Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE	MINISTÈRE DES AFFAIRES SOCIALES ET DE LA SANTÉ MINISTÈRE DU TRAVAIL, DE L'EMPLOI ET DU DIALOGUE SOCIAL MINISTÈRE DES DROITS DES FEMMES, DE LA VILLE, DE LA JEUNESSE ET DES SPORTS	

	DATE : 30 avril 2014 NB PAGES : **79** VERSION : 2.0 REFERENCE : IMAGE-IGC-PC05 STATUT : Validé
Projet :	**IMAGE**
Titre :	**POLITIQUE DE CERTIFICATION** **AC HORODATAGE** **OID : 1.2.250.1.179.1.5.1.1.1**

SOMMAIRE

Historique des versions

Version	Date	Modification
1.0	01/12/2009	Première version
2.0	30 avril 2014	Création DSI

Références documentaires

Référence	Titre
[PRIS-PC]	Politique de Référencement Intersectorielle de Sécurité - Version 2.1 Service d'Authentification Politique de Certification Type OID : 1.2.250.1.137.2.2.1.2.2.1
[PRIS-profils]	Politique de Référencement Intersectorielle de Sécurité Service d'Authentification - Politiques de Certification Types - Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques - Version 2.1.
[PC-profils]	IMAGE : Profils de certificats AC Horodatage
[PH]	IMAGE : Politique d'Horodatage

1. INTRODUCTION

1.1. Présentation générale

Présentation du projet IMAGE :

Le développement de l'administration électronique passe par la mise en place de moyens permettant d'apporter la confiance nécessaire à la dématérialisation des processus.

Le projet IMAGE (**I**nfrastructure **M**inistérielle de gestion de clés, de services d'**A**uthentification et de services de confiance pour la **G**estion de la signature **E**lectronique et de la confidentialité) est un projet porté par la Direction des Systèmes d'Information assurant le support des MINISTÈRE DES AFFAIRES SOCIALES ET DE LA SANTE, MINISTÈRE DU TRAVAIL, DE L'EMPLOI ET DU DIALOGUE SOCIAL, MINISTÈRE DES DROITS DES FEMMES, DE LA VILLE, DE LA JEUNESSE ET DES SPORTS, ci-après dénommés « le Ministère ». Ce projet consiste à mettre en œuvre, d'une part, une Infrastructure de Gestion de Clés (IGC) permettant des services d'authentification forte, et d'autre part, une plate-forme de services de confiance

Grâce à la mise en œuvre de l'IGC, le Ministère généralise au sein de son système d'information l'utilisation de services d'authentification forte pour l'accès à différents composants (postes de travail, applications sensibles).

Ce projet s'inscrit notamment dans le champ d'application de l'ordonnance n°2005-1516 du 8 décembre 2005 et « relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ».

Présentation de la Politique de Certification AC Horodatage :

Le présent document fait partie d'un ensemble de documents décrivant les politiques de certification utilisées dans le cadre du projet IMAGE.

Ce document s'applique à un type de certificat émis par une Autorité de Certification (AC), et définit les règles et les exigences auxquelles l'autorité se conforme dans la mise en place des prestations adaptées et appliquées à ce type de certificat.

Le présent document s'applique à l'autorité de certification « AC Horodatage », ci-après dénommée « l'AC », générant un type de certificat utilisé par une unité d'horodatage pour signer ses tampons d'horodatage.

Les unités d'horodatage et l'AC Horodatage contribuent à la fourniture du même service d'horodatage, et sont contenues à l'intérieur du même système technique d'horodatage.

La présente Politique de Certification (PC) couvre la gestion et l'utilisation des clés et des certificats. La gestion d'un certificat comprend notamment l'ensemble des phases du cycle de vie d'un certificat, de la demande d'attribution d'un certificat, jusqu'à la fin de vie de ce certificat (fin de validité ou révocation).

Les détenteurs de rôle de confiance de l'IGC et les tiers utilisateurs des certificats objets de cette Politique ont des obligations spécifiques définies dans cette Politique de Certification.

La politique d'horodatage n'est pas décrite dans le présent document. Elle est définie dans un document distinct [PH].

1.2. Identification du document

L'OID de la présente PC dans sa version 1 est : **1.2.250.1.179.1.5.1.1.1**

Le dernier chiffre permet de faire évoluer le numéro de version du document.

1.3. Relation avec la PRIS

Cette Politique de Certification se veut conforme aux exigences stipulées pour le niveau fort (niveau « 2 étoiles » ou **) des documents [PRIS-PC] et [PRIS-profils].

1.4. Définitions et abréviations

1.4.1. Définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent :

Administrateur central : Personne autorisée par l'AC à opérer les diverses fonctions de l'Autorité, et ayant notamment délégation des fonctions de l'AEL.

Autorité Administrative de l'AC : Personne responsable de l'AC sur le plan réglementaire et juridique.

Autorité de Certification (AC) : Dans le cadre du présent document, ce terme désigne, selon les cas :

- la personne ou l'Autorité chargée de l'application de la présente Politique de Certification,
- l'infrastructure technique réalisant les fonctions dévolues à l'AC. A cet effet, elle utilise notamment les clés de signature de l'AC.

Autorité de Certification Déléguée (ACD) : Autorité de Certification dont la bi-clé est certifiée par l'Autorité Racine.

Autorité de Certification Horodatage (ACH) : une Autorité de Certification Déléguée destinée à émettre les certificats utilisés par l'Autorité d'Horodatage.

Autorité de Certification Racine (ACR) : Autorité de Certification point de confiance de l'IGC IMAGE, et certifiant les Autorités de Certification Déléguées.

Autorité d'Enregistrement Locale : Autorité désignée par l'Autorité Administrative qui a pour rôle d'organiser l'enregistrement du porteur et la gestion des clés.

Autorité d'Horodatage (AH) : autorité responsable de la gestion d'un service d'horodatage.

Certificat [électronique] : Certificat délivré à une personne physique ou à une composante technique et portant sur une bi-clé détenue par celle-ci. L'usage de ce certificat est indiqué au sein de celui-ci (authentification client ou serveur, signature, signature de certificat ou de crl…)

Carte IMAGE : Support cryptographique personnel sous forme de carte à puce délivrée dans le cadre du projet IMAGE, utilisée par le porteur pour stocker et mettre en œuvre ses clés privée et certificats.

Code d'activation : (ou code PIN) Code d'activation de la carte IMAGE choisi par le porteur et permettant l'usage des clés privées associées aux certificats stockés.

Composante de l'AC : Module technique ou plate-forme jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'AC.

Contremarque de temps : donnée qui lie une représentation d'une donnée à un temps particulier, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là.

Coordinated Universal Time (UTC) : échelle de temps liée à la seconde, équivalent au temps solaire au méridien principale (0°), temps moyen de Greenwich (GMT).

Déclaration des Pratiques de Certification : Enoncé des pratiques de certification effectivement mises en œuvre par l'AC pour l'émission, la gestion, la révocation, le renouvellement des certificats en conformité avec la Politique de Certification qu'elle s'est engagée à respecter.

Identifiant d'objet (OID) : Série d'entiers globalement unique permettant d'identifier un objet.

Infrastructure de Gestion de Clés (IGC) : Ensemble de composantes, fonctions et procédures dédiées à la génération et à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance.

Liste des Certificats Révoqués (LCR) : Liste signée indiquant un ensemble de certificats qui ne sont plus considérés comme valides par l'AC.

Politique de Certification : Ensemble de règles, comportant un identifiant (OID) et définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes.

Politique d'horodatage (PH) : ensemble de règles portant un nom qui indique l'applicabilité d'une contremarque de temps à une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes.

Porteur : Personne physique identifiée dans le certificat et détentrice de la clé privée correspondant à la clé publique présente dans ce certificat, la clé privée étant contenue dans la carte IMAGE du porteur.

Rôle de confiance : Rôle dévolu à un acteur intervenant dans la mise en œuvre ou l'exploitation de l'AC afin d'assurer, ou maintenir en opération, une ou plusieurs de ses fonctions.

Service d'horodatage: ensemble de prestations nécessaires à la génération et à la gestion de contremarques de temps

Tiers utilisateur : Utilisateur ou système faisant confiance à un certificat.

Tiers utilisateur d'un jeton d'horodatage : application ou service utilisateur d'un jeton d'horodatage.

Unité d'Horodatage : ensemble de matériel et logiciel en charge de la création de contremarques de temps qui a une seule clé de signature de contremarques de temps active à un instant donné.

X.509 v3 : Format standard de certificat électronique.

1.4.2. Abréviations

Pour les besoins du présent document, les abréviations suivantes s'appliquent :

AA	Autorité Administrative
AC	Autorité de Certification
ACD	Autorité de Certification Déléguée
ACH	Autorité de Certification Horodatage
ACR	Autorité de Certification Racine
AEL	Autorité d'Enregistrement Locale
AH	Autorité d'Horodatage
CN	*Common name* ; nom commun
DN	*Distinguished Name* ; nom distinctif
DPC	Déclaration des Pratiques de Certification
EAL	*Evaluation Assurance Level* ; niveau d'assurance d'évaluation d'un objet de sécurité selon les Critères Communs. Par exemple : EAL 2+ (« niveau EAL 2 augmenté »), EAL 4+ (« niveau EAL4 augmenté »)

IGC	Infrastructure de Gestion de Clés
IMAGE	Infrastructure Ministérielle de gestion de clés, de services d'Authentification et de services de confiance pour la Gestion de la signature
LCR	Liste des Certificats Révoqués
LDAP	*Light Directory Access Protocol* ; protocole d'interrogation et de modification de contenu d'annuaire
OID	*Object Identifier* ; Identifiant d'objet
PIN	*Personal Identification Number* ; nombre personnel d'identification
PC	Politique de Certification
PRIS	Politique de Référencement Intersectorielle de Sécurité
RSA	*Rivest Shamir Adleman* ; algorithme de chiffrement asymétrique, du nom de leurs trois inventeurs.
UTC	*Universal Time Coordinated* ; temps universel coordonné

1.5. Entités intervenant dans l'IGC

1.5.1. Autorité Administrative

Le rôle d'Autorité Administrative est assuré par le Directeur de la Direction des Systèmes d'Information (DSI) du Ministère.

Les fonctions assurées par l'Autorité Administrative en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- rendre accessible l'ensemble des prestations déclarées dans la PC aux administrateurs et aux tiers utilisateurs.
- s'assurer que les exigences de la PC et les procédures de la DPC sont adéquates et conformes aux normes en vigueur.
- s'assurer que ces exigences et procédures sont appliquées par chacun des détenteurs de rôles auprès de l'IGC.
- mettre en œuvre les mesures de sécurité techniques et non techniques nécessaires pour couvrir les risques identifiés et assurer la continuité de l'activité de l'IGC en conformité avec les exigences de la présente PC.
- mettre en œuvre les différentes fonctions identifiées dans la PC, notamment en matière de génération des certificats, de gestion des révocations et d'information sur l'état des certificats.
- mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans la présente PC, notamment en termes de fiabilité, de qualité et de sécurité.
- générer, et renouveler lorsque nécessaire, la bi-clé de l'AC et le certificat correspondant (signature de certificats, de LCR et de réponses OCSP).
- Diffuser son certificat d'AC aux administrateurs et aux tiers utilisateurs de certificats.

1.5.2. Autorité de Certification

Le rôle d'Autorité de Certification est assuré par le Sous-directeur de la sous direction infrastructures et support aux utilisateurs (SDISU).

L'Autorité de Certification (AC) a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) et s'appuie pour cela sur une infrastructure technique : une Infrastructure de Gestion de Clés (IGC).

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

Fonction de génération des certificats : Cette fonction génère les certificats à partir des informations transmises par l'Autorité d'Enregistrement Locale.

Fonction de publication : Cette fonction met à disposition des différentes parties concernées les différents documents établis par l'AC (Politiques et Pratiques…), les certificats d'AC et toute autre information pertinente destinée aux administrateurs et aux tiers utilisateurs de certificats, hors informations d'état des certificats.

Fonction de gestion des révocations : Dans le cadre de cette fonction, l'AC traite les demandes de révocation (notamment identification et 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 tiers utilisateurs de certificats des informations sur l'état des certificats (révoqués, non révoqués). Cette fonction est mise en oeuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR) et également selon un mode requête / réponse temps réel au moyen d'un service OCSP.

1.5.3. Autorité d'Enregistrement Locale

Le rôle d'AEL est assuré par la DSI.

Sur le plan opérationnel, le rôle d'AEL est assuré par les administrateurs centraux de l'AC Horodatage.

L'AEL assure les fonctions suivantes :

Fonction d'enregistrement d'une unité d'horodatage (UH) : Cette fonction assure la vérification des informations d'identification de l'UH, et de son enregistrement en vue de l'obtention d'un certificat. La

fonction inclut, lorsque cela est nécessaire, la re-vérification des informations fournies par l'administrateur lors du renouvellement du certificat par celui-ci.

Fonction d'enregistrement des administrateurs : Cette fonction assure la vérification des informations d'identification, et l'enregistrement des futurs administrateurs. La fonction inclut, lorsque cela est nécessaire, la re-vérification des informations de l'administrateur lors du renouvellement du certificat de celui-ci.

Fonction de gestion des révocations : Dans le cadre de cette fonction, l'AEL enregistre les demandes de révocation pour transmission et traitement par l'AC.

Dans le cadre de ces fonctions, l'AEL assure notamment les tâches suivantes :

- la prise en compte et la vérification des informations d'un futur administrateur, ainsi que la constitution du dossier d'enregistrement correspondant ;
- la prise en compte et la vérification des informations d'une UH, la vérification de l'identité de l'administrateur ainsi que la constitution du dossier d'enregistrement correspondant ;
- l'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC;
- la conservation des pièces des dossiers d'enregistrement ;
- la conservation et la protection en confidentialité et en intégrité des données personnelles de l'administrateur, y compris lors des échanges de ces données avec les autres fonctions de l'IGC.

Pour l'enregistrement des premiers administrateurs dans l'AC Horodatage, le rôle d'opérateur d'enregistrement est rempli par le super-administrateur d'installation.

Successivement ce rôle est rempli par les administrateurs.

L'AEL a aussi pour rôle de d'assurer l'interface avec les administrateurs disposant d'un certificat en cours de validité. Pour cela, l'AEL assure les tâches suivantes :

- la prise en compte des demandes de révocation,
- le renouvellement des certificats émis.

1.5.4. Administrateur du service d'horodatage, ou administrateur

Les administrateurs assurent le rôle d'administration technique de l'AC Horodatage, et le rôle d'opérateur d'enregistrement.

Ils assurent également le rôle d'administrateur des unités d'horodatage.

L'administrateur utilise sa clé privée d'authentification et le certificat correspondant dans le cadre de ses activités professionnelles et aux seules fins pour lesquelles le certificat a été émis. L'administrateur est un agent du Ministère.

L'administrateur établit la demande initiale d'enregistrement d'une UH. Il est responsable de la bonne mise en œuvre du couple clé privée / certificat d'authentification de l'UH.

Le certificat étant attaché à l'UH et non à l'administrateur, ce dernier peut être amené à changer en cours de validité du certificat : départ de l'administrateur, changement d'affectation et de responsabilité au sein de l'entité, etc.

En cas de changement de l'administrateur, le nom de l'administrateur doit être modifié pour chaque certificat dans la base de données de l'AC. Le certificat émis conserve l'identifiant (adresse e-mail) de l'administrateur ayant effectué la demande initiale de certificat.

1.5.5. Tiers utilisateurs des certificats

Les tiers utilisateurs des certificats d'unités d'horodatage émis dans le cadre de la présente PC sont les destinateurs et utilisateurs des tampons d'horodatage, afin de vérifier la chaîne de certification associée.

1.6. Usage des certificats

1.6.1. Bi-clés et certificats administrateurs

La présente PC traite des bi-clés et des certificats à destination des administrateurs identifiés ci-dessus, afin que ces administrateurs puissent s'authentifier auprès de l'AC Horodatage.

L'utilisation des clés privées et des certificats associés émis par l'AC Horodatage doit rester limitée à l'usage identifié dans la présente PC.

L'AC décline toute responsabilité en ce qui concerne l'utilisation des certificats pour des usages autres que ceux qui sont définis dans la présente PC.

1.6.2. Bi-clés et certificats des Unités d'Horodatage

La présente PC traite des bi-clés et des certificats à destination des UH identifiées ci-dessus, afin que ces UH puissent émettre des tampons d'horodatage.

L'utilisation des clés privées et des certificats associés émis par l'AC Horodatage doit rester limitée à l'usage identifié dans la présente PC.

L'AC décline toute responsabilité en ce qui concerne l'utilisation des certificats pour des usages autres que ceux qui sont définis dans la présente PC.

1.6.3. Bi-clés et certificats de l'AC Horodatage et de ses composantes

L'AC dispose de plusieurs clés et certificats décomposés de la manière suivante :

- la clé de signature de l'AC utilisée pour signer les certificats générés par l'AC ainsi que les informations sur l'état des certificats (LCR et réponses OCSP),
- les clés internes d'infrastructure, utilisées par les composantes de l'AC à des fins de signature et de chiffrement des données échangées ou stockées au sein de l'IGC.

Le certificat de l'AC Horodatage émis par l'Autorité racine du Ministère, ainsi que les certificats des composantes et les engagements relatifs à ces certificats, font l'objet du document [PC-ACR].

1.7. Gestion de la PC

1.7.1. Entité gérant la Politique de Certification

L'AC est responsable de l'établissement de la présente Politique de Certification, de son application et de sa diffusion.

L'Autorité Administrative est responsable de la validation de la présente PC.

1.7.2. Mise à jour de la PC

Les différentes versions de cette PC sont établies par l'AC et validées par l'AA.

Le numéro de version de la PC est modifié à chaque nouvelle version, et le tableau contenant l'historique des versions mises en application est maintenue à jour.

Par contre l'OID de la PC est modifié uniquement si un attribut fonctionnel du certificat est modifié.

Dans ce cas :

- la PC est mise à jour avec la nouvelle description fonctionnelle, ainsi que le nouvel OID,
- le profil de certificat est modifié ; le nouvel OID remplace l'OID précédent dans le certificat,
- la nouvelle version de la PC est publiée ; l'ancienne version de la PC reste accessible, tant que des certificats contenant une référence à l'ancienne OID restent valides.

L'OID n'est pas modifié en cas de modification technique de profil de certificat.

1.7.3. Point de contact

Pour toute information relative à la présente PC, il est possible de contacter :

MINISTÈRE DES AFFAIRES SOCIALES ET DE LA SANTE

MINISTÈRE DU TRAVAIL, DE L'EMPLOI ET DU DIALOGUE SOCIAL

MINISTÈRE DES DROITS DES FEMMES, DE LA VILLE, DE LA JEUNESSE ET DES SPORTS

Direction des Systèmes d'Information/ SDISU/ Bureau I3P Projet IMAGE

Tour Mirabeau

39-43 Quai André Citroën 75902 PARIS CEDEX 15

dsi-sdisu-prod-image@sg.social.gouv.fr

1.7.4. Déclaration des Pratiques de Certification (DPC)

L'AC s'engage à rédiger le document [DPC], décrivant les procédures et mesures mises en œuvre pour le respect des dispositions de la présente PC. Ce document n'est pas public.

Ce document est fourni à l'auditeur lors d'un audit interne de l'AC.

1.7.5. Procédure d'approbation de la DPC

Le document [DPC] est approuvé par l'AA afférente.

2. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS PUBLIEES

2.1. Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des utilisateurs de certificat, l'AC met en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats.

2.2. Informations publiées

L'AC publie les informations suivantes à destination des utilisateurs de certificats :

- les politiques de certification en cours de validité,
- les profils des certificats, de la LCR et des réponses OCSP,
- la Liste des Certificats Révoqués en cours (LCR) [1],
- les certificats de l'AC en cours de validité,
- les certificats auto-signés de l'AC Racine du Ministère à laquelle elle est subordonnée, ou les informations permettant aux tiers utilisateurs de certificats de s'assurer de l'origine de ces certificats (empreintes),
- l'adresse permettant d'obtenir des informations concernant l'AC Racine du Ministère,
- les certificats auto-signés de l'IGC/A à laquelle l'AC Racine du Ministère est subordonnée, ou les informations permettant aux tiers utilisateurs de certificats de s'assurer de l'origine de ces

[1] L'adresse de la LCR figure pour chaque certificat dans l'extension « *CRLdistributionPoint* ». Le protocole HTTP est utilisé.

certificats (empreintes),

- l'adresse permettant d'obtenir des informations concernant l'IGC/A.

Ces éléments sont disponibles sur le site « igc.sante.gouv.fr ».

L'AC fournit en outre un service OCSP en accès libre sur Internet, selon le protocole HTTP, à destination des tiers utilisateurs de certificat, leur permettant de connaître l'état révoqué/ non révoqué des certificats. L'adresse de ce service est indiquée dans l'extension « *AuthorityInformationAccess* » de chaque certificat.

2.3. Délais et fréquences de publication

Les délais et les fréquences de publication dépendent des informations concernées :

Informations liées à l'IGC (nouvelle version de la Politique de Certification, etc.)	
Délais de publication	L'information est publiée 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.
Disponibilité de l'information	L'infrastructure assurant cette fonction est disponible les jours ouvrés, avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 8 heures (jours ouvrés) et une durée totale maximale d'indisponibilité par mois de 32 heures, ceci hors cas de force majeure.

Certificats d'AC	
Délais de publication	Ceux-ci sont diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants sous un délai de 24 heures.
Disponibilité de l'information	L'infrastructure assurant cette fonction a une disponibilité de 24h/24 7j/7, avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2 heures et une durée totale maximale d'indisponibilité par mois de 8 heures, ceci hors cas de force majeure.
Informations d'état des certificats	
Délais de publication	Les exigences portant sur la fonction de publication de ces informations sont définies au chapitre 4.11.2.
Disponibilité de l'information	

2.4. Contrôle d'accès aux informations publiées

L'information publiée est accessible avec accès en lecture seulement sur le site Internet du Ministère, à l'adresse suivante : http://igc.sante.gouv.fr

L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) est strictement limité aux rôles de confiance de l'IGC adéquats et identifiés, au travers d'un **contrôle d'accès fort** (basé sur une authentification au moins à deux facteurs).

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux rôles de confiance de l'IGC adéquats et identifiés, au travers d'un **contrôle d'accès de type mot de passe,** basée sur une politique de gestion stricte des mots de passe.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1. Nommage

3.1.1. Types de noms

Dans chaque certificat, émis au format X.509v3, l'AC émettrice et le sujet (« Subject ») sont identifiés par un nom distinctif (« *Distinguished Name* » ou DN) de type X.501.

3.1.2. Utilisation de noms explicites

Le nom choisi pour désigner les certificats d'UH est explicite, le champ sujet a la structure suivante :

CN=<nom de l'UH>

OU=0002 110 036 035 00019
O= Ministere en charge des affaires sanitaires et sociales
C=FR

Les noms choisis pour désigner les administrateurs de certificats sont explicites, le champ sujet a la structure suivante :

CN= <prénom nom>

OU=0002 110 036 035 00019
O= Ministere en charge des affaires sanitaires et sociales
C=FR

Le nom commun de l'administrateur (CN) est constitué à partir des prénom et nom de son état civil tel que porté sur les documents d'identité présentés lors de son enregistrement auprès de l'AEL.

3.1.3. Unicité des noms

3.1.3.1 UH

Afin d'assurer l'identification unique d'une UH dans ses certificats successifs (renouvellement) et pour éviter toute ambiguïté, le DN du champ « *Subject* » de chaque certificat ne peut être réutilisé.

3.1.3.2 Administrateur

Afin d'assurer l'identification unique de l'administrateur au sein du domaine de l'AC dans ses certificats successifs (renouvellement) et pour éviter toute ambiguïté, le DN attribué à un administrateur ne peut être attribué à un autre administrateur, et ce durant toute la durée de vie de l'AC.

3.1.4. Autres identifiants

Les certificats des administrateurs contiennent dans l'extension « *SubjectAlternativeName* » l'adresse de messagerie professionnelle de l'administrateur.

3.2. Validation initiale de l'identité

3.2.1. Méthode pour prouver la possession de la clé privée

Pour les certificats d'UH, la bi-clé est générée par l'AC.

Pour les administrateurs, la bi-clé est générée par la carte IMAGE lors d'un face-à-face avec l'opérateur d'enregistrement en utilisant le matériel / logiciel de l'opérateur d'enregistrement.

3.2.2. Validation de l'identité d'un administrateur

L'authentification de l'administrateur par l'AEL est réalisée lors d'un face-à-face physique, à partir d'une pièce d'identité[2], en cours de validité et comportant une photographie.

[2] Carte Professionnelle d'Identité du Ministère, Carte d'accès à l'un des sites du Ministère comportant nom et photographie, Carte Nationale d'Identité, Passeport, Permis de conduire, ou autre document officiel d'identité (carte de séjour…)

3.2.3. Informations non vérifiées des administrateurs

Les adresses de messagerie professionnelles ainsi que les différents éléments identifiants techniques destinés à être contenus dans les certificats et déclarés par un administrateur ne sont pas vérifiées.

3.3. Identification et validation pour le renouvellement des clés

Le renouvellement de la bi-clé d'une UH ou d'un administrateur entraîne la génération et la fourniture d'un nouveau certificat associé à la nouvelle bi-clé.

3.3.1. Identification et validation pour un renouvellement courant

En cas de renouvellement, l'administrateur s'identifie et s'authentifie en présentant une pièce d'identité, comme pour l'enregistrement initial.

3.3.2. Identification et validation pour un renouvellement après révocation

Suite à la révocation d'un certificat, quelle qu'en soit la cause, il n'y a pas de renouvellement possible du certificat. La procédure à suivre est celle de l'enregistrement initial.

3.4. Identification et validation pour une révocation

En cas de besoin, la demande de révocation d'un certificat d'UH est enregistrée par l'administrateur auprès de l'AEL.

L'AEL procède à la révocation du certificat de façon immédiate dès la réception de la demande.

De même, la révocation d'un certificat administrateur est enregistrée par celui-ci auprès de l'AEL.

Dans tous les cas, le porteur confirme sa demande de révocation par mail, en utilisant son adresse de messagerie professionnelle.

L'AEL procède à la révocation du certificat de façon immédiate dès la réception de la demande.

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

La présente PC concerne 2 types de certificat et d'enregistrement :

- Les certificats d'administrateur de l'Horodatage
- Les certificats d'Unité d'Horodatage (UH)

Dans les 2 cas l'enregistrement est effectué par un administrateur de l'AC Horodatage.

4.1. Enregistrement initial

4.1.1. Origine de l'enregistrement initial

Les enregistrements se limitent à ceux nécessaires pour le fonctionnement du service d'horodatage : administrateurs du service d'horodatage, et unités d'horodatage.

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

Certificats administrateur :

Les éléments d'identification relatifs au nouvel administrateur contenus dans la demande de certificat sont déclarés par le porteur.

Certificats UH :

Le formulaire d'enregistrement, contenant les éléments d'identification nécessaires, est rempli par l'administrateur de l'UH et signé par celui-ci.

4.2. Déroulement de l'enregistrement

4.2.1. Processus d'identification et de validation

L'identité de la personne physique est vérifiée conformément aux exigences du chapitre précédent.

L'AEL effectue les opérations suivantes pour l'enregistrement d'un futur administrateur :

- valide l'identité du futur administrateur,
- informe le futur administrateur sur les modalités applicables à l'utilisation du certificat, ou s'assure que ce dernier dispose de ces informations,
- fournit une carte IMAGE et prend en compte la demande de certificat.

L'AEL conserve ensuite une trace des justificatifs présentés.

Pour les certificats d'UH, l'AEL effectue les opérations suivantes :

- valide l'identité de l'UH à certifier,
- identifie la politique d'horodatage à appliquer,
- identifie l'administrateur de l'UH, et obtient son adresse de courrier électronique.

L'AEL conserve ensuit une trace des justificatifs présentés.

4.2.2. Acceptation ou rejet de l'enregistrement

L'administrateur vérifie les données d'enregistrement avant validation de la demande par l'AEL et envoi à l'AC.

4.2.3. Durée d'établissement du certificat

Les certificats d'administrateur sont valables pour une durée de trois ans.

Les certificats d'UH sont valables pour une durée de sept ans.

4.3. Délivrance du certificat

4.3.1. Actions de l'AC concernant la délivrance du certificat

Pour les administrateurs, suite à l'authentification de l'origine de la demande provenant de l'AEL, l'AC déclenche le processus de génération du certificat.

Pour les UH, l'AC déclenche le processus de génération de bi-clé en central dans l'HSM de l'AC, et génère le certificat.

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

Pour un administrateur, la remise du certificat se fait sur la carte IMAGE lors de la session face-à-face.

Pour l'UH, le certificat est transféré dans l'UH par une opération technique interne au système d'horodatage.

4.4. Acceptation du certificat

Un administrateur ne peut prendre possession du dispositif qu'après l'acceptation de l'attribut CN contenu dans le champ « *Subject* » du certificat ainsi que de l'adresse de messagerie contenue dans l'extension « *SubjectAlternativeName* » du certificat.

La personnalisation du code PIN de la carte IMAGE par son porteur, à l'invitation de l'opérateur d'enregistrement, ainsi que l'utilisation du certificat, marquent l'acceptation de celui-ci par le nouvel administrateur.

4.5. Publication du certificat

Les certificats ne sont pas publiés.

4.6. Usages de la bi-clé et du certificat

4.6.1. Utilisation de la clé privée et du certificat par l'UH

Pour un certificat du type horodatage, l'utilisation de la clé privée de l'UH et du certificat associé est strictement limitée à la signature de contremarques de temps.

Les administrateurs doivent s'assurer du respect strict des usages autorisés des bi-clés et des certificats au niveau de l'UH. Dans le cas contraire, leur responsabilité est engagée.

L'usage autorisé de la bi-clé d'horodatage et du certificat associé est indiqué dans le certificat lui-même, via les extensions concernant les usages des clés ou des extensions spécifiques :

- par la présence de l'extension critique « *keyUsage* » qui prend la valeur « *digitalSignature* » et de l'extension critique « *extendedKeyUsage* » qui prend la valeur « *timeStamping* »,

4.6.2. Utilisation de la clé privée et du certificat par les administrateurs

Pour un certificat du type authentification pour les administrateurs de l'AC Horodatage, l'utilisation de la clé privée et du certificat associé est strictement limitée au service d'établissement d'une session sécurisée de type client SSL avec authentification du porteur vis-à-vis des composantes de l'AC Horodatage. L'usage autorisé de la bi-clé et du certificat associé est indiqué dans le certificat lui-même, par la présence de :

- l'extension critique « *keyUsage* » qui prend la valeur « *digitalSignature* »,
- l'extension non critique « *extendedKeyUsage* » qui prend la valeur « *ClientAuthentication* »

L'adresse de messagerie professionnelle de l'administrateur figure dans le champ « *SubjectAlternativeName* ». Cette adresse ne doit pas être utilisée à des fins de chiffrement ou d'authentification de messages.

Les porteurs concernés doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité est engagée.

4.6.3. Utilisation de la clé publique et du certificat par un tiers utilisateur

Les certificats horodatage doivent uniquement être utilisés pour les usages mentionnés ci-dessus.

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

4.7. Renouvellement d'un certificat sans changement de bi-clé

Le simple renouvellement du certificat (changement des dates de validité du certificat, sans changement de la bi-clé) n'est pas supporté.

4.8. Renouvellement d'un certificat avec changement de la bi-clé

Les certificats et les bi-clés des administrateurs sont renouvelés tous les trois ans.

Les certificats et les bi-clés des UH sont renouvelés tous les ans.

4.8.1. Causes possibles de changement d'une bi-clé

Les bi-clés sont changées à chaque renouvellement de certificat.

Dans le cas où un certificat est révoqué, la bi-clé et le certificat sont renouvelés par anticipation. Ce cas suit alors le processus d'enregistrement initial, et non celui du renouvellement.

4.8.2. Origine d'une demande de renouvellement de certificat

Les administrateurs sont informés par courriel de la prochaine expiration de leurs certificats et des certificats dont ils ont la charge et sont invités à les renouveler.

4.8.3. Procédure de traitement d'une demande de renouvellement de certificat

L'identification se déroule comme précisée dans le paragraphe §3.3.1, et l'enregistrement se poursuit comme pour l'enregistrement initial, voir §4.2.

4.8.4. Notification au porteur de l'établissement du nouveau certificat

Le renouvellement a lieu en face-à-face ; la procédure de notification du nouveau certificat à

l'administrateur est identique à celle de l'enregistrement initial.

4.8.5. Démarche d'acceptation du nouveau certificat

La démarche d'acceptation du nouveau certificat est identique à celle d'acceptation du certificat originel.

Le certificat renouvelé contient les mêmes informations d'identification que le certificat orginel.

4.8.6. Publication du nouveau certificat

Le certificat renouvelé n'est pas publié.

4.9. Modification du certificat

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

4.10. Révocation et suspension des certificats

4.10.1. Causes possibles d'une révocation

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

- les informations de l'UH figurant dans son certificat ne sont plus valables, ceci avant l'expiration normale du certificat ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- la clé privée de l'UH est suspectée de compromission ou a été compromise ;
- l'UH est définitivement arrêtée ;
- l'administrateur n'a pas respecté les modalités d'utilisation du certificat ;
- l'administrateur n'a pas respecté ses obligations découlant de la PC de l'AC,

- le certificat n'a plus d'administrateur clairement identifié.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications), le certificat concerné doit être révoqué.

En cas de cessation d'activité de l'administrateur, celui-ci en informe l'AEL et un nouvel administrateur est désigné. Dans le cas contraire, la révocation du certificat de l'UH concernée est réalisée.

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

- l'une des informations nominatives de l'administrateur figurant dans son certificat est périmée, ceci avant l'expiration normale du certificat[3] ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement de l'administrateur ;
- la carte IMAGE est perdue ou est volée ;
- l'administrateur ne dispose plus des droits d'administration pour lesquels le certificat lui avait été émis ;
- la carte IMAGE est détruite ou n'est plus en état de fonctionnement.

Lorsque l'une des circonstances ci-dessus se réalise ; le certificat concerné doit être révoqué.

4.10.2. Origine d'une demande de révocation

Les personnes qui peuvent demander la révocation d'un certificat d'UH sont les suivantes :

- Dans le cas d'un certificat d'UH : son administrateur ou le responsable hiérarchique de celui-ci ;
- Dans le cas d'un certificat administrateur : l'administrateur ou le responsable hiérarchique de celui-ci ;

[3] Il appartient à l'administrateur de signaler tout changement dans celles-ci.

- l'AC,
- l'AEL.

4.10.3. Procédure de traitement d'une demande de révocation

Pour révoquer un certificat dont il a la responsabilité, un administrateur doit demander cette révocation à l'AEL, avec confirmation de la demande par messagerie électronique professionnelle.

L'AEL prend en compte la demande quelle que soit son mode de transmission initial et sans attendre la confirmation par messagerie.

L'administrateur peut préciser la cause de la révocation à l'AEL, qui la saisit dans le dossier à l'aide d'un commentaire libre.

L'AEL confirme à l'administrateur la bonne prise en compte de la demande de révocation, par messagerie électronique.

Une fois la demande reçue et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée via une LCR et est aussi accessible au service OCSP.

L'opération est enregistrée dans les journaux d'évènements avec, le cas échéant, la cause ayant entraîné la révocation du certificat.

Les causes de la révocation ne sont pas publiées.

4.10.4. Délai accordé à l'administrateur pour effectuer la révocation

Dès que l'administrateur a connaissance qu'une des causes possibles de révocation se vérifie, il doit effectuer sa demande de révocation sans délai.

4.10.5. Délai de traitement par l'AC d'une demande de révocation

L'AEL traite pendant les jours et heures ouvrés les demandes de révocation reçues.

Le traitement de la révocation suite à l'enregistrement de la demande se déroule sans délai.

La disponibilité de cette fonction de gestion des révocations en ligne est la suivante :

Disponibilité	24h / 24 7j / 7
Durée maximale d'indisponibilité par interruption de service (panne ou maintenance)	une heure
Durée maximale totale d'indisponibilité par mois	4 heures

Toute révocation de certificat est effective dans un délai inférieur ou égal à un jour ouvré, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des tiers utilisateurs de certificats.

4.10.6. Exigences de vérification de la révocation par les tiers utilisateurs de certificats

Les tiers utilisateurs de certificats sont tenus de vérifier, avant leur utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée, consultation de la LCR en cours de validité ou interrogation OCSP, ainsi que la fréquence des interrogations (liée à la durée de validité des informations éventuellement gardées dans un cache) est à l'appréciation des tiers utilisateurs de certificats selon les contraintes liées à leur application.

4.10.7. Fréquence d'établissement de la LCR

Une nouvelle LCR est publiée toutes les 12 heures. En outre, l'AC peut émettre une LCR mise à jour, sans attendre la publication faite toutes les douze heures.

Chaque LCR est émise avec une durée de validité de 72 heures.

4.10.8. Délai maximum de publication d'une LCR

Une LCR est publiée dans un délai maximum de 30 minutes suite à sa génération.

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

Un service OCSP est mis en œuvre. L'adresse de ce service est spécifiée pour chaque certificat dans l'extension « *authorityInformationAccess* » . Ce service est disponible en accès libre depuis Internet.

4.10.10. Autres moyens disponibles d'information sur les révocations

Les administrateurs centraux ont la possibilité, après authentification, de vérifier l'état révoqué / non révoqué d'un certificat en interrogeant directement l'application de l'IGC.

4.10.11. Exigences spécifiques en cas de compromission de la clé privée

La clé privée contenue dans une UH peut être compromise dans les cas suivants :

- L'UH a fait l'objet d'une attaque.

Pour les UH, les administrateurs sont tenus de demander la révocation des certificats dans les meilleurs délais en cas de compromission suspectée ou réelle.

La clé privée d'un administrateur contenue dans la carte IMAGE peut être compromise dans les cas suivants :

- le code d'activation et la carte IMAGE ont tous les deux été obtenus sous la contrainte par un attaquant ou par négligence de l'administrateur,
- le code d'activation a été espionné, puis la carte IMAGE a été volée,
- la carte IMAGE a été volée ou perdue, puis a fait l'objet d'une attaque en laboratoire.

En cas de vol ou suspicion de vol, l'administrateur est tenu d'effectuer une demande de révocation dans les meilleurs délais.

En cas de suspicion de compromission de son code d'activation, l'administrateur est tenu de le changer lui-même sans tarder.

En cas de suspicion de perte ou d'oubli de sa carte IMAGE, il est recommandé à l'administrateur d'effectuer une demande de révocation, s'il ne le retrouve pas sous un délai maximum de 24 heures.

4.10.12. Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC.

4.11. Fonction d'information sur l'état des certificats

4.11.1. Caractéristiques opérationnelles

L'AC fournit aux tiers utilisateurs de certificat les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat, c'est-à-dire :

- de vérifier la signature du certificat par l'AC Horodatage,
- de vérifier la présence ou non du certificat dans la LCR émise par l'AC Horodatage,
- de vérifier la signature de cette LCR par l'AC Horodatage.

via la consultation libre de la LCR.

La LCR émise par l'AC Horodatage est au format V2 et est accessible au moyen du protocole HTTP depuis Internet.

Les informations nécessaires à la vérification du statut du certificat de l'AC Horodatage relèvent de la responsabilité de l'AC Racine et peuvent donc être obtenues auprès de celle-ci.

4.11.2. Disponibilité de la fonction

La disponibilité de la fonction d'information sur l'état des certificats est la suivante :

Disponibilité	24h / 24 et 7j / 7
Durée maximale d'indisponibilité par interruption de service (panne ou maintenance)	inférieure à 2 heures
Durée maximale totale d'indisponibilité par mois	inférieure à 8 heures

4.12. Séquestre de clé et recouvrement

Les clés privées des administrateurs et des UH ne sont pas séquestrées.

4.13. Blocage d'une carte IMAGE

La carte IMAGE se bloque si, pour une période définie, le nombre autorisé de trois tentatives de saisie de code PIN est dépassé.

Pour des cartes IMAGE générées sur l'AC Horodatage :

- si le PIN est connu, la carte peut être débloquée
- si le PIN est inconnu, il n'est pas possible de débloquer la carte ; elle doit être recyclée.

5. MESURES DE SECURITE NON TECHNIQUES

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

L'infrastructure de l'IGC est hébergée sur le site nominal dans un local sécurisé vis-à-vis des risques naturels.

Une infrastructure de secours est hébergée dans un local sécurisé vis-à-vis des risques naturels sur un autre site, distant du site nominal de plusieurs kilomètres.

5.1.2. Accès physique

Les zones hébergeant les systèmes informatiques de l'AC sont physiquement protégées. 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 un tel accès.

5.1.3. Alimentation électrique et climatisation

Les serveurs hébergeant l'IGC sur le site nominal bénéficient d'une double alimentation électrique. Les modules cryptographiques de l'IGC bénéficient d'une alimentation secourue.

Les locaux hébergeant l'IGC sont climatisés.

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

5.1.4. Vulnérabilité aux dégâts des eaux

Les locaux hébergeant l'IGC sont protégés contre les dégâts des eaux :

- par un dispositif de détection d'eau,
- par le plan de prévention des inondations.

5.1.5. Prévention et protection incendie

Les locaux hébergeant l'IGC bénéficient des moyens de prévention et de lutte contre les incendies par des dispositifs de détection d'incendie et d'extinction.

Les alertes remontées par les dispositifs contre les dégâts des eaux et contre l'incendie sont remontées au PC Sécurité, dans le cadre de la GTC (Gestion Technique Centralisée).

5.1.6. Conservation des supports

Les sauvegardes des données et de l'application IGC sont conservées dans une enceinte sécurisée, accessible aux seules personnes autorisées.

Les supports papier de l'IGC sont également conservés avec des mesures de sécurité compatibles avec leur niveau de sensibilité.

La DPC identifie les différentes informations et données intervenant dans les activités de l'AC, ainsi que les mesures de sécurité qui leur sont appliquées, afin d'en garantir la confidentialité, l'intégrité et la disponibilité.

5.1.7. Mise hors service des supports

Les supports papier et électroniques de l'IGC en fin de vie sont systématiquement détruits par des moyens appropriés, permettant d'éviter toute perte de confidentialité.

Les matériels et supports informatiques de l'IGC ne sont pas utilisés à d'autres fins avant destruction complète des informations liées à l'IGC qu'ils sont susceptibles de contenir.

5.1.8. Sauvegardes hors site

Les sauvegardes sont conservées sur un site externe selon la Politique de Sauvegarde.

5.2. Mesures de sécurité procédurales

5.2.1. Rôles de confiance auprès de l'AC

Les rôles de confiance définis au niveau de l'AC sont :

Administrateur central : Personne chargée de la configuration applicative et du maintien en conditions opérationnelles de l'application IGC, de l'habilitation des opérateurs d'enregistrement, ainsi que de l'analyse régulière des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc, et ayant également reçu délégation du rôle d'AEL, et réalisant à ce titre les opérations de gestion des certificats serveurs et porteurs.

Auditeur : Personne désignée par l'Autorité Administrative et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par l'AC par rapport à la Politique de Certification et à la Déclaration des Pratiques de Certification de l'AC.

Autorité Qualifiée : Personne chargée de la Sécurité de l'application IGC pour le compte de l'Autorité Administrative.

Responsable de l'application IGC : Personne ayant reçu délégation par l'AC de la mise en oeuvre de la Politique de Certification et de la Déclaration des Pratiques de Certification de l'AC, au niveau de l'application IGC. Sa responsabilité couvre l'ensemble des fonctions rendues par l'application IGC et des performances correspondantes.

Responsable Qualité : Personne ayant reçu délégation par l'AC de la vérification de la cohérence des actions des différents rôles décrits précédemment et de la qualité des processus de l'IGC.

5.2.2. Rôles de confiance mutualisés à d'autres applications

Ci-dessous sont décrits les fonctions assurées par ces rôles dans le cadre de l'IGC ou ayant une

incidence sur les processus de l'IGC :

Administrateur Sécurité : Personne chargée d'assurer la gestion de la sécurité au niveau des systèmes.

Administrateur système : Personne chargée d'assurer l'administration des systèmes, la mise en route et la configuration des équipements composant l'infrastructure. Elle réalise notamment le contrôle des fichiers d'audit du système, ainsi que de l'analyse courante des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

Exploitant : Personne chargée d'assurer l'exploitation, la surveillance et la maintenance des systèmes et des réseaux.

Fonctionnaire de Sécurité des Systèmes d'Informations (FSSI) : Personne chargée de la Politique de Sécurité du SI du Ministère.

Responsable de production : Personne chargée du maintien en conditions opérationnelles du système d'information du Ministère.

Responsable de salle : Personne chargée de la gestion des accès physiques aux salles informatiques hébergeant l'infrastructure et aux équipements.

5.2.3. Nombre de personnes requises par tâches

Les rôles liés à la gestion des systèmes sont distincts des rôles de gestion de l'application IGC, ainsi que des rôles intervenants sur les données enregistrées au niveau de l'application.

Ces différents rôles sont assurés par des personnes distinctes.

Par ailleurs, toute opération impliquant les secrets principaux de l'IGC nécessite l'intervention de trois personnes.

La DPC précise les opérations nécessitant l'intervention de plusieurs personnes ainsi que les contraintes que ces personnes doivent respecter.

5.2.4. Identification et authentification pour chaque rôle

Tout accès à l'application IGC est soumis à authentification forte, les droits d'accès étant définis en fonction des rôles. Notamment, toute personne susceptible d'intervenir auprès de l'application IGC, et ainsi de modifier des données ou des informations de configuration, doit être préalablement enregistré dans l'IGC et disposer d'un certificat d'authentification.

Pour les autres rôles en relation avec l'IGC, l'Autorité Administrative fait vérifier l'identité et les autorisations du personnel concerné avant :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux hébergeant la plate-forme de l'IGC ;
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans ces systèmes.

Ces contrôles sont décrits dans la DPC.

Chaque attribution de rôle dans l'IGC est notifiée par écrit.

5.2.5. 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, et dans le respect des règles de non-cumul définis dans la section 5.2.3. Les attributions associées à chaque rôle sont décrites dans la DPC de l'AC.

Les règles de non-cumul des rôles de confiance sont décrites au sein de la DPC.

5.3. Mesures de sécurité vis-à-vis du personnel

Au sein de la présente section ; le terme « personnel » désigne les détenteurs de rôles de confiance.

5.3.1. Qualifications, compétences et habilitations requises

Tous les personnels intervenant sur l'IGC sont soumis à un devoir de réserve.

Le responsable de l'application IGC s'assure que les attributions des personnels détenteurs de rôle de confiance correspondent à leurs compétences professionnelles et tient à jour la liste des personnels intervenants sur l'IGC.

Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'AC.

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

- de ses responsabilités relatives aux services de l'AC,
- des procédures liées à la sécurité du système et au contrôle du personnel,

par une lettre de mission signée par l'Autorité Administrative.

5.3.2. Procédures de vérification des antécédents

Le personnel amené à assurer un rôle de confiance vis-à-vis de l'AC a fait l'objet lors de son entrée en fonction, d'une vérification de ses antécédents par les services du Ministère.

Ces personnes ne doivent pas notamment avoir fait l'objet de condamnation incompatible avec leurs attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflits d'intérêts préjudiciables à l'impartialité de leurs tâches. En particulier, les porteurs de secrets permettant la reconstitution de la clé privée de l'AC ne doivent pas subir de pression hiérarchique les incitant à se dessaisir de leur secret.

5.3.3. Formation initiale

En préalable à leur entrée en fonction, les opérateurs d'enregistrement ainsi que le personnel des cellules informatiques sont formés aux concepts et objectifs de l'IGC IMAGE, ainsi qu'aux procédures à mettre en œuvre.

Les exploitants et administrateurs système sont formés aux concepts et objectifs de l'IGC IMAGE, ainsi

qu'aux logiciels, matériels et procédures d'exploitation applicables.

Les administrateurs centraux sont formés aux concepts et objectifs de l'IGC IMAGE, aux diverses procédures à mettre en œuvre au niveau de l'IGC, notamment en terme de gestion des secrets et de délégation des droits.

5.3.4. Formation continue

Avant toute évolution majeure de l'infrastructure de l'IGC ou des procédures, une étude d'impact est réalisée par l'AC, avec élaboration d'un plan de formation le cas échéant.

5.3.5. Fréquence et séquence de rotation entre différentes attributions

Aucune rotation programmée des attributions n'est prévue.

5.3.6. Sanctions en cas d'actions non autorisées

Sont applicables les actions disciplinaires s'il y a lieu.

5.3.7. Documentation fournie au personnel

Le personnel dispose de la documentation relative aux procédures opérationnelles ou organisationnelles et aux outils spécifiques qu'il met en œuvre.

5.4. Procédures de constitution des données d'audit

5.4.1. Types d'évènements enregistrés

5.4.1.1 Enregistrements sur papier ou bureautique

Sont enregistrés sur outil bureautique :

- Les actions de maintenance et de changements de configuration des systèmes de

l'infrastructure, suivant les procédures d'exploitation ;

- Les changements apportés au personnel détenteur de rôle de confiance ;
- Mises à jour de la présente PC, au sein du présent document.

5.4.1.2 Enregistrements électroniques par l'application IGC

Toute action sur un dossier d'administrateur ou d'UH est enregistrée, et un historique complet du dossier est conservé dans la base de données de l'AC.

De plus, les événements suivants font l'objet d'un enregistrement électronique de type log par l'application IGC :

- acceptation ou refus de connexion à l'application IGC ;
- demande de renouvellement de certificat, ainsi que l'éventuelle acceptation ou refus de la demande ;
- génération des certificats ;
- importation du certificat ou du fichier PKCS#12 en vue de sa remise au porteur/au RCSI ;
- demande de révocation ;
- révocation de certificat ;
- génération puis publication de la LCR ;
- requête et réponse concernant la validité d'un certificat (OCSP) ;
- modification des droits des personnels autorisés à intervenir auprès de l'application IGC;
- modification des paramètres de configuration de l'IGC.

5.4.1.3 Autres enregistrements électroniques

Les accès physiques aux locaux hébergeant l'infrastructure matérielle font l'objet d'un enregistrement électronique automatique.

Les événements suivants font l'objet d'un enregistrement électronique au niveau des systèmes

d'exploitation de la plate-forme hébergeant l'IGC, dès le démarrage de ceux-ci :

- 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 ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation ;
- modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des détenteurs des rôles de confiance, et les tentatives non réussies correspondantes.

5.4.1.4 Caractéristiques communes

Pour tous les types d'enregistrements présentés ci-dessus, chaque enregistrement d'événement contient au minimum les informations suivantes :

- type de l'évènement ;
- nom ou service de l'exécutant ou référence du système déclenchant l'évènement ;
- date et heure de l'évènement ;
- résultat de l'évènement (échec ou réussite).

La personne, le service ou le système ayant exécuté l'événement est responsable de sa journalisation.

Les opérations de journalisation électronique sont effectuées au cours du processus ou à la fin de celui-ci.

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

5.4.2.1 Enregistrements sur papier ou bureautique

Les journaux enregistrés sous forme bureautique sont éventuellement revus lors des différents audits.

5.4.2.2 Enregistrements électroniques par l'application IGC

Le contenu du journal électronique d'événements applicatifs de l'application IGC est surveillé lors de chaque audit interne afin de vérifier le fonctionnement normal de l'AC, et de mettre en évidence les tentatives d'intrusion au niveau de l'application.

5.4.2.3 Autres enregistrements électroniques

Les autres journaux enregistrés sous forme électronique sont éventuellement revus lors des opérations de corrélation avec les journaux de l'application IGC.

5.4.3. Période de conservation des journaux d'évènements sur site

5.4.3.1 Enregistrements bureautiques

Les enregistrements bureautiques sont conservés sur site et par leur dépositaire pendant 5 ans.

5.4.3.2 Enregistrements électroniques par l'application IGC

Les enregistrements des journaux sont conservés au sein de l'application IGC sans limitation de durée.

5.4.3.3 Autres enregistrements électroniques

Les autres journaux d'enregistrement sous forme électronique sont sauvegardés puis purgés chaque début de mois.

5.4.4. Protection des journaux d'évènements

5.4.4.1 Enregistrements bureautiques

Les journaux sous forme de documents bureautiques sont soumis à contrôle d'accès en écriture. Ces contrôles d'accès sont gérés par le rédacteur du document.

5.4.4.2 Enregistrements électroniques par l'application IGC

Les journaux d'événements conservés par l'application IGC sont protégés en intégrité.

Ils ne sont accessibles qu'en lecture et exclusivement pour les administrateurs centraux.

5.4.4.3 Autres enregistrements électroniques

Les droits en modification/suppression/écriture des journaux d'événements des systèmes d'exploitation sont réservés aux utilisateurs avec droits avancés (« compte administrateur »).

5.4.5. Procédure de sauvegarde des journaux d'évènements

5.4.5.1 Enregistrements bureautiques

Les enregistrements sous forme de documents bureautiques sont sauvegardés selon les procédures applicables à ce type de documents.

5.4.5.2 Enregistrements électroniques par l'application IGC

Les journaux d'événements de l'application IGC sont sauvegardés selon la procédure de sauvegarde des données de l'application IGC. Les journaux sauvegardés sont protégés en intégrité par le même mécanisme qu'au sein de l'application IGC.

5.4.5.3 Autres enregistrements électroniques

Les autres journaux sous forme électroniques sont sauvegardés par un système centralisé de sauvegardes.

5.4.6. Système de collecte des journaux d'évènements

Dans tous les cas, il n'est pas prévu de système de collecte des journaux d'événements.

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

Dans tous les cas, il n'est pas prévu de notification de l'enregistrement d'un événement à son responsable.

5.4.8. Evaluation des vulnérabilités

L'Autorité de Certification est en mesure de détecter toute tentative de violation de son intégrité ; les accès à l'application IGC étant soumis à authentification forte et journalisés.

Les anomalies liées à des tentatives d'accès en échec peuvent être consultées à tout moment par consultation des journaux d'évènements.

La mise en relation des différents journaux d'événements est réalisée en cas de détection de compromission ou de suspicion de tentative de compromission de l'application IGC.

5.5. Archivage des données

5.5.1. Types de données archivées

5.5.1.1 Données sous forme papier ou bureautique

Les données conservées sous forme papier et archivées par leur dépositaire sont :

- Les dossiers d'enregistrements des administrateurs et des UH. Ils sont remis par l'administrateur central ayant procédé à leur constitution à l'AC, qui prend en charge leur archivage.

Les données conservées sous forme de documents bureautiques et archivées sont :

- les journaux d'événements tels qu'identifiés dans la section ci-dessus, archivés selon la procédure d'archivage applicable à ce type de document. L'archivage est sous la responsabilité de leurs rédacteurs ;
- l'ensemble des documents référencés applicables à l'AC (i.e. la présente Politique de Certification, la DPC et ses annexes…). L'archivage est sous la responsabilité du responsable de l'application IGC.

5.5.1.2 Données de l'application IGC (sous forme électronique)

L'ensemble des données créées et/ou utilisées par l'application IGC est archivé, y compris les LCR.

5.5.1.3 Autres données sous forme électronique

Les logiciels et fichiers de configuration sont sauvegardés périodiquement mais non archivés.

Les journaux d'événements autres que ceux de l'application IGC et tels que définis dans la section précédente sont sauvegardés mais non archivés.

5.5.2. Période de conservation des archives

Dossiers d'enregistrement et certificats

Les dossiers électroniques d'enregistrement et les certificats attachés sont conservés par l'application IGC pendant toute la vie de l'IGC sans être purgés.

Les dossiers papier d'enregistrement sont conservés par l'AC sans limitation de durée.

Les dossiers d'enregistrements et les certificats attachés peuvent être présentés par l'AC lors de toute sollicitation par les autorités habilitées.

Ces dossiers permettent de retrouver l'identité des personnes physiques désignées dans les certificats émis par l'AC.

LCR émis par l'AC

Les LCR successives produites sont archivées sans limitation de durée par l'application IGC.
Journaux d'évènements

Les journaux d'événements de l'application IGC sont conservés par celle-ci sans limitation de durée. Leur intégrité est garantie par les mécanismes mis en œuvre lors de leur constitution.

Données sous forme papier et bureautique

Les données sont archivées durant au moins 5 ans ; hormis l'ensemble des documents référencés applicables à l'AC archivés sans limitation de durée.

5.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives :

- sont protégées en intégrité selon les mécanismes mis en œuvre lors de la constitution des données qu'elles contiennent ;
- sont accessibles uniquement aux personnes autorisées ;
- peuvent être relues et exploitées.

Les moyens mis en oeuvre pour archiver les pièces en toute sécurité sont indiqués dans la DPC.

5.5.4. Procédure de sauvegarde des archives

5.5.4.1 Données sous forme papier ou bureautique

Les archives des données sous forme papier ou bureautique ne sont pas sauvegardées.

5.5.4.2 Données de l'application IGC (sous forme électronique)

Les données de l'application IGC sont archivées par l'application IGC elle-même et font donc l'objet de sauvegardes régulières selon les modalités définies dans la section 5.4.5.

5.5.5. Datation des données

5.5.5.1 Données sous forme papier ou bureautique

La datation des données enregistrées est réalisée à partir d'une source de temps d'utilisation courante supposée correcte avec une précision inférieure à 5 minutes.

5.5.5.2 Données de l'application IGC (sous forme électronique)

La datation des données est réalisée selon les modalités définies au 6.10.

5.5.6. Système de collecte des archives

5.5.6.1 Données sous forme papier ou bureautique

Les archives des données sous forme papier ou bureautique ne sont pas collectées mais conservées par leur rédacteur ou dépositaire.

5.5.6.2 Données de l'application IGC (sous forme électronique)

Les données électroniques sont collectées et conservées en ligne dans la base de données de l'AC.

5.5.7. Procédures de récupération et de vérification des archives

Les modalités d'accès aux différentes archives papier, bureautique et électroniques sont définies au sein de la DPC.

5.5.7.1 Données sous forme papier ou bureautique

Les archives sous format papier et bureautique peuvent être récupérées dans un délai inférieur à deux jours ouvrés.

5.5.7.2 Données de l'application IGC (sous forme électronique)

Les archives électroniques sont disponibles en ligne via l'application IGC pour les personnes autorisées à y accéder.

5.6. Changement de clé d'AC

Le renouvellement du certificat d'AC et de sa bi-clé privée sera planifié de façon à ce que le certificat de l'AC soit valide au plus tard lors de la fin de validité de tous les certificats porteur et serveur qu'elle a émis et de façon à pouvoir émettre des certificats sans discontinuité.

La nouvelle bi-clé générée servira à signer les nouveaux certificats émis ainsi que la LCR relative à ces nouveaux certificats.

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

5.7. Reprise suite à compromission et sinistre

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

Le fonctionnement des systèmes composant l'IGC et leur environnement technique sont surveillés par les exploitants de l'IGC, qui traitent et remontent les incidents.

Les administrateurs centraux de l'AC mettent en œuvre des procédures et des moyens de remontée et de traitement des compromissions, notamment au travers de l'analyse des différents journaux d'évènements.

Les procédures de traitement des incidents et des compromissions font l'objet d'un Plan de Reprise d'Activité dédié.

En particulier, l'AC s'engage à prévenir dans les meilleurs délais les administrateurs et les tiers utilisateurs de certificat en utilisant tout moyen à sa convenance (messagerie, appel téléphonique, affichage, site Web, ...) en cas d'incident impactant durablement ses services.

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

L'IGC dispose d'un Plan de Reprise d'Activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'AC découlant de la présente PC et identifiées comme critiques.

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 de l'AC ou de l'une de ses composantes

Dans le cas de compromission de la clé de l'AC Horodatage, l'AC demandera la révocation de son certificat auprès de l'AC Racine ; ceci après avoir demandé le renouvellement de son certificat et

assuré la continuité de ses services critiques, conformément au Plan de Reprise d'Activité.

La compromission des clés des composantes techniques de l'IGC fait l'objet du document [PC-ACR].

5.7.4. Capacités de continuité d'activité suite à un sinistre

En cas d'incident sur le site nominal, l'exploitation de l'IGC est transférée sur le site de secours en moins de 24 heures

En particulier, en complément des sauvegardes sur site, les données créées par l'application IGC sont répliquées par le réseau interne sécurisé du Ministère à des intervalles réguliers sur le site de secours.

5.8. Fin de vie de l'IGC

Transfert d'activité ou cessation d'activité affectant l'AEL

La mise en œuvre des services de révocation, de mise à disposition des informations de révocation et d'archivage étant de la responsabilité de l'AC, le transfert ou la cessation d'activité d'administrateurs centraux est sans incidence sur ces fonctions et sur la validité des certificats émis antérieurement.

Cessation d'activité affectant l'AC

Dans l'hypothèse d'une cessation d'activité totale, l'AC s'engage à assurer la continuité des fonctions de révocation des certificats et la publication de la LCR, dans la limite de ses propres possibilités.

En particulier, lors de l'arrêt du service, l'AC :

1) s'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats ;
2) prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
3) demande la révocation de son certificat auprès des autorités ayant certifié sa clé ;
4) révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
5) informe tous les porteurs des certificats révoqués ou à révoquer.

6. MESURES DE SECURITE TECHNIQUES

6.1. Génération des bi-clés

6.1.1. Génération des bi-clés de l'Autorité

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé.

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique conforme aux exigences de l'annexe 2 du document [PRIS-PC].

La génération de la clé de signature de l'AC Horodatage est effectuée dans des circonstances contrôlées, par des personnels dans des rôles de confiance, dans le cadre de « Cérémonies de Clés ». Ces Cérémonies se déroulent suivant des scripts préalablement définis.

L'initialisation de l'IGC et/ou la génération des clés de signature d'AC s'accompagnent de la génération de parts de secrets. 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, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC.

Suite à 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. Un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets est mise en oeuvre par son porteur.

Les détails de la méthode utilisée pour la génération des parts de secrets sont fournis dans la [PC-ACR].

Les Cérémonies de Clés se déroulent sous le contrôle de deux témoins impartiaux et de confiance désignés par l'Autorité Administrative, qui attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

6.1.2. Génération des bi-clés des UH et des administrateurs

La génération de la bi-clé d'une UH est :

- effectuée par l'AC.

La génération de la bi-clé d'un administrateur est effectuée dans un dispositif d'authentification répondant aux exigences de l'annexe 3 du document [PRIS-PC].

6.1.3. Transmission de la clé privée à son propriétaire

Certificat UH : la clé privée est générée par l'AC, et transmise à l'UH par une opération technique interne.

Certificat administrateur : La carte IMAGE destinée à l'administrateur génère elle-même la bi-clé. La clé privée n'est donc jamais transmise.

6.1.4. Transmission de la clé publique d'un administrateur à l'AC

Lors de la transmission de la clé publique d'un administrateur vers l'AC, la clé est protégée en intégrité et son origine est authentifiée.

6.1.5. Transmission de la clé publique de l'AC aux tiers utilisateurs de certificats et aux administrateurs

La clé publique de l'AC est diffusée dans son certificat, signé par l'AC Racine.

6.1.6. Tailles des clés

Les clés d'AC sont des clés RSA de 2048 bits. Les clés des administrateurs et des UH sont des clés RSA de 2048 bits.

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

Les équipements de génération de bi-clés, cartes IMAGE pour les administrateurs et boîtiers cryptographiques pour l'Autorité et les UH, utilisent des paramètres respectant les normes de sécurité

propres à l'algorithme correspondant à la bi-clé.

6.1.8. Objectifs d'usage de la clé

L'utilisation de la clé privée de l'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR, et des réponses OCSP.

L'utilisation de la clé privée d'une UH et du certificat associé est strictement limitée aux services indiqués dans la présente Politique.

L'utilisation de la clé privée d'un administrateur et du certificat associé est strictement limitée aux services d'authentification tels que décrits dans la présente PC.

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

6.2.1. Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC pour la génération et la mise en œuvre de ses clés de signature, répondent au minimum aux exigences de l'annexe 2 du document [PRIS-PC]. Les cartes cryptographiques utilisées ont été évaluées selon les Critères Communs au niveau EAL4+.

Ni les clés privées d'AC, ni les clés privées des UH, ni les clés privées des administrateurs ne sont séquestrées ni archivées. Les clés privées des UH ou des administrateurs ne font l'objet d'aucune copie de secours par l'AC et d'aucune archive.

6.2.2. Dispositifs d'authentification des administrateurs (cartes IMAGE)

Les cartes IMAGE des administrateurs, pour la mise en œuvre des clés privées d'authentification, respectent les exigences de l'annexe 3 du document [PRIS-PC].

L'AC fournit ce dispositif au porteur via l'AEL.

L'activation de la clé privée du porteur est contrôlée via un code d'activation (code PIN) et permet de

répondre aux exigences de l'annexe 3 du document [PRIS-PC].

La clé privée d'un administrateur est désactivée dès que la carte IMAGE est déconnectée.

6.3. Autres aspects de la gestion des bi-clés

6.3.1. Archivage des clés publiques

Les clés publiques de l'AC, des UH et des administrateurs sont archivées dans le cadre de l'archivage des certificats correspondants.

6.3.2. Durées de vie des bi-clés et des certificats

Les bi-clés des UH ont une validité de 18 mois, et les certificats associés couverts par la présente PC ont une durée de validité de sept ans.

Les bi-clés et certificats des administrateurs couverts par la présente PC ont une durée de validité de trois ans.

La durée de validité des clés d'authentification d'AC et des certificats correspondants est de 18 ans, mais ces derniers sont renouvelés après une période de 11 ans maximum, afin que le certificat d'AC couvre toute la période de validité des certificats que celle-ci émet.

6.4. Données d'activation des clés d'AC

6.4.1. Génération et installation des données d'activation

La génération et l'installation des données d'activation des modules cryptographiques de l'IGC se font lors de la phase d'initialisation et de personnalisation de ce module, pendant la Cérémonie des Clés. Les données d'activation sont choisies et saisies par les porteurs de secret responsables de ces données.

6.4.2. Protection des données d'activation

Les données d'activation ne sont connues que par les porteurs de secret nommément identifiés dans le cadre des rôles qui leurs sont attribués.

Elles sont scellées et conservées en coffre-fort par les responsables de ces données eux-mêmes, de manière à les protéger en intégrité et en confidentialité.

6.5. Données d'activation des clés privées des UH

Les clés privées sont transmises à l'UH et activées par une opération technique interne.

6.6. Données d'activation des cartes IMAGE

Les administrateurs sont invités à choisir un code d'activation (PIN) qu'ils puissent mémoriser, mais non trivial.

6.7. Mesures de sécurité des systèmes informatiques

Les mesures de sécurité mises en place au niveau des systèmes informatiques couvrent les objectifs de sécurité suivants :

- identification et authentification forte des détenteurs de rôles de confiance pour l'accès à la plate-forme de l'IGC,
- identification et authentification forte des administrateurs centraux pour l'accès à l'application IGC,
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels,
- gestion des comptes des administrateurs centraux au niveau de l'application IGC,
- gestion des comptes des détenteurs de rôles de confiance au niveau des systèmes de la plate-forme de l'IGC,
- 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 transitent

entre les composantes de l'IGC,

- fonctions d'audits (non-répudiation et nature des actions effectuées),
- gestion des incidents,
- protection en confidentialité, en intégrité et en disponibilité des clés nécessaires au fonctionnement de l'AC.

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.

6.8. Mesures de sécurité des systèmes durant leur cycle de vie

6.8.1. Mesures de sécurité liées au développement des systèmes

La configuration des systèmes de la plate-forme d'IGC (systèmes d'exploitation, application IGC…), ainsi que toute modification et mise à niveau, sont documentées et contrôlées.

6.8.2. Mesures liées à la gestion de la sécurité

L'Autorité Qualifiée est tenue informée de toute évolution majeure sur les systèmes de la plate-forme d'IGC.

Celle-ci est documentée et apparaît dans les procédures d'exploitation de l'AC.

6.9. Mesures de sécurité réseau

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

De plus, les échanges au sein de l'application IGC mettent en œuvre systématiquement des services d'intégrité et de confidentialité.

6.10.Système de datation

La datation des évènements enregistrés par les différentes fonctions de l'AC dans les journaux est basée sur l'heure système de la plate-forme hébergeant l'AC, après synchronisation par rapport à une source fiable de temps UTC, au minimum à la seconde près.

7. PROFILS DES CERTIFICATS, DE LA LCR ET DES REPONSES OCSP

Les profils des certificats d'authentification émis par l'AC Horodatage, ainsi que les profils de la LCR et des réponses OCSP correspondantes figurent dans un document séparé intitulé :

« Profils relatifs à la PC Horodatage ».

Ce document est référencé selon l'OID de la présente PC et fait partie intégrante du présent document. Toute modification majeure de ce document entraîne une évolution de l'OID de la présente PC, et vice-versa.

8. AUDITS INTERNES ET DE CONFORMITE

L'Autorité Administrative de l'AC Horodatage fait contrôler la conformité de son service de certification pour le profil « Certificat horodatage » proposé par son AC avec les exigences du document [PRIS-PC] selon le niveau de sécurité « fort – (niveau **) ».

Les audits internes ont notamment pour but de vérifier que l'AC respecte ce qui est écrit dans la présente PC et dans la DPC associée.

Les audits de conformité, ou audits « externes », ont notamment pour but de vérifier la conformité des points relatifs au service de certification pour le profil « Horodatage » de la PC et de la DPC vis-à-vis des exigences du document [PRIS-PC] au même niveau. Pour ces audits externes :

- La reconnaissance du respect par l'AC pour ce service des exigences du document [PRIS-PC] est effectuée par un organisme de qualification de services de confiance choisi parmi les organismes accrédités par le COFRAC selon la norme EN NF 45012 (ou ISO 17021) et le programme CEPE REF 21 (Exigences spécifiques pour la qualification des prestataires de services de confiance).
- Les résultats de l'audit de conformité sont communiqués par l'auditeur à l'Autorité Administrative de l'AC. Suite au résultat de l'audit de conformité, l'auditeur rend un avis à l'Autorité Administrative. Suivant les résultats, celle-ci met éventuellement en place des actions correctives et peut demander ensuite un nouvel audit de conformité auprès de l'auditeur.
- En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC devra :
    - 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 de ses différentes composantes.
    - au plus tard un mois après la fin de l'opération, en informer l'organisme accrédité.

La suite du présent chapitre ne concerne que les audits et évaluation *internes* de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son AC.

8.1. Fréquences et / ou circonstances des évaluations

Suite à la première mise en service de l'application IGC ou suite à toute modification significative de celle-ci ou des procédures fonctionnelles applicables, l'Autorité Administrative de l'AC fait procéder à un audit interne global ou limité au périmètre de l'impact de la modification.

L'Autorité Administrative de l'AC fait aussi procéder régulièrement à un audit interne de l'ensemble de son AC, une fois tous les deux ans.

8.2. Identités / qualifications des évaluateurs

Le contrôle d'un périmètre particulier de l'IGC (procédure, application, fonction, rôle) est assigné par l'Autorité Administrative de l'AC à une équipe d'auditeurs, compétents en sécurité des systèmes d'information et dans le domaine couvert par le périmètre à auditer.

8.3. Relations entre évaluateurs et entités évaluées

L'auditeur ne doit pas posséder de rôle de confiance auprès de l'AC, autre que le présent rôle et doit être dûment autorisé à pratiquer les contrôles visés.

8.4. Sujets couverts par les évaluations

Les audit internes portent sur un rôle, une procédure, une fonction de l'AC ou sur l'application IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'AC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la présente PC et dans la DPC associée, ainsi que des éléments qui en découlent (procédures opérationnelles, ressources déployées, etc.).

8.5. Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle, l'auditeur rend à l'Autorité Administrative, 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'auditeur émet des recommandations à l'Autorité Administrative de l'AC pouvant être la cessation (temporaire ou définitive) d'activité, la suppression du rôle de confiance, la modification de la procédure, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'Autorité Administrative de l'AC et doit respecter ses politiques de sécurité internes, pour les références de ces politiques voir le document interne [DPC-AD].
- en cas de résultat « A confirmer », l'auditeur remet à l'Autorité Administrative de l'AC un avis précisant sous quel délai les non-conformités doivent être réparées. Puis, un contrôle de « confirmation» permettra de vérifier que tous les points critiques ont bien été résolus.
- en cas de réussite, l'auditeur confirme à l'Autorité Administrative de l'AC la conformité aux exigences de la PC et la DPC.

En cas d'échec ou de résultat « à confirmer », l'Autorité Administrative informe, selon un moyen à sa convenance, les tiers utilisateurs de ce résultat.

8.6. Communication des résultats

Les résultats des audits internes sont tenus à la disposition de l'organisme de qualification de services de confiance accrédité.

9. AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1. Tarifs

Sans objet.

9.2. Responsabilité financière

Sans objet.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations et données à caractère confidentiel sont listées et classifiées au sein de la DPC. La DPC détaille les mesures de sécurité applicables à chaque niveau de sécurité identifié.

9.3.2. Responsabilités en terme de protection des informations confidentielles

La présente PC ne formule pas d'exigences supplémentaires autres que celles prévues par la législation et la réglementation en vigueur sur le territoire français relatives à la protection des informations confidentielles.

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

Toute collecte et tout usage de données à caractère personnel par l'AC et les rôles de confiance de l'AC sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier la 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.

En particulier, l'AC en tant qu'infrastructure de stockage et de gestion de données nominatives contenues dans les certificats électroniques, est déclarée et soumise à l'avis de la CNIL selon les termes de la Loi n° 78-17 du 6 janvier 1978 « informatique et les libertés ».

Le récépissé de cette déclaration porte le numéro : 1245693.

9.4.2. Informations à caractère personnel

Les informations considérées comme personnelles sont les suivantes :

- les causes de révocation des certificats des administrateurs ou des UH ;
- les dossiers d'enregistrement des administrateurs.

9.4.3. Informations à caractère non personnel

Les informations considérées comme non personnelles sont au moins les suivantes :

- Les identifiants techniques des UH et contenus dans les certificats,
- Les dossiers d'enregistrement des UH,
- Les adresses de messagerie professionnelles des administrateurs.

9.4.4. Responsabilité en terme de protection des données personnelles

La présente PC ne formule pas d'exigences supplémentaires autres que celles prévues par la législation et la réglementation en vigueur sur le territoire français relatives à la protection des données personnelles.

9.4.5. Notification et consentement d'utilisation des données personnelles

La présente PC ne formule pas d'exigence particulière sur ce point.

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

La communication aux autorités judiciaires des données personnelles sera effectuée en cas de demande de leur part.

9.4.7. Autres circonstances de divulgation d'informations personnelles

Le dossier d'enregistrement du porteur peut faire l'objet d'une divulgation auprès de la hiérarchie du porteur ou du service du personnel dont dépend le porteur.

9.5. Droits sur la propriété intellectuelle et industrielle

La présente PC ne formule pas d'exigences supplémentaires autres que celles prévues par la législation et la réglementation en vigueur sur le territoire français.

9.6. Interprétations contractuelles et garanties

Les obligations communes aux rôles de confiance de l'AC sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques et privées) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la présente PC et les documents applicables,
- respecter et appliquer la partie de la DPC leur incombant (cette partie étant communiquée aux rôles de confiance correspondants),
- se soumettre aux contrôles de conformité effectués par l'auditeur mandaté par l'AC et l'organisme de qualification accrédité,
- 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. Obligations applicables à l'Autorité de Certification

L'AC s'oblige à :

- garantir aux tiers utilisateurs de certificats qu'elle a émis un certificat pour une UH donnée et que l'administrateur en charge de cette UH a accepté le certificat, conformément aux exigences de la présente PC,
- garantir aux tiers utilisateurs de certificats qu'elle a émis un certificat pour un administrateur donné et que cet administrateur a accepté le certificat, conformément aux exigences de la présente PC.
- garantir et maintenir la cohérence de sa DPC avec la présente PC.
- prendre les mesures raisonnables pour s'assurer que les administrateurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion de leurs clés privées et des certificats.
- prendre les mesures raisonnables pour mettre à disposition des tiers utilisateurs les informations relatives à leurs droits et obligations en ce qui concerne l'utilisation des certificats UH et administrateurs.
- prendre les mesures raisonnables pour s'assurer que les détenteurs de rôle de confiance auprès de l'AC ont connaissance de leurs droits et obligations conférés de par l'attribution de ce rôle.

L'AC est responsable de la conformité des exigences et dispositions de la présente PC relatives aux certificats UH, avec les exigences définies dans le document [PRIS-PC] pour le niveau de sécurité « fort ».

L'AC assume toute conséquence dommageable résultant du non-respect de la présente PC par elle-même ou l'un de ses rôles de confiance.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou d'une personne assurant un rôle de confiance auprès de l'AC, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des administrateurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les

applications de gestion des certificats de l'AC.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même.

9.6.2. Obligations applicables aux administrateurs centraux

Les administrateurs centraux ont notamment pour obligation :

- d'assurer leur rôle dans le respect de la présente PC, et notamment d'assurer les fonctions dévolues à l'AEL telles que précisées dans la présente PC,
- de contrôler et vérifier l'identité des futurs administrateurs,
- de conserver les dossiers d'enregistrement des administrateurs et des UH.

9.6.3. Obligations applicables aux administrateurs

Les administrateurs ont le devoir de respecter les exigences décrites dans la présente PC.

Ils s'engagent notamment :

- à ne demander que des certificats portant sur des UH détenues par le Ministère,
- à signaler à l'AEL tout changement d'administrateur pour chaque certificat dont ils sont responsables,
- à respecter les usages des certificats émis,
- à demander dans les plus brefs délais la révocation des certificats dont ils sont responsables en cas de suspicion de compromission des clés privées associées.

9.6.4. Obligations applicables aux tiers utilisateurs de certificats

Les tiers utilisateurs de certificats d'UH et d'administrateur doivent :

- vérifier et respecter les conditions d'utilisation pour lesquelles un certificat a été émis et décrites dans la présente PC,

- Contrôler la validité du certificat de l'AC Horodatage :
  - par contrôle de la signature par l'AC Racine du Ministère en charge des affaires sanitaires et sociales ;
  - par contrôle des dates de validité ;
  - par contrôle de l'absence de révocation, d'après la dernière Liste de Révocation de Certificats en cours de validité émis par l'AC Racine ;
- Contrôler la validité de chaque certificat :
  - par contrôle de la signature par l'AC Horodatage ;
  - par contrôle des dates de validité ;
  - par contrôle de l'absence de révocation, d'après la dernière Liste de Révocation de Certificats en cours de validité émis par l'AC Horodatage.
- vérifier et respecter les obligations des tiers utilisateurs de certificats exprimées dans la présente PC,
- contrôler que le certificat émis par l'AC Horodatage est référencé au niveau de sécurité requis par l'application.

9.7. Limite de responsabilité

L'objectif de l'AC est d'émettre des certificats qui soient acceptés par le système d'information du Ministère, par ses applications, et par les applications d'autres ministères ou d'autres partenaires, auxquelles le personnel du Ministère pourrait être amené à accéder.

L'AC est responsable en cas de négligence ou de faute intentionnelle des préjudices causés à une personne physique ou morale qui s'est fiée raisonnablement à ses certificats. La responsabilité de l'AC pourra être mise en jeu si une personne assurant un rôle de confiance auprès de l'AC a commis une erreur accidentelle ou volontaire, ou bien une négligence.

L'AC ne pourra pas être tenue pour responsable d'un fait dommageable qui relèverait de sa compétence en cas de 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.

9.8. Indemnités

Les indemnités sont à l'appréciation des tribunaux compétents.

9.9. Durée et fin anticipée de validité de la PC

9.9.1. Durée de validité et fin de validité de la présente PC

La présente PC est valide jusqu'à :

- L'émission d'une mise à jour majeure du présent document, avec évolution du numéro de version,
- L'information publique de la part de l'Autorité Administrative, de l'invalidité de la présente PC. Dans ce cas, les certificats publiés selon la présente PC seront également révoqués.

9.9.2. Effets de la fin de validité et clauses restant applicables

Les traces d'audit enregistrées avant la fin de validité de la PC restent valables.

9.10. Amendements à la PC

9.10.1. Procédures d'amendements

Avant chaque évolution envisagée de la présente PC, l'Autorité Administrative contrôlera que son projet de modification est conforme aux exigences du document [PRIS-PC] pour le niveau « fort » pour les exigences et dispositions relatives aux certificats UH. En cas de changement important, l'AC s'engage à faire appel à un auditeur pour en contrôler l'impact.

9.10.2. Mécanisme et période d'information sur les amendements

Le cas échéant, les administrateurs seront avertis des amendements au moyen de leur adresse de messagerie et/ou sur l'Intranet du Ministère.

Les tiers utilisateurs de certificat peuvent prendre connaissance des amendements au moyen des sites web de publication.

9.10.3. Circonstances selon lesquelles l'OID doit être changé

L'OID de la présent PC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) ou du document décrivant les profils associés (cf. 7 Profils des certificats, de la LCR et des réponses OCSP) se traduira par une évolution de l'OID. Ainsi, les porteurs et tiers utilisateurs de certificat pourront clairement identifier les exigences que respecte un certificat déjà émis.

9.11. Dispositions concernant la résolution de conflits

A défaut d'une résolution à l'amiable, les conflits sont résolus par les tribunaux compétents.

9.12. Juridictions compétentes

En cas de litige, ces derniers seront soumis à l'appréciation des tribunaux compétents.

9.13. Conformité aux législations et réglementations

L'AC s'engage à respecter les textes de lois et décrets d'application relatifs aux moyens de cryptologie, selon l'article 28 de la loi n°90-1170 du 29 décembre 1990 (Loi de Réforme des Télécommunications).