LCR

7.1 Certificats

La référence à consulter concernant la structure des certificats est le document [GAB_ET1_ET2].

7.2 LCR

La référence à consulter concernant la structure des LCR est le document [GAB_ET1_ET2].

7.3 deltaLCR

La référence à consulter concernant la structure des deltaLCR est le document [GAB_ET1_ET2].

Une delta-LCR est publiée à chaque fois qu'une LCR est publiée, de manière simultanée.

En comparaison avec la LCR, la delta-LCR contient :

- Le même contenu pour les extensions thisUpdate, nextUpdate et crlNumber.
- Une extension deltaCrlIndicator avec le crlNumber de la LCR précédente.
- La liste des certificats révoqués depuis la publication de la LCR précédente.

7.4 OCSP

L'IGC met à disposition un service OCSP permettant la vérification en ligne des certificats émis au titre de cette PC. Il est disponible via le protocole HTTP à l'URL http://ocsp.esante.gouv.fr. Cette URL figure dans l'extension « authorityInfoAccess » des certificats.

Ce service est conforme au [RFC2560].

8 Audit de conformité et autres évaluations

Afin de s'assurer que l'ensemble de l'IGC est bien conforme aux engagements affichés dans cette PC et aux pratiques énoncées dans la DPC, le Responsable de l'IGC fait réaliser des audits et autres évaluations.

8.1 Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de l'IGC ou à la suite de toute modification significative au sein d'une composante, le Responsable de l'IGC procède à un contrôle de conformité de cette composante.

Le Responsable de l'IGC procède également, une fois tous les trois ans, à un contrôle de conformité de l'ensemble de l'IGC.

8.2 Identités / qualifications des évaluateurs

Le contrôle d'une composante de l'IGC est assigné par le Responsable de l'IGC à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définis dans la 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

À l'issue d'un contrôle de conformité, le Responsable de l'IGC reçoit de l'équipe d'audit un avis parmi les suivants : « réussite », « échec », « à confirmer ».

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations pour le Responsable de l'IGC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par le Responsable de l'IGC et respecte les politiques de sécurité internes de l'AC.
- En cas de résultat « à confirmer », le Responsable de l'IGC remet à l'entité opérant la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permet de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, le Responsable de l'IGC confirme à l'entité opérant la composante contrôlée la conformité aux exigences de la PC et la DPC.

8.6 Communication des résultats

Les résultats des contrôles de conformité sont communiqués aux personnes suivantes :

- Le Responsable de l'IGC.
- Les responsables de la composante de l'IGC contrôlée.

9 Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

La délivrance de certificats pour les services applicatifs ne fait pas l'objet d'une facturation.

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

Sans objet.

9.1.5 Politique de remboursement

Sans objet.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

L'Agence a contracté une assurance couvrant son activité de prestataire de services de certification.

9.2.2 Autres ressources

Sans objet.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- Tous les secrets de l'IGC (dont les clés privées de l'AC et des composantes de l'IGC et les données d'activation associées aux clés privées de l'AC).
- La DPC et les procédures associées.
- Les journaux d'évènements des composantes de l'IGC.

- Les dossiers d'enregistrement des services applicatifs et des RC.
- Les causes de révocations, sauf accord explicite du RC.

Remarque : les clés privées de services applicatifs (et éventuelles données d'activation associées) ne figurent pas dans cette liste car elles ne sont jamais en possession d'une composante de l'IGC.

9.3.2 Informations hors du périmètre des informations confidentielles

Les informations concernant l'IGC publiées par le SP sont considérées comme non confidentielles.

9.3.3 Responsabilités en termes de protection des informations confidentielles

L'AC et l'ensemble des composantes de l'IGC appliquent des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, l'AC en garantit l'intégrité.

L'AC respecte notamment la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des services applicatifs à des tiers dans le cadre de procédures légales. Elle donne également l'accès à ces informations au RC.

9.4 Protection des données à caractère personnel

9.4.1 Politique de protection des données à caractère personnel

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble des composantes de l'IGC sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL].

9.4.2 Données à caractère personnel

Les données considérées comme personnelles sont au moins les suivantes :

- Les causes de révocation des certificats de services applicatifs (qui sont considérées comme confidentielles sauf accord explicite du RC).
- Le dossier d'enregistrement du RC.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données à caractère personnel

Les responsabilités de l'AC et de l'ensemble des composantes de l'IGC en termes de protection des données personnelles sont celles découlant du respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL].

9.4.5 Notification et consentement d'utilisation des données à caractère personnel

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les RC à l'AC ne sont ni divulguées ni transférées à

un tiers sauf dans les cas suivants : consentement préalable du RC, décision judiciaire ou autre autorisation légale.

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

La divulgation d'informations personnelles aux autorités judiciaires ou administrative est effectuée conformément à la législation et à la réglementation en vigueur sur le territoire français.

9.4.7 Autres circonstances de divulgation de données à caractère personnel

Sans objet.

9.5 Droits de propriété intellectuelle

La législation et la réglementation en vigueur sur le territoire français sont appliquées.

Des clauses particulières concernant la propriété des logiciels et matériels utilisés pour l'exécution des services de l'IGC sont mentionnées dans la DPC.

9.6 Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC sont les suivantes :

- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées.
- N'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par cette PC et les documents qui en découlent.
- Respecter et appliquer la partie de la DPC leur incombant (cette partie est communiquée à la composante correspondante).
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par le Responsable de l'IGC (cf. chapitre 8).
- Documenter leurs procédures internes de fonctionnement.
- Respecter les accords ou contrats qui les lient entre elles ou aux RC.
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1 Autorités de Certification

L'AC a pour obligation de :

- Garantir et maintenir la cohérence de la DPC avec la PC.
- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un service applicatif donné et que le RC correspondant a accepté le certificat, conformément aux exigences du chapitre 4.4.
- Prendre toutes les mesures raisonnables pour s'assurer que ses RC sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC.

Le Responsable de l'IGC prend les dispositions nécessaires pour que l'Agence couvre ses responsabilités liées à ses opérations et/ou activités, et pour qu'elle possède la stabilité

financière et les ressources exigées pour fonctionner en conformité avec la présente politique.

De plus, le Responsable de l'IGC engage la responsabilité de l'Agence en cas de faute ou de négligence de l'AC ou de l'une des composantes de l'IGC, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des RC à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

Par ailleurs, le Responsable de l'IGC a à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par l'AC ou l'une des composantes de l'IGC. Il est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle l'AC s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni est approuvée par le Responsable de l'IGC.

9.6.2 Service d'enregistrement

Cf. les obligations pertinentes du chapitre 0.

9.6.3 RC

Le RC a le devoir de :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat.
- Protéger la clé privée du service applicatif dont il a la responsabilité par des moyens appropriés à son environnement.
- Protéger les données d'activation de cette clé et, le cas échéant, les mettre en œuvre.
- Protéger l'accès à la base de certificats du service applicatif.
- Respecter les conditions d'utilisation de la clé privée du service applicatif et du certificat correspondant.
- Informer l'AC de toute modification concernant les informations contenues dans le certificat électronique.
- Faire, sans délai, une demande de révocation du certificat électronique dont il est responsable auprès de l'AE ou de l'AC en cas de compromission ou suspicion de compromission de la clé privée correspondante (ou de ses données d'activation).

9.6.4 Utilisateurs de certificats

Les utilisateurs de certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis.
- Pour chaque certificat de la chaîne de certification, du certificat final jusqu'à l'AC Racine, vérifier la signature numérique du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation).
- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

9.7 Limite de garantie

L'AC garantit au travers de ses services d'IGC :

- L'identification et l'authentification de l'ACR avec son certificat.
- L'identification et l'authentification des ACI avec les certificats d'AC générés par l'ACR.

- La gestion des certificats correspondants et des informations de validité des certificats selon la présente PC.

Aucune autre garantie ne peut être mise en avant entre l'AC et les utilisateurs de certificats dans leurs accords contractuels (s'il en est).

9.8 Limite de responsabilité

Pour les domaines de la santé et du médico-social, l'Agence décline toute responsabilité à l'égard de l'usage qui est fait des certificats que l'AC a émis dans des conditions et à des fins autres que celles prévues dans la présente PC ainsi que dans tout autre document contractuel applicable associé.

En dehors des domaines de la santé et du médico-social, l'Agence décline toute responsabilité.

9.9 Indemnités

Sans objet.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

La PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Fin anticipée de validité

Le Responsable de l'IGC peut être amené à faire évoluer la PC.

La mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

9.10.3 Effets de la fin de validité et clauses restant applicables

Les seules clauses restant applicables au-delà de la fin de validité de la PC, sont celles concernant l'archivage des données sauf lorsque la PC est remplacée par une PC prévoyant de nouvelles règles d'archivage. La nouvelle PC peut prévoir que les nouvelles règles s'appliquent à toutes les données archivées, y compris pendant la période de validité de l'ancienne PC.

9.11 Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, le Responsable de l'IGC doit au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et des différentes composantes de l'IGC.

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

Le Responsable de l'IGC révise cette PC à chaque fois qu'une évolution des systèmes de l'IGC ou qu'une évolution remarquable de l'état de l'art le justifie.

9.12.2 Mécanisme et période d'information sur les amendements

Le Responsable de l'IGC donne un préavis de deux mois au moins aux composantes de l'IGC de son intention de modifier cette PC avant de procéder aux changements.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des RC, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) se traduit par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

9.13 Dispositions concernant la résolution de conflits

L'Agence met en place des politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles elle fournit des services électroniques de confiance ou d'autres points qui y sont liés.

L'Agence 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

La législation et la réglementation en vigueur sur le territoire français sont appliquées.

9.15 Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre 10.1.

9.16 Dispositions diverses

9.16.1 Accord global

Sans objet.

9.16.2 Transfert d'activités

Cf. chapitre 5.8.

9.16.3 Conséquences d'une clause non valide

Les conséquences d'une clause non valide, le cas échéant, seront traitées en fonction de la législation en vigueur.

Au cas où une clause de la présente 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

Sans objet.

9.16.5 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.

9.16.6 Autres dispositions

Sans objet.

10 Annexe 1 : Documents cités en référence

10.1 Réglementation

Renvoi	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
[RGS]	Référentiel Général de Sécurité – Version 2.0
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 1.20

10.2 Documents fonctionnels

Renvoi	Document
[AE-PROCESS]	Processus d'enregistrement appliqués par les Autorités d'Enregistrement de l'IGC-Santé

10.3 Documents techniques

Renvoi	Document
[GAB_ET1_ET2]	« IGC-Santé – Etapes 1 et 2 – Les gabarits des certificats X.509 et des CRLs – Gamme Elémentaire – Domaines Personnes et Organisations » Document produit par l'Agence et disponible à l'adresse http://integrateurs-cps.asipsante.fr/pages/IGC-Sant%C3%A9-Gabarits.
[RFC3647]	« Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework » Novembre 2003
[RFC5280]	« Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile » Mai 2008
[ISO/IEC 9594-8; ITU-T X.509]	« Information Technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks » ; « Public-key and attribute certificate frameworks »
[ISO/IEC 9798-1]	« Information Technology – Security Techniques – Entity authentication – Part 1: General »
[ISO/IEC 10118-1]	« Information Technology – Security Techniques – Hash-functions – Part 1: General »

Renvoi	Document
[2nd DIS ISO/IEC 11770-3]	« Information Technology – Security Techniques –Key management – Part 3: Mechanisms using asymmetric techniques » - 2e edition
[ISO/IEC 13335-1]	« Information Technology – Security Techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management »

11 Annexe 2 : Exigences de sécurité du module cryptographique de l'AC

11.1 Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR et deltaLCR) répond aux exigences de sécurité suivantes :

- Assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie.
- Etre capable d'identifier et d'authentifier ses utilisateurs.
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné.
- Etre capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur.
- Permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance des clés privées.
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité.
- Pour la fonction de sauvegarde et de restauration des clés privées de l'AC, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.
- Détecter les tentatives d'altération physiques et entrer dans un état sûr quand une tentative d'altération est détectée.

11.2 Exigences sur la qualification

Le module cryptographique utilisé par l'AC est qualifié au niveau renforcé, selon le processus décrit dans le [RGS], et est conforme aux exigences du chapitre 11.1.

12 Annexe 3 : Exigences de sécurité du dispositif de protection des éléments secrets

Le dispositif de protection des éléments secrets, utilisé par le service applicatif pour stocker et mettre en œuvre sa clé privée, et le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- Si la bi-clé du service applicatif est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée.
- Assurer la correspondance entre la clé privée et la clé publique.
- Générer une fonction de sécurité qui ne peut être falsifiée sans la connaissance de la clé privée.

Par ailleurs, des mesures de sécurité organisationnelles, procédurales ou techniques sont mises en place afin de :

- Détecter les défauts lors des phases d'initialisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée.
- Garantir la confidentialité et l'intégrité de la clé privée.
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.
- Assurer pour le serveur légitime uniquement la fonction de génération des cachets électroniques et protéger la clé privée contre toute utilisation par des tiers.

Remarque : Les dispositifs matériels, de types cartes à puces ou modules cryptographiques qualifiés par l'ANSSI, respectent ces exigences. Toutefois, des solutions logicielles sont susceptibles de respecter ces exigences pourvu que des mesures de sécurité additionnelles propres à l'environnement dans lequel est déployé la clé privée soient mises en place. Cet environnement dans lequel est déployée la clé privée doit faire l'objet d'un audit de sécurité.