Politique de Certification de l'IGC-Santé
ACR Gammes ELEMENTAIRE, STANDARD et FORT
1.2.250.1.213.1.7.1.1.3.1.1 (EL-ACR)
1.2.250.1.213.1.7.1.2.3.1.1 (ST-ACR)
1.2.250.1.213.1.7.1.3.3.1.1 (FO-ACR)

Identification du document	
Référence	PC-AC_Racines-V1.2
Date de création	13/10/2015
Date de dernière mise à jour	02/01/2023
Etat	Validé
Version	1.2
Classification	Non sensible public
Nombre de pages	59

Historique du document

Version	Date	Auteur	Commentaires
V 1.0	19/02/2016	ASIP Santé	Première version publiée
V 1.1	09/09/2021	ANS	Mise à jour durée de validité des certificats
V 1.2	02/01/2023	ANS	Mise à jour adresse

Agence du Numérique en Santé
2 - 10 Rue d'Oradour-sur-Glane
75015 Paris
Standard : 01 58 45 32 50
esante.gouv.fr

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.

Le 20 décembre 2019, l'ASIP Santé devient l'ANS (Agence du Numérique en Santé). Dans la suite du document, les références à l'agence s'effectueront sous le nom d'ANS. Mais pour assurer la continuité du service, ce changement de nom n'est pas répercuté sur la structuration de l'IGC-Santé qui mentionne toujours le nom Agence des Systèmes d'information Partagé de Santé.

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

L'ANS 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'ANS 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.

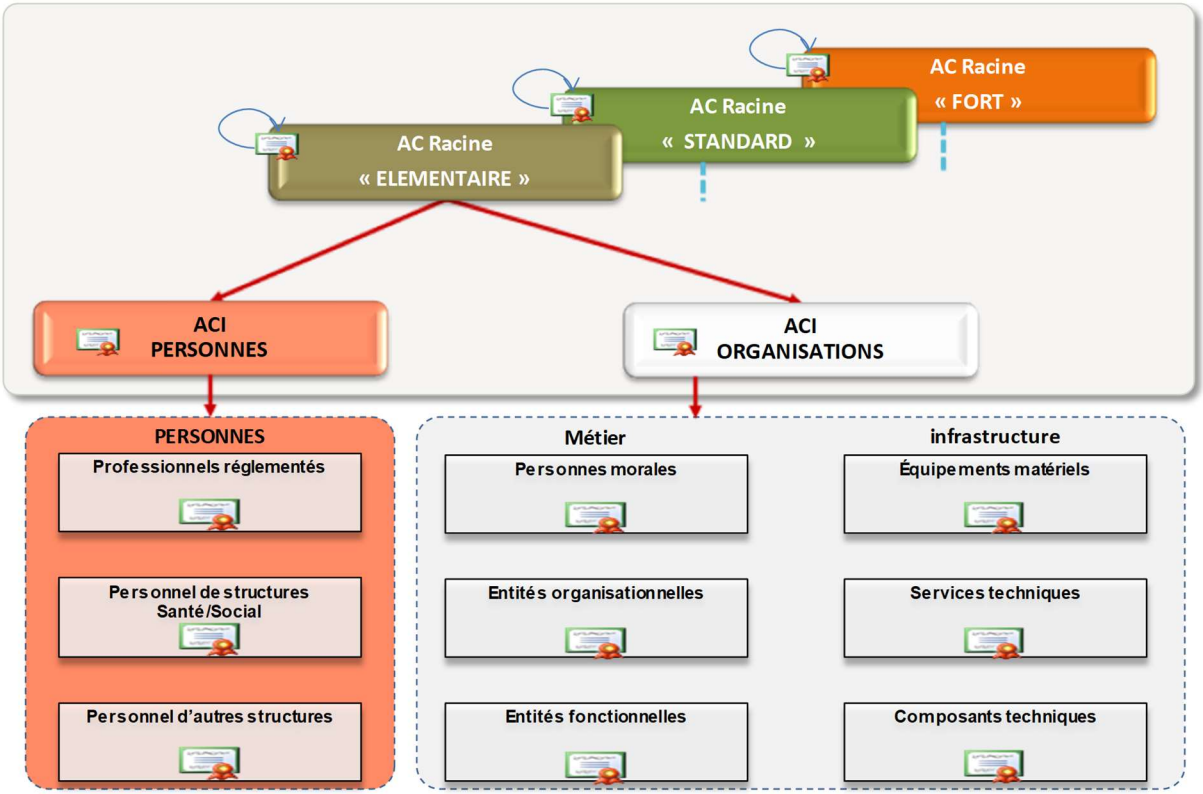
Les certificats finaux des porteurs ou services applicatifs sont gérés par des Autorités de Certification Intermédiaires (ACI)[1] « en ligne » structurées en fonction des domaines adressés (Personnes et Organisations). Ces ACI sont signées par des Autorités de Certification Racines (ACR) « hors ligne » 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)[2].

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

[2] L'ACI du domaine « ORGANISATIONS » de la branche « FORT » n'est pas mise en œuvre au sein de l'IGC-Santé, ce qui explique certaines particularités dans cette PC (par exemple le fait que le certificat de cette ACI ne soit pas publié).



Hiérarchie d'AC de l'IGC-Santé

La structure de cette PC est conforme à la [RFC3647].

1.2 Identification du document

Ce document constitue la Politique de Certification (PC) des ACR « gamme ELEMENTAIRE », gamme « STANDARD » et « gamme FORT » de l'IGC-Santé. Il est la propriété de l'ANS.

Cette PC couvre les exigences de sécurité relatives à la gestion du cycle de vie des certificats et bi-clés associés des ACR et ACI de l'IGC-Santé. Dans la mesure où les trois ACR de l'IGC-Santé respectent les mêmes exigences et ont de grandes similarités, elles sont traitées dans un document unique.

Les numéros d'OID[3] correspondants à cette PC sont :

- 1.2.250.1.213.1.7.1.1.3.1.1 (en tant que PC de l'ACR gamme ELEMENTAIRE, désignée dans ce document sous la référence EL-ACR lorsque la précision est nécessaire).
- 1.2.250.1.213.1.7.1.2.3.1.1 (en tant que PC de l'ACR gamme STANDARD, désignée dans ce document sous la référence ST-ACR lorsque la précision est nécessaire).
- 1.2.250.1.213.1.7.1.3.3.1.1 (en tant que PC de l'ACR gamme FORT, désignée dans ce document sous la référence FO-ACR lorsque la précision est nécessaire).

[3] 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, 3 = AC Racines), « 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-Santé. 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'ANS.

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-Santé (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'ANS, 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[4] :

- Autorité d'enregistrement (AE)[5] - 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 éléments secrets du porteur - Cette fonction génère les éléments secrets à destination du porteur, si l'AC a en charge une telle génération, et les prépare en vue de leur remise au porteur (par exemple, personnalisation de la carte à puce destinée au porteur, courrier sécurisé avec le code d'activation, etc.). De tels éléments secrets peuvent être, par exemple, directement la bi-clé du porteur, les codes (activation / déblocage) liés au dispositif de stockage de la clé privée du porteur ou encore des codes ou clés temporaires permettant au porteur de mener à distance le processus de génération / récupération de son certificat.
- 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 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).

[4] 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.

[5] 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.

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

- 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 de 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 aux 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.

Dans le cas particulier de cette PC, il convient de préciser que :

- L'AC émettrice est une ACR. Dans ce document, le terme « AC » employé sans précision désigne toujours l'ACR émettrice.
- Les certificats délivrés sont des certificats d'AC (ACR ou ACI). Dans ce document, pour éviter la confusion avec l'AC émettrice, le terme « AC » lorsqu'il concerne le certificat émis est toujours complété de la précision « (ACR ou ACI) ».
- Le porteur de ces certificats est toujours l'ANS en tant que personne morale.
- Dans certains cas, cette PC évoque les certificats émis par les ACI et les porteurs de ces certificats. Pour apporter la précision au sein de ce document, les termes « certificats finaux » et « porteurs finaux » sont employés (le qualificatif « final » est employé car les certificats émis par les ACI sont au niveau le plus bas de la chaîne de certification).
- L'AC prend en charge la fonction de génération des éléments secrets du porteur.
- Concernant la fonction d'information sur l'état des certificats, seule la publication de LAR est réalisée.

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'ANS.

La Direction Générale de l'ANS 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'ANS – 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 remise au porteur ou au RC.
- Fonction de gestion des révocations.
- Fonction d'information sur l'état des certificats, uniquement pour le mode requête / réponse temps réel (OCSP)[6].

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.

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

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.

1.4.2 Autorité d'enregistrement

L'AE a pour rôle de vérifier l'identité du futur porteur de certificat.

Dans le cadre de cette PC :

- Le porteur de certificat est toujours l'ANS(cf. chapitre 1.4.1).
- L'AE est toujours le Responsable de l'IGC.

La vérification de l'identité du porteur est donc implicite.

L'AE assure les tâches d'établissement et de transmission de la demande de certificat à la fonction adéquate de l'IGC.

1.4.3 Porteurs de certificats

Le porteur d'un certificat d'AC (ACR ou ACI) est toujours l'ANS.

L'ANS respecte les conditions qui lui incombent en tant que porteur, telles que définies dans la présente PC.

1.4.4 Utilisateurs de certificats

L'utilisateur d'un certificat d'AC (ACR ou ACI) est toute entité ou personne physique qui s'y fie pour vérifier la validité de la chaîne de certification d'un certificat final émis par une ACI de l'IGC-Santé.

1.4.5 Autres participants

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'ANS ne saurait être engagée dans ce cadre particulier (voir chapitre 9.8).

Chaque ACR dispose d'une seule bi-clé et d'un certificat associé pour signer des certificats d'ACI et des Listes d'Autorités Révoquées (LAR). Le certificat d'une ACR est autosigné.

Chaque ACI dispose d'une seule bi-clé et d'un certificat associé pour signer des certificats de porteurs finaux, des Listes de Révocation de Certificat (LCR) et des deltaLCR.

Les certificats d'AC (ACR ou ACI) ne peuvent être utilisés par un utilisateur de certificat qu'à des fins de validation d'une chaîne de confiance, de vérification de LAR (pour ce qui concerne les certificats d'ACR) ou de vérification de LCR ou deltaLCR (pour ce qui concerne les certificats d'ACI).

1.5.2 Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.5, en fonction du niveau de sécurité. L'AC respecte ces restrictions et impose leur respect par l'ANS (en tant que porteur) et ses utilisateurs de certificats. À cette fin elle communique à

tous les porteurs 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 :

Agence du numérique en santé

Responsable de l'IGC-Santé

2 - 10 Rue d'Oradour-sur-Glane

75015 Paris

e-mail : Responsable-IGC-Sante@esante.gouv.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 porteurs 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 porteurs 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.
LAR	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 LAR figurent dans les certificats émis. La publication de cette information sur une page web permet aux utilisateurs de certificats de s'assurer de l'état des certificats d'ACR (cf. chapitre 4.10).
Certificats d'ACR 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.
Hash SHA-1 des certificats d'ACR	Publication	Serveur WEB : ➢ A l'adresse http://igc-sante.esante.gouv.fr/PC, par affichage directement sur la page, près du lien de téléchargement du certificat d'ACR correspondant.	La publication de cette information permet aux utilisateurs de certificats de s'assurer de l'origine des certificats d'ACR. C'est une mesure de sécurité décrite au chapitre 6.1.4.
Certificats d'ACI 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.

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 aux LAR sont :

- En HTTP :
  - http://igc-sante.esante.gouv.fr/CRL/ACR-EL.crl
  - http://igc-sante.esante.gouv.fr/CRL/ACR-ST.crl
  - http://igc-sante.esante.gouv.fr/CRL/ACR-FO.crl
- En LDAP :
  - ldap://annuaire-igc.esante.gouv.fr/cn=AC RACINE IGC-SANTE ELEMENTAIRE,ou=IGC-SANTE,ou=0002 187512751,o=ASIP-SANTE,c=FR?certificaterevocationlist;binary?base?objectClass=pkiCA
  - ldap://annuaire-igc.esante.gouv.fr/cn=AC RACINE IGC-SANTE STANDARD,ou=IGC-SANTE,ou=0002 187512751,o=ASIP-SANTE,c=FR?certificaterevocationlist;binary?base?objectClass=pkiCA
  - ldap://annuaire-igc.esante.gouv.fr/cn=AC RACINE IGC-SANTE FORT,ou=IGC-SANTE,ou=0002 187512751,o=ASIP-SANTE,c=FR?certificaterevocationlist;binary?base?objectClass=pkiCA

Les URL permettant un accès direct aux certificats des AC (ACR et ACI) sont :

- http://igc-sante.esante.gouv.fr/AC/ACR-EL.cer
  - http://igc-sante.esante.gouv.fr/AC/ACI-EL-PP.cer
  - http://igc-sante.esante.gouv.fr/AC/ACI-EL-ORG.cer
- http://igc-sante.esante.gouv.fr/AC/ACR-ST.cer
  - http://igc-sante.esante.gouv.fr/AC/ACI-ST-PP.cer
  - http://igc-sante.esante.gouv.fr/AC/ACI-ST-ORG.cer
- http://igc-sante.esante.gouv.fr/AC/ACR-FO.cer
  - http://igc-sante.esante.gouv.fr/AC/ACI-FO-PP.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 que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC. Le site publiant ces informations (à l'exception des informations d'état des certificats) est accessible les jours ouvrés.

Les certificats d'AC et les informations permettant aux utilisateurs de certificats de s'assurer de l'origine des certificats d'AC sont diffusés préalablement à toute diffusion de certificats de porteurs (certificats d'ACI) et/ou de LAR correspondantes. Le site publiant ces informations est accessible 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 non disponibilité de cette information ; et les exigences de disponibilité des systèmes publiant les informations mentionnées ci-dessus s'appliquent également à la disponibilité des informations publiées sur ces systèmes.

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 fort (basé sur une authentification au moins à deux facteurs).

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 d'ACR (conforme à la norme X.509), l'AC émettrice (champ « issuer ») et le porteur (champ « subject ») sont identifiés par un « Distinguished Name » (DN) de type X.501.

La construction du DN de ces champs est précisée dans le document [GAB_ET1].

3.1.2 Nécessité d'utilisation de noms explicites

Les noms utilisés dans les champs « issuer » et « subject » des certificats d'AC (ACR ou d'ACI) sont explicites.

3.1.3 Pseudonymisation des porteurs

Sans objet : l'identité utilisée dans les certificats d'AC (ACR ou ACI) n'est pas un pseudonyme, il est clairement mentionné « ASIP-SANTE ».

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

Au sein du domaine de certification de chaque AC, les DN du champ « subject » (correspondants au certificat d'ACR lui-même ou au certificat d'une ACI rattachée à cette ACR) sont uniques.

Cette unicité est assurée au travers du processus de cérémonie de clés.

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

3.2.1 Méthode pour prouver la possession de la clé privée

La génération des bi-clés et certificats d'AC (ACR ou ACI) est effectuée dans des circonstances parfaitement contrôlées dans le cadre d'une cérémonie de clés, par des

personnels dans des rôles de confiance, garantissant la possession des clés privées correspondantes.

3.2.2 Validation de l'identité d'un organisme

Dans le cas de l'émission d'un certificat d'AC (ACR ou ACI) :

- Le porteur est toujours l'Agence.
- Le Responsable de l'IGC, qui comme indiqué au chapitre 1.3.1 est la Direction Générale de l'Agence, est à la fois le seul à pouvoir faire le demande de certificat, et celui remplissant le rôle d'AE.

Il n'y a donc pas à proprement parler de validation de l'identité de l'organisme présent dans le certificat, qui est toujours l'Agence.

3.2.3 Validation de l'identité d'un individu

Sans objet : dans le cas de l'émission d'un certificat d'AC (ACR ou ACI), l'identité présente dans le certificat n'est jamais celle d'un individu.

3.2.4 Informations non vérifiées du porteur

Aucune information non vérifiée n'est introduite dans les certificats.

3.2.5 Validation de l'autorité du demandeur

Seul le Responsable de l'IGC a l'autorité pour effectuer une demande de certificat pour une AC (ACR ou ACI).

Lors de la cérémonie de clés au cours de laquelle le certificat d'AC (ACR ou ACI) est généré, il est vérifié que les demandes proviennent du Responsable de l'IGC.

3.2.6 Certification croisée d'AC

Sans objet.

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

Le renouvellement de la bi-clé d'une AC (ACR ou ACI) entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne peut pas être délivré à une AC (ACR ou ACI) sans renouvellement de la bi-clé correspondante (cf. chapitre 4.6).

3.3.1 Identification et validation pour un renouvellement courant

Les vérifications relatives au renouvellement d'une bi-clé sont effectuées conformément aux procédures initiales (cf. chapitre 3.2).

3.3.2 Identification et validation pour un renouvellement après révocation

Les vérifications relatives au renouvellement d'une bi-clé sont effectuées conformément aux procédures initiales (cf. chapitre 3.2).

3.4 Identification et validation d'une demande de révocation

L'OSC – qui a en charge la fonction de gestion des révocations – s'assure que les demandes lui parvenant ont bien été formulées par le Responsable de l'IGC ou une autorité judiciaire. Comme indiqué au chapitre 4.9.2, ce sont les seuls habilités à faire une demande de révocation de certificat d'AC (ACR ou ACI).

Lorsque la demande émane du Responsable de l'IGC, elle est formulée par écrit et signée. La signature manuscrite est comparée à une signature préalablement enregistrée.

Lorsque la demande émane d'une autorité judiciaire, il doit s'agir d'une décision de justice.

4 Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Seul le Responsable de l'IGC peut effectuer une demande de certificat pour une AC (ACR ou ACI).

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

Les demandes de certificat d'AC (ACR ou ACI) sont formulées par le Responsable de l'IGC.

Une demande de génération de certificat d'AC (ACR ou ACI) contient au minimum :

- Le nom à utiliser dans le champ « subject » du certificat.
- Le nom à utiliser dans le champ « issuer » du certificat (c'est-à-dire l'identifiant de l'ACR qui doit signer le certificat).

4.2 Traitement d'une demande de certificat

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

Comme indiqué au chapitre 3.2.2, il n'y a pas à proprement parler de validation de l'identité de l'organisme présent dans le certificat, qui est toujours l'Agence.

Toute demande de certificat d'AC (ACR ou ACI) émanant du Responsable de l'IGC est réputée valide. En effet, il est à la fois le seul à pouvoir faire la demande, et le seul à pouvoir la traiter (en tant qu'AE).

4.2.2 Acceptation ou rejet de la demande

Toute demande de certificat d'AC (ACR ou ACI) émanant du Responsable de l'IGC est réputée acceptée. En effet, il est à la fois le seul à pouvoir faire la demande, et le seul à pouvoir la traiter (en tant qu'AE).

Le Responsable de l'IGC transmet la demande à l'OSC afin de procéder à une cérémonie de clés.

4.2.3 Durée d'établissement du certificat

Le certificat est établit au cours d'une cérémonie de clés dans un délai convenu entre le Responsable de l'IGC et l'OSC.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

La demande formulée par le Responsable de l'IGC est vérifiée par l'OSC :

- Son origine et son authenticité sont vérifiées.
- Sa complétude est vérifiée.

Une fois ces vérifications effectuées, l'OSC organise une cérémonie de clés au cours de laquelle le certificat d'AC (ACR ou ACI) est généré.

Une cérémonie de clés se déroule dans des conditions particulières de sécurité. Il est ainsi garantit que le processus de génération du certificat est lié de manière sécurisée au processus de génération de la bi-clé : l'ordonnancement des opérations est assuré ainsi que l'intégrité et l'authentification des échanges entre les composantes de l'IGC. Par ailleurs, la clé privée est transmise de façon sécurisée à des personnes désignées par le Responsable de l'IGC, en en garantissant l'intégrité et la confidentialité.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres 5 et 6, notamment la séparation des rôles de confiance (cf. chapitre 5.2).

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

La notification est effectuée à la fin de la cérémonie de clés par la remise en mains propres du certificat d'AC généré, à la personne représentant le Responsable de l'IGC.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Dès que l'adéquation entre le certificat d'AC (ACR ou ACI) produit et la demande de certificat est confirmée par la personne représentant le Responsable de l'IGC, le certificat est accepté.

4.4.2 Publication du certificat

Une fois le certificat d'AC (ACR ou ACI) accepté, il est mis à disposition sur le SP.

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

S'agissant de certificats d'AC (ACR ou ACI) :

- L'OSC délivre le certificat généré à l'AC.
- L'AC engage des actions de communication pour notifier d'autres entités de la délivrance du certificat. Il s'agit notamment des AE des IGC assurant les prestations d'ACI (ces AE sont détaillées dans les PC des ACI mises à disposition sur le SP).
- Les utilisateurs sont informés par la publication du certificat (cf. chapitre 4.4.2).

4.5 Usages de la bi-clé et du certificat

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

L'utilisation de la clé privée d'une AC (ACR ou ACI) et du certificat associé est strictement limitée aux domaines indiqués au chapitre 1.4.1. En cas de mauvaise utilisation des clés

privées et des certificats associés par les AC (ACR ou ACI), la responsabilité de l'Agence peut être engagée.

L'usage autorisé des bi-clés d'AC (ACR ou ACI) et des certificats associés est indiqué dans les certificats via les extensions concernant les usages de clés (cf. chapitre 7.1).

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 peut être engagée.

4.6 Renouvellement d'un certificat

Conformément à la [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 porteur).

Le renouvellement de certificat n'est pas autorisé par la présente PC.

4.6.1 Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification au porteur de l'établissement du nouveau certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6 Publication du nouveau certificat

Sans objet.

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

Sans objet.

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

Conformément à la [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat d'AC (ACR ou ACI) liée à la génération d'une nouvelle bi-clé.

4.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés des AC (ACR ou ACI) sont périodiquement renouvelées :

- Selon les recommandations émises par l'ANSSI en matière de cryptanalyse, afin de minimiser les possibilités d'attaques cryptographiques.
- Pour que chaque ACR puisse continuer à délivrer des certificats d'ACI d'une durée constante.

Par ailleurs une bi-clé et un certificat d'AC (ACR ou ACI) peuvent être renouvelés à la suite d'une révocation du certificat (cf. chapitre 4.9).

Le changement de bi-clé entraîne le changement de certificat, la procédure à suivre est identique à la procédure initiale de certification.

Remarque - Dans la suite de ce chapitre, le terme « fourniture d'un nouveau certificat » est utilisé. L'AC étant en charge de la fonction de génération des éléments secrets du porteur, cela couvre aussi la fourniture de la bi-clé.

4.7.2 Origine d'une demande d'un nouveau certificat

La fourniture d'un nouveau certificat n'est pas automatique.

Les exigences opérationnelles concernant la demande d'un nouveau certificat pour une AC (ACR ou ACI) sont les mêmes que celles concernant la demande du certificat initial, précisées au chapitre 4.1.

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

Les exigences opérationnelles concernant le traitement d'une demande d'un nouveau certificat pour une AC (ACR ou ACI) sont les mêmes que celles concernant le traitement de la demande du certificat initial, précisées au chapitre 4.2.

4.7.4 Notification au porteur de l'établissement du nouveau certificat

Les exigences opérationnelles concernant la délivrance d'un nouveau certificat pour une AC (ACR ou ACI) sont les mêmes que celles concernant la délivrance du certificat initial, précisées au chapitre 4.3.

4.7.5 Démarche d'acceptation du nouveau certificat

Les exigences opérationnelles concernant la démarche d'acceptation d'un nouveau certificat pour une AC (ACR ou ACI) sont les mêmes que celles concernant la démarche d'acceptation du certificat initial, précisées au chapitre 4.4.1.

4.7.6 Publication du nouveau certificat

Les exigences opérationnelles concernant la publication d'un nouveau certificat pour une AC (ACR ou ACI) sont les mêmes que celles concernant la publication du certificat initial, précisées au chapitre 4.4.2.

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

Les exigences opérationnelles concernant la notification par l'AC aux autres entités de la délivrance d'un nouveau certificat pour une AC (ACR ou ACI) sont les mêmes que celles concernant la notification par l'AC aux autres entités de la délivrance du certificat initial, précisées au chapitre 4.4.3.

4.8 Modification du certificat

Conformément à la [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre 4.7) et autres qu'uniquement la modification des dates de validité (cf. chapitre 4.6).

La modification de certificat n'est pas autorisée par la présente PC.

4.8.1 Causes possible de modification d'un certificat

Sans objet.

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

Sans objet.

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

Sans objet.

4.8.4 Notification au porteur de l'établissement du certificat modifié

Sans objet.

4.8.5 Démarche d'acceptation du certificat modifié

Sans objet.

4.8.6 Publication du certificat modifié

Sans objet.

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

Sans objet.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

Les causes possibles de révocation d'un certificat d'AC (ACR ou ACI) sont les suivantes :

- Cessation d'activité de l'AC.
- Compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de l'AC (perte du secret principal, perte du code d'activation, perte d'un nombre de parts de secrets ne permettant plus le chargement sécurisé dans un nouveau module cryptographique de la clé privée d'AC sauvegardée lors de la cérémonie de clés).
- Décision de changement à la suite de la détection d'une non-conformité des procédures appliquées au sein d'une composante de l'IGC avec celles annoncées dans la DPC (par exemple à la suite d'un audit de conformité négatif).
- Changement d'informations dans le certificat.
- Obsolescence de la cryptographie au regard des exigences de l'ANSSI.

Par ailleurs la révocation d'un certificat d'ACR est une cause possible de la révocation des certificats ACI qui en dépendent.

4.9.2 Origine d'une demande de révocation

La révocation d'un certificat d'AC (ACR ou ACI) ne peut être décidée que par le Responsable de l'IGC, ou par les autorités judiciaires via une décision de justice.

4.9.3 Procédure de traitement d'une demande de révocation

Le Responsable de l'IGC transmet la demande à l'OSC.

La DPC précise les procédures mises en œuvre en cas de révocation d'un certificat d'AC (ACR ou ACI).

En cas de révocation d'un certificat d'AC (ACR ou ACI), l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs finaux concernés que leurs certificats ne sont plus valides car l'un des certificats de la chaîne de certification n'est plus valide.

4.9.4 Délai accordé pour formuler la demande de révocation

Dès que le Responsable de l'IGC a connaissance qu'une cause possible de révocation d'un certificat d'AC (ACR ou ACI) est effective, il doit formuler une demande de révocation sans délai, et la transmettre à l'OSC.

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

Les demandes de révocation d'un certificat d'AC (ACR ou ACI) sont traitées immédiatement par l'OSC. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la LAR de l'ACR qui a émis le certificat, et que cette liste est accessible au téléchargement.

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

L'utilisateur d'un certificat d'AC (ACR ou ACI) est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.

S'agissant de certificats d'AC (ACR ou ACI), la seule méthode utilisable est la vérification de LAR.

4.9.7 Fréquence d'établissement des LCR

Remarque : les LCR sont en fait des LAR car elles concernent des certificats d'AC (ACR ou ACI).

Bien que la probabilité de révoquer un certificat d'AC (ACR ou ACI) soit très faible compte tenu des fortes exigences de sécurité requises pour toute demande de certificat, l'AC s'efforce de couvrir les objectifs de sécurité suivants pour l'établissement de ses LAR :

- La fréquence doit être assez rapprochée pour limiter le temps de latence pendant lequel les applications qui ont chargé la LAR précédente n'iront pas consulter la nouvelle LAR ; en effet, selon la [RFC5280], les applications n'ont aucune obligation de vérifier la présence d'une nouvelle LAR avant la date de publication de la prochaine LAR indiquée dans la LAR en cours.
- La publication est mensuelle.
- Le SP a jusqu'au premier jour ouvré du mois pour publier une LAR valide au premier jour du mois.

Ces objectifs sont couverts par les exigences suivantes :

- La fréquence de mise à jour des listes de certificats révoqués est mensuelle. En cas de révocation en urgence, une nouvelle LAR est publiée indépendamment de cette périodicité.
- La LAR publiée précise la date de publication de la LAR suivante. La nouvelle LAR est publiée au plus tard à cette date par l'AC. Une LAR est valide 45 jours.

4.9.8 Délai maximum de publication d'une LCR

Remarque : les LCR sont en fait des LAR car elles concernent des certificats d'AC (ACR ou ACI).

Les LAR mensuelles sont signées par anticipation et par lots de douze LAR au maximum.

Le délai maximum de publication d'une LAR mensuelle par une AC est le délai de recouvrement entre la date de début de validité de la LAR et la date de fin de validité de la LAR précédente. Avec des LAR valides 45 jours à partir du 1e jour du mois, le délai maximum de publication va donc de 14 jours (si le mois précédent a 31 jours) à 17 jours (si le mois précédent a 28 jours).

En cas de révocation urgente, la publication de la LAR est faite dans les 24 heures.

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

Seul un mécanisme de LAR pour les certificats d'AC (ACR ou ACI) est mis en œuvre.

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

Sans objet.

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

Outre les exigences du chapitre 4.9.3, la révocation à la suite d'une compromission de clé privée d'AC (ACR ou ACI) fait l'objet d'une information clairement diffusée au moins sur le site Internet de l'Agence et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

4.9.13 Causes possibles d'une suspension

La suspension de certificat n'est pas autorisée par la présente PC.

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 d'AC (ACR ou ACI).

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LAR.

Ces LAR sont des LCR au format V2, publiées dans un annuaire accessible en protocole LDAP V3 et en HTTP. L'adresse de ces points de distribution est indiquée au chapitre 2.2.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24 heures / 24 et 7 jours / 7. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4 heures et une durée maximale totale d'indisponibilité par mois de 16 heures.

4.10.3 Dispositifs optionnels

Sans objet.

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

Sans objet : le porteur des certificats d'AC (ACR ou ACI) est toujours l'Agence, il n'existe donc pas de relation contractuelle entre le porteur et l'AC.

4.12 Séquestre de clé et recouvrement

Les clés privées d'AC (ACR ou ACI) ne sont pas séquestrées.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

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 ou 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-Santé sont installés dans des locaux situés sur le territoire national.

La construction des sites respecte les règlements et 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.

Pour les fonctions de génération des certificats, de génération des éléments secrets du porteur et de gestion des révocations :

- L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.
- Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

Remarque - On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisés pour la mise en œuvre de ces fonctions.

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 exigences de la présente PC en matière de disponibilité des fonctions de l'IGC, 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 exigences de la présente PC en matière de disponibilité des fonctions de l'IGC, 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 exigences de la présente PC en matière de disponibilité des fonctions de l'IGC, 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.) correspondants à ces informations sont gérés selon des procédures conformes aux besoins de sécurité définis. 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 exigences de 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 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.

Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, au moins, mettent en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions à la suite de la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.).

Les fonctions de sauvegarde et de restauration sont effectuées par les rôles de confiance appropriés et conformément aux mesures de sécurité procédurales.

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 de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc. 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 des applications pour les fonctions mises en œuvre par la composante.
- Contrôleur - Personne désignée par une autorité ayant compétence pour le faire, et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.

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, les cumuls suivants sont interdits :

- Responsable de sécurité et ingénieur système / opérateur.
- Contrôleur et tout autre rôle.
- Ingénieur système et opérateur.

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 dispose 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. Ils doivent remettre à leur employeur une copie du

bulletin n°3 de leur casier judiciaire. 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 fréquence et la séquence de rotation entre les différentes attributions sont précisées dans la DPC.

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 doit être 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 éléments secrets du porteur (bi-clés, codes d'activation…).
- Génération des certificats des porteurs.
- Transmission des certificats aux porteurs et, selon les cas, acceptations / rejets explicites par les porteurs.
- 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 LAR.

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.

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 sensibilité des journaux d'évènements est évaluée par l'AC. 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 au moins 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 par semaine 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 différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) est effectué au moins une fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler 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 certificats d'AC (ACR ou ACI) et LAR tels qu'émis ou publiés.
- Les récépissés ou notifications (à titre informatif).
- Les registres et scripts de cérémonie de clés.
- L'attribution des rôles de confiance.
- Les journaux d'évènements des différentes entités de l'IGC.

5.5.2 Période de conservation des archives

Dossiers de demande de certificat

Tout dossier de demande de certificat d'AC (ACR ou ACI) accepté est archivé aussi longtemps qu'une demande de certificat final qui a ce certificat d'AC dans sa chaîne de certification doit être archivé (voir chapitres équivalents à celui-ci dans les PC des ACI), aux fins notamment de preuve de la certification. Ainsi, le dossier de demande de certificat peut être présenté par l'AC lors de toute sollicitation par les autorités habilitées pendant toute cette durée.

Certificats et LAR émis par l'AC

Les certificats d'AC (ACR ou ACI), ainsi que les LAR produites, sont archivés pendant au moins 5 années après leur expiration.

Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 sont archivés pendant au moins 5 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

Pour rappel le chapitre 5.4.4 indique que les journaux d'évènements sont horodatés.

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 2 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 serait 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 au moins 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 devient insuffisant pour son utilisation prévue restante, alors le Responsable de l'IGC :

- Informe tous 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 le 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 de 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 deux 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 (cf. chapitre 5.7.2) en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, se reporter au chapitre 4.9.

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 (cf. chapitre 5.7.2).

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 en matière de faillite.

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 ACR ou des ACI et des informations relatives aux certificats).
2. Assure la continuité de la fonction de révocation (prise en compte d'une demande de révocation et publication des LAR), 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 utilisateurs de certificats, l'Agence les avise aussitôt que nécessaire et, au moins 1 mois avant les changements.

Cessation d'activité affectant une ACR

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité d'une seule ACI parmi celles dépendant de l'ACR concernée). 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 LAR conformément aux engagements pris dans sa 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 la clé privée d'ACR lui ayant permis d'émettre des certificats d'AC (ACR ou ACI).
2. Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante.
3. Révoque le certificat d'ACR.
4. Révoque tous les certificats d'ACI que l'ACR a signés et qui seraient encore en cours de validité.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

La génération des clés de signature d'AC (ACR ou ACI) est effectuée dans un environnement sécurisé (cf. chapitre 5).

Les clés de signature d'AC (ACR ou ACI) sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre 11.

La génération des clés de signature d'AC (ACR ou ACI) est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre 5.2.1), dans le cadre de « cérémonies de clés ». Ces cérémonies de clés se déroulent suivant des scripts préalablement définis.

L'initialisation de l'IGC et/ou la génération des clés de signature d'AC (ACR ou ACI) s'accompagne de la génération de parts de secrets d'IGC. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC (ACR ou ACI), notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC (ACR ou ACI) sauvegardées lors de la cérémonie de clés.

A la suite de leur génération, les parts de secrets sont remises à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme, un même porteur ne peut détenir plus d'une part de secrets de l'AC à un moment donné. Chaque part de secrets est mise en œuvre par son porteur.

Les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins un est externe à l'AC et est impartial. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie de clés par rapport au script préalablement défini.

6.1.2 Transmission de la clé privée à son propriétaire

La clé privée de l'AC (ACR ou ACI) est générée au cours d'une cérémonie de clés. A l'issue de cette cérémonie de clés, une copie de secours de la clé privée (respectant les exigences définies au chapitre 6.2.4) est remise à un ou plusieurs porteurs de parts de secrets, préalablement désignés par le Responsable de l'IGC.

6.1.3 Transmission de la clé publique à l'AC

La clé publique de l'AC (ACR ou ACI) est générée puis transmise à l'ACR au cours d'une cérémonie de clés. Dans ces conditions de transmission, l'intégrité de la clé publique est garantie, et son origine est authentifiée.

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 un certificat racine autosigné.

Un certificat racine autosigné ne permet pas de garantir par lui-même que la clé publique correspondante appartient bien à l'AC considérée. Sa diffusion s'accompagne de la diffusion, via des sources de confiance, de l'empreinte numérique du certificat ainsi que d'une déclaration qu'il s'agit bien de la clé publique de l'AC.

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 recommandations des organismes nationaux et internationaux compétents (relatives aux longueurs de clés, algorithmes de signature, algorithme de hachage…) sont périodiquement consultées afin de déterminer si les paramètres utilisés dans l'émission de certificats d'AC (ACR ou ACI) doivent ou ne doivent pas être modifiés.

Les certificats d'AC (ACR ou ACI) utilisent l'algorithme RSA avec la fonction de hachage SHA-256.

La taille de la bi-clé de chaque ACR est de 4096 bits.

La taille de la bi-clé de chaque ACI est de 4096 bits.

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

Les équipements utilisés pour la génération des bi-clés d'AC (ACR ou ACI) sont des ressources cryptographiques conformes aux exigences du chapitre 6.2.11 et respectent donc les normes de sécurité propres à l'algorithme correspondant à la bi-clé (cf. chapitre 6.1.5).

6.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée d'une ACR et du certificat associé est strictement limitée à la signature de certificats d'ACI et de LAR.

L'utilisation de la clé privée d'une ACI et du certificat associé est strictement limitée à la signature de certificats finaux, de LCR et de deltaLCR.

Ces usages correspondent aux domaines d'utilisation décrits au chapitre 1.5.1 et aux usages décrits au chapitre 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 modules cryptographiques utilisés par une AC (ACR ou ACI) pour la génération et la mise en œuvre de ses clés de signature, sont conformes aux exigences du chapitre 11.

Ces modules cryptographiques utilisent des générateurs d'aléas qui sont conformes à l'état de l'art, aux standards en vigueur ou suivent les spécifications de la normalisation lorsqu'ils sont normalisés. Les algorithmes utilisés sont conformes aux standards en vigueurs ou suivent les spécifications de la normalisation lorsqu'ils sont normalisés.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée d'une AC (ACR ou ACI) pour l'exportation / l'importation hors / dans un module cryptographique.

La génération de la bi-clé est traitée au chapitre 6.1.1.

L'activation de la clé privée est traitée au chapitre 6.2.8.

La destruction de la clé privée est traitée au chapitre 6.2.10.

Le contrôle des clés privées des AC (ACR ou ACI) est assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets (système « n parmi m » où les n intervenants doivent s'authentifier).

6.2.3 Séquestre de la clé privée

Sans objet (cf. chapitre 4.12).

6.2.4 Copie de secours de la clé privée

Les clés privées d'AC (ACR ou ACI) font l'objet de copies de secours, 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 correspondant offre un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuie sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée.

Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC (ACR ou ACI) ne sont à aucun moment en clair en dehors du module cryptographique.

Le contrôle des opérations de chiffrement / déchiffrement est conforme aux exigences du chapitre 6.2.2.

6.2.5 Archivage de la clé privée

Les clés privées d'AC (ACR ou ACI) ne sont pas archivées.

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

Tous les transferts de clés privées d'AC (ACR ou ACI) se font sous forme chiffrée, conformément aux exigences du chapitre 6.2.4.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées liées aux certificats d'AC (ACR ou ACI) sont stockées dans un module cryptographique conforme aux exigences du chapitre 11.

Dans le cas des copies de secours, le stockage est effectué en dehors d'un module cryptographique moyennant le respect des exigences du chapitre 6.2.4.

Quel que soit le moyen utilisé, l'AC garantit que les clés privées d'AC (ACR ou ACI) ne sont pas compromises pendant leur stockage ou leur transport.

6.2.8 Méthode d'activation de la clé privée

La méthode d'activation des clés privées d'AC (ACR ou ACI) dans un module cryptographique permet de répondre aux exigences définies dans le chapitre 11.

L'activation des clés privées d'AC (ACR ou ACI) dans un module cryptographique est contrôlée via des données d'activation (cf. chapitre 6.4) et fait intervenir au moins deux personnes dans des rôles de confiance.

6.2.9 Méthode de désactivation de la clé privée

La désactivation des clés privées d'AC (ACR ou ACI) dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

Ces conditions de désactivation permettent de répondre aux exigences définies dans le chapitre 11.

6.2.10 Méthode de destruction des clés privées

La méthode de destruction des clés privées d'AC (ACR ou ACI) permet de répondre aux exigences définies dans le chapitre 11.

Les clés privées d'AC (ACR ou ACI) sont détruites quand elles ne sont plus utilisées ou quand les certificats auxquels elles correspondent sont expirés ou révoqués. La destruction d'une clé privée implique la destruction des copies de sauvegarde, et l'effacement de cette clé sur la ressource cryptographique qui la contient, de manière à ce qu'aucune information ne puisse être utilisée pour la recouvrer.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs de création de signature

Les exigences de qualification des modules cryptographiques utilisés par les AC (ACR ou ACI) sont précisées au chapitre 11.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques des AC (ACR et ACI) sont archivées dans le cadre de l'archivage des certificats (cf. chapitre 5.5).

6.3.2 Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des ACR ont une durée de vie de 20 ans.

Les bi-clés et les certificats des ACI ont une durée de 20 ans - 1 jour.

La fin de validité d'un certificat d'une ACR est toujours postérieure à la fin de vie des certificats d'ACI qu'elle émet.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC se fait lors de la phase d'initialisation et de personnalisation de ce module. Les données d'activation des clés privées d'AC (ACR ou ACI) sont générées durant les cérémonies des clés selon un schéma de partage des secrets décrit au chapitre 6.2.2.

Si les données d'activation ne sont pas choisies et saisies par les responsables de ces données eux-mêmes, elles leur sont transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. chapitre 5.2.1).

6.4.2 Protection des données d'activation

Les données d'activation des modules cryptographiques de l'IGC sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.4.3 Autres aspects liés aux données d'activation

Les données d'activation ne sont en aucun cas transmises à une entité tierce, en particulier dans le cas où les modules cryptographiques sont changés ou retournés au constructeur pour maintenance. Les autres aspects de la gestion des données d'activation sont précisés dans la DPC.

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).
- 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 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.

6.6.1 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.

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

Sans objet.

6.7 Mesures de sécurité réseau

Les composantes de l'IGC chargées des fonctions suivantes ne sont jamais connectées à un réseau :

- Autorité d'Enregistrement.
- Fonction de génération des certificats.
- Fonction de génération des éléments secrets du porteur.
- Fonction de remise au porteur.
- Fonction de gestion des révocations.

Pour ce qui concerne les autres composantes de l'IGC, 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.

6.8 Horodatage / Système de datation

Il n'y a pas d'horodatage utilisé par l'AC mais une datation des évènements qui permet, à partir d'une date fournie par le système d'exploitation de l'AC de séquencer les évènements.

Des procédures automatiques ou manuelles sont utilisées pour maintenir l'heure du système. Les réglages de l'horloge sont des évènements susceptibles d'être audités.

7 Profils des certificats, OCSP et des LCR

7.1 Certificats

La référence à consulter concernant la structure des certificats d'AC (ACR et ACI) est le document [GAB_ET1].

7.2 LCR

La référence à consulter concernant la structure des LAR est le document [GAB_ET1].

En conformité avec la [RFC5280], l'entrée « revokedCertificates » est absente s'il n'y a pas de certificat révoqué.

Les LAR sont publiées mensuellement. Leur durée de validité est de 45 jours. Le recouvrement est au minimum de 14 jours et au maximum de 17 jours.

7.3 deltaLCR

Sans objet.

7.4 OCSP

Sans objet.

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 régulièrement, au moins une fois tous les deux ans à un contrôle de conformité de l'ensemble de son 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 AC (ACR ou ACI) 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 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 :

- La DPC et les procédures associées.
- Les clés privées de l'AC et des composantes de l'IGC.
- Les clés privées des ACI.
- Les données d'activation associées aux clés privées d'AC (ACR ou ACI).

- Tous les secrets de l'IGC.
- Les journaux d'évènements des composantes de l'IGC.
- Les éléments relatifs à la cérémonie de clés.
- Les causes de révocations, sauf accord explicite formulé par le Responsable de l'IGC.
- Les rapports des audits.

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.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

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 Informations à caractère personnel

Les informations suivantes sont des informations à caractère personnel :

- Identité des porteurs de secret.
- Identités des opérateurs de l'IGC.
- Demandes de révocation.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

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 personnelles

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles identifiées dans cette PC ne sont ni divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable des personnes concernées, 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 d'informations personnelles

Sans objet.

9.5 Droits sur la propriété intellectuelle et industrielle

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-Santé 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).
- Respecter les accords ou contrats qui les lient entre elles.
- Documenter leurs procédures internes de fonctionnement.
- 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 :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat d'AC (ACR ou ACI) et que ce certificat a été accepté, conformément aux exigences du chapitre 4.4.
- Garantir et maintenir la cohérence de la DPC avec la PC.
- Prendre toutes les mesures raisonnables pour s'assurer que les composantes de l'IGC 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 porteurs 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 9.6.1.

9.6.3 Porteurs de certificats

L'Agence, en tant que porteur des certificats d'AC (ACR ou ACI) a le devoir de :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat.
- Protéger la clé privée par des moyens appropriés à son environnement.
- Protéger ses données d'activation et, le cas échéant, les mettre en œuvre.
- Protéger l'accès à sa base de certificats.
- Respecter les conditions d'utilisation de la clé privée et du certificat correspondant.

9.6.4 Utilisateurs de certificats

Les utilisateurs de certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis.
- Vérifier la signature numérique du certificat 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.

9.6.5 Autres participants

Sans objet.

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 d'AC (ACR ou ACI) 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.

En fonction de la nature et de l'importance des évolutions apportées à la PC, le délai de mise en conformité sera arrêté conformément aux modalités prévues par la réglementation en vigueur.

De plus, 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. Les composantes de l'IGC décrites au chapitre 1.3 sont informées de la révision de la PC.

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

Sans objet (aucun OID n'est associé à cette PC).

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.

9.17 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]	« IGC-Santé – Etape 1 – 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://igc-sante.esante.gouv.fr/PC.
[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 »
[2nd DIS ISO/IEC 11770-3]	« Information Technology – Security Techniques –Key management – Part 3: Mechanisms using asymmetric techniques » - 2e edition

Renvoi	Document
[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

Dans le cas particulier de cette PC, les certificats délivrés sont des certificats d'AC (ACR ou ACI). Les exigences de ce chapitre s'appliquent aussi bien aux modules cryptographiques de l'AC émettrice (une ACR) qu'aux modules cryptographique de l'AC qui se fait certifier (une ACI).

11.1 Exigences sur les objectifs de sécurité

Les modules cryptographiques, utilisés par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LAR, des LCR ou deltaLCR), répond aux exigences de sécurité suivantes :

- Garantir que les générations de bi-clés de signature sont réalisées exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées.
- 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 de ces clés privées.
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité.
- Pour ce qui concerne 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.

11.2 Exigences sur la qualification

Les modules cryptographiques utilisés par l'AC sont qualifiés au niveau renforcé par l'ANSSI, et conformes aux exigences du chapitre 11.1.

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

Sans objet dans le cadre de cette PC qui concerne les AC Racines de l'IGC-Santé et ne délivre pas de certificats finaux.