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 : **88** VERSION : 2.0 REFERENCE : IMAGE-IGC-PC06 STATUT : Validé
Projet :	**IMAGE**
Titre :	**POLITIQUE DE CERTIFICATION** **AC PERSONNES : CHIFFREMENT** **OID : 1.2.250.1.179.1.2.1.3.1**

SOMMAIRE

Historique des versions

Version	Date	Modification
0.1	26/11/2009	Première version publiée
2.0	30/04/2014	Création DSI

Références documentaires

Référence	Titre
[PC-Profils]	IMAGE : Profils de certificats AC Personnes Chiffrement
[PC-Personnes-Authentification]	IMAGE : Politique de Certification de l'AC Personnes relative aux certificats d'authentification
[PC-Personnes - Signature].	IMAGE : Politique de Certification de l'AC Personnes relative aux certificats de signature
[Charte-Confidentialité]	« Charte d'Utilisation de la Confidentialité »
[PRIS-PC]	Politique de Référencement Intersectorielle de Sécurité Version 2.1 Service de Confidentialité 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 de

	Confidentialité - Politiques de Certification Types - Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques - Version 2.1".
[DPC]	IMAGE : Déclaration des Pratiques de Certification - AC Déléguées
[PC-ACR]	IMAGE : Politique de Certification - AC Racine

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.

Le projet IMAGE 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 ».

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).

L'ensemble du personnel du Ministère est muni d'une carte à puce IMAGE qui contient un certificat d'authentification permettant d'accéder au poste de travail et un certificat de signature. Cette fourniture de cartes IMAGE se déroule en conformité avec les Politiques de Certification [PC-Personnes-Authentification] et [PC-Personnes-Signature].

Présentation de la Politique de Certification AC Personnes Chiffrement :

Le présent document fait partie d'un ensemble de documents décrivant les politiques de certification

utilisées dans le cadre du projet IMAGE.

Chaque document s'applique à un type de certificat émis par une autorité de certification, 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 Personnes », ci-après dénommée « l'AC », et au type de certificat Chiffrement. Il spécifie les exigences concernant la politique mise en œuvre par l'AC Personnes délivrant des certificats de chiffrement et les clés privées associées stockés sur une carte IMAGE.

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). La politique est définie indépendamment des détails de l'environnement utilisé pour la mise en œuvre de l'infrastructure de gestion de clés (IGC) à laquelle elle s'applique.

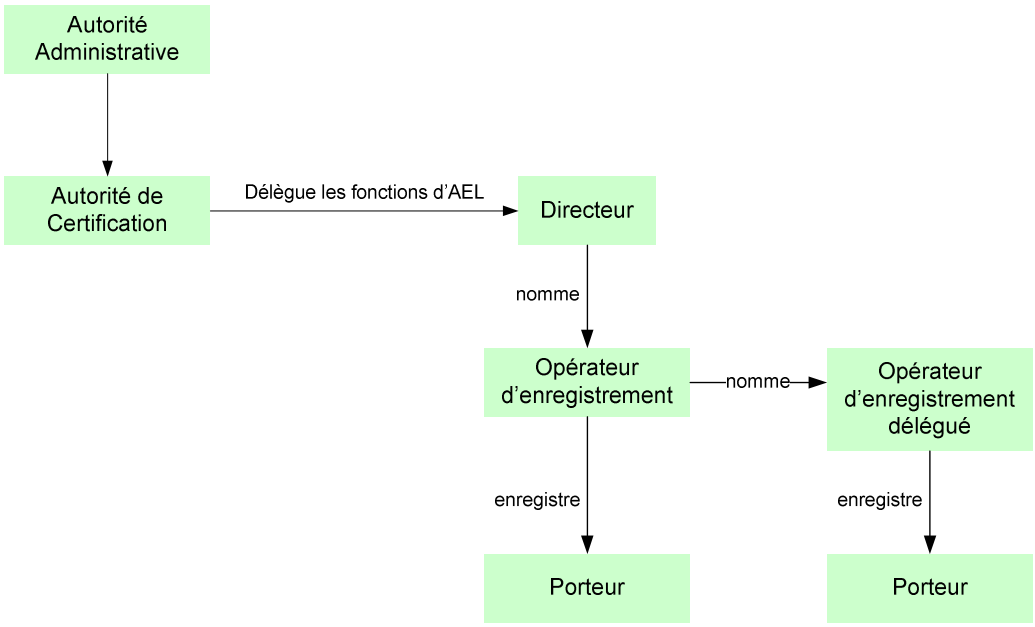
Les porteurs et les tiers utilisateurs de certificat ont des obligations spécifiques qui sont définies dans cette politique de certification.

1.2. Identification du document

La présente PC dans sa version 1 est identifiée par l'OID : **1.2.250.1.179.1.2.1.3.1**

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

1.3. Entités intervenant dans l'IGC



Le schéma ci-dessous ne constitue qu'une illustration synthétique des délégations de certains rôles de confiance auprès de l'IGC.

1.3.1. 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 porteurs 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 remise au porteur, 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 terme 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 porteurs et aux tiers utilisateurs de certificat.

1.3.2. 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 séquestre : Cette fonction conserve d'une manière sécurisée les clés privées de chiffrement des porteurs, de manière à permettre ces mêmes clés d'être recouvrées en cas de besoin.

Fonction de publication : Cette fonction met à disposition des différentes parties concernées les différents documents établis par l'AC (Conditions d'Utilisation,

Politiques et Pratiques…), les certificats d'AC et toute autre information pertinente destinée aux porteurs et aux utilisateurs de certificat, 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 œuvre 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.

1.3.3. Autorité d'Enregistrement Locale

Le rôle d'AEL est assuré par les différents Directeurs du Ministère.

L'AEL assure les fonctions d'enregistrement des porteurs, de remise des cartes IMAGE aux porteurs, et de gestion des cartes IMAGE.

Ces fonctions sont décrites dans le document [PC-Personnes-Authentification].

Dans le cadre de la présente PC, le rôle spécifique de l'AEL est :

Identification des personnes concernées par la confidentialité L'AEL définit le périmètre de la confidentialité et identifie les personnes concernées

Fonction de demande de certificat de chiffrement L'AEL effectue la demande de certificat de chiffrement pour les personnes concernées par la confidentialité.

Fonction de recouvrement : L'AEL traite les besoins de recouvrement de clés privées des porteurs, et réalise le recouvrement.

Fonction de gestion des révocations : L'AEL enregistre dans certains cas les demandes de révocation pour transmission et traitement par l'AC.

Sur le plan opérationnel, ces fonctions sont déléguées à la cellule informatique de la direction. Dans ce cas les membres de la cellule agissent comme opérateurs d'enregistrement.

Dans le présent document le terme «opérateur d'enregistrement» est utilisé pour désigner les personnes de la cellule informatique qui remplissent le rôle d'opérateur d'enregistrement pour les demandes de certificat de chiffrement, et qui administrent la confidentialité sur le plan technique. Ils assurent également la fonction de recouvrement.

L'AEL assure notamment à ce titre les tâches suivantes :

- la vérification de l'identité du porteur ;
- l'enregistrement de la demande de certificat de chiffrement dans l'IGC ;
- la gestion des certificats de chiffrement en cas de départs et mutations ;
- le recouvrement de clés privées de chiffrement en cas de besoin.

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

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

1.3.4. Porteur

La présente PC ne concerne que des personnes qui sont déjà porteur de carte IMAGE, et qui ont été identifiés nominativement par leur direction d'appartenance (AEL) comme des personnes ayant besoin d'accéder à des documents sensibles. Seules ces personnes concernées par la confidentialité peuvent obtenir un certificat de chiffrement IMAGE.

Le porteur utilise sa clé privée et le certificat correspondant dans le cadre de ses activités professionnelles.

Le porteur concerné peut être :

1. un agent du Ministère,

2. une personne externe n'appartenant pas au personnel du Ministère, mais hébergée sur un site du Ministère.

Les certificats de chiffrement ne sont pas attribués à des personnes externes au Ministère qui ne travaillent pas sur le site du Ministère.

1.3.5. Utilisateurs des certificats

Les utilisateurs des certificats sont les mêmes porteurs concernés par la confidentialité du paragraphe précédent. Cette utilisation s'effectue par le biais du logiciel de chiffrement mis en œuvre au Ministère.

Dans la suite du document, le terme « utilisateur » s'applique à la personne qui accède aux données chiffrées (en général, le détenteur du poste).

1.4. Usage des certificats

1.4.1. Bi-clés et certificats porteurs

La présente PC traite des bi-clés et des certificats à destination des porteurs concernés par la confidentialité identifiés dans le paragraphe 1.3.4, afin que ces porteurs puissent chiffrer ou déchiffrer des données dans le cadre du service de confidentialité du Ministère.

L'utilisation de la clé privée du porteur et du certificat associé doit rester strictement limitée au service de confidentialité.

Les bi-clés et les certificats de chiffrement sont utilisés par le logiciel de chiffrement mis en place par le Ministère. Les données sont chiffrées par une clé secrète gérée par ce logiciel. L'accès à cette clé est protégé par un mécanisme cryptographique asymétrique, de type RSA, avec chiffrement par la clé publique du porteur, et déchiffrement par sa clé privée.

Les certificats et les clés privées sont utilisés pour le :

- chiffrement des données locales contenues sur les postes de travail pour la protection renforcée contre l'accès en cas de vol matériel (portable, disque dur,..), ou l'accès par des personnes n'ayant pas besoin d'en connaître,

- chiffrement des données partagées contenues dans les serveurs de fichiers pour la protection renforcée des données qui transitent sur les réseaux locaux et contre l'accès de personnes n'ayant pas besoin d'en connaître,

L'AC décline toute responsabilité en ce qui concerne l'utilisation des certificats de chiffrement pour des usages autres que ceux qui sont définis dans la présente PC et dans le document [Charte-Confidentialité].

1.4.2. Bi-clés et certificats de l'AC Personnes 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 d'authentification et de chiffrement des données échangées ou stockées au sein de l'IGC, etc.

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

1.5. Gestion de la PC

1.5.1. Entité gérant la Politique de Certification

L'AC est responsable de l'établissement de la présente Politique de Certification en conformité avec le document [PRIS-PC], de son application et de sa diffusion.

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

1.5.2. 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

1.5.3. 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 ou d'un audit de conformité de la PC.

1.5.4. Procédure d'approbation de la DPC

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

1.5.5. Niveau de conformité

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

1.6. Définitions et abréviations

1.6.1. 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) : Personne chargée de l'application de la présente Politique de Certification

Autorité de Certification Racine : Autorité de Certification auto-signée, point de confiance de l'IGC, et certifiant les Autorités de Certification Déléguées, dont l'AC Personnes.

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.

Certificat [électronique] : Certificat délivré à une personne physique et portant sur une bi-clé d'authentification, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

Cellules informatiques : Service fournissant des services de soutien technique de niveau 1 aux porteurs. Il s'agit, selon le cas, de soutien informatique, bureautique, ou réseau.

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 privées et certificats.

Code d'activation : (ou PIN) Nombre choisi par le porteur de la carte IMAGE et permettant l'usage de la clé privée associée au certificat d'authentification.

Code PIN : Voir « Code d'activation »

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.

Conditions d'Utilisation des certificats et cartes IMAGE : Document reprenant les informations pertinentes de la présente PC (conditions d'usages des certificats et des cartes IMAGE, obligations et responsabilités, etc) et décliné suivant les catégories de porteurs auxquelles il s'adresse.

Conditions d'Utilisation des certificats et cartes IMAGE applicables aux tiers utilisateurs : Document reprenant les informations pertinentes de la présente PC (conditions d'utilisation des certificats, obligations et responsabilités des différentes parties, garanties et limites de garanties de l'AC, etc.) à destination des tiers utilisateurs de certificat.

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.

Guichet Unique des Services (GUS) : Centre d'appels qui assure le support informatique de niveau 2, disponible 24h/24 et 7j/7, et répondant par téléphone aux appels des cellules informatiques et, cas particulier, à des porteurs référencés.

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

Infrastructure de Gestion de Clés (IGC) : Ensemble de composantes, fonctions et procédures dédiées 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.

Opérateur d'enregistrement : Personne ayant délégation de fonctions de l'Autorité d'Enregistrement Locale.

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.

Porteur : Personne physique identifiée dans un certificat et détentrice de la clé privée correspondant à la clé publique présente dans ce certificat, et détentrice d'une carte IMAGE.

Réponse OCSP : Réponse par l'AC à une interrogation par un tiers utilisateur indiquant l'état révoqué ou non d'un certificat 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 de maintenir en opération, une ou plusieurs de ses fonctions.

Tiers utilisateur : Utilisateur d'un certificat de porteur et qui fait confiance à ce certificat (maîtrise d'ouvrage d'application).

Format X.509 v3 : Format standard de certificat électronique

1.6.2. Abréviations

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

AA	Autorité Administrative
AC	Autorité de Certification
AEL	Autorité d'Enregistrement Locale
BIMS	Annuaire Bureautique Infrastructure Messagerie Stockage
CN	*Common Name* ; Nom commun
CU	Conditions d'Utilisation
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 »)

GUS Guichet Unique des Services

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 Electronique et de la confidentialité

LCR Liste des Certificats Révoqués

LDAP *Light Directory Access Protocol* ; protocole d'interrogation et de modification de contenu d'annuaire

OCSP *Online Certificate Status Protocol* ; protocole en-ligne de vérification de statut de certificat

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.

USB *Universal Serial Bus* ; bus série universel

UTC *Universal Time Coordinated* ; temps universel coordonné

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 porteurs et des tiers 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 tiers utilisateurs de certificat et des porteurs :

- les politiques de certification en cours de validité,
- les profils des certificats, de la LCR et des réponses OCSP,
- les différents documents « Conditions d'Utilisation des certificats et des cartes IMAGE »
- 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

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

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'IGC/A (*).

(*) Les adresses où ces informations sont disponibles sont indiquées dans les différents documents « Conditions d'Utilisation des certificats et des cartes IMAGE ».

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 « Authority Information Access » 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 4.10.
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

Les demandes de certificat de chiffrement sont réalisées à partir de l'enregistrement du porteur effectué lors de l'établissement de la carte IMAGE. La possession de la carte IMAGE est un pré-requis pour obtenir un certificat de chiffrement.

3.1.1. Types de noms

Les noms qui désignent les porteurs de certificats de chiffrement sont ceux enregistrés lors de l'établissement de la carte IMAGE, voir le document [PC-Personnes-Authentification].

3.1.2. Utilisation de noms explicites

Voir le document [PC-Personnes-Authentification].

3.1.3. Unicité des noms

Voir le document [PC-Personnes-Authentification].

3.1.4. Identifiants attribués aux personnes internes et aux personnes externes sur site

Voir le document [PC-Personnes-Authentification].

3.1.5. Identifiant attribué aux personnes externes hors site

Les certificats de chiffrement ne sont pas attribués à des personnes externes au Ministère ne travaillant pas sur le site du Ministère.

3.2. Validation initiale de l'identité

L'enregistrement des porteurs s'effectue dans le cadre de l'émission de la carte IMAGE, voir le document [PC-Personnes-Authentification].

3.2.1. Méthode pour prouver la possession de la clé privée

La bi-clé est générée en central dans l'IGC dans le module de sécurité matériel HSM.

Elle est importée dans la carte IMAGE par une procédure automatique, lors du retrait du certificat de chiffrement par le porteur.

3.2.2. Validation de l'identité d'un porteur

Voir le document [PC-Personnes-Authentification].

3.2.3. Validation des autres identifiants attribués aux personnes internes et aux « externes sur site »

Voir le document [PC-Personnes-Authentification].

3.2.4. Validation des autres identifiants attribués aux personnes externes hors site

Les certificats de chiffrement ne sont pas attribués à des personnes externes au Ministère ne travaillant pas sur le site du Ministère.

3.2.5. Informations non vérifiées du porteur

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

3.3. Identification et validation pour le renouvellement des clés

Le renouvellement de la bi-clé d'un porteur 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

Le renouvellement de certificats est effectué par l'opérateur après confirmation du besoin par l'AEL. Le porteur s'identifie en présentant sa pièce d'identité.

3.3.2. Identification et validation pour un renouvellement après révocation

La procédure d'identification et de validation du renouvellement est identique à la précédente.

3.4. Identification et validation pour une révocation

La demande de révocation se fait via un service en ligne (serveur web). Ce service est protégé par un dispositif de protection contre les attaques par robot sur des pages accessibles par Internet, connu sous l'acronyme CAPTCHA ("*Completely Automated Public Turing text to Tell Computers and Humans Apart"*).

Le porteur est alors identifié par son adresse de messagerie telle qu'enregistrée par l'opérateur d'enregistrement lors de l'enregistrement. Son authentification est basée sur la série de trois questions / réponses portant sur des informations propres au porteur, et dont les réponses ne peuvent réellement être connues que du porteur (ces questions/ réponses ont été choisies par le porteur lors de l'enregistrement).

3.5. Identification et validation d'une demande de carte IMAGE supplémentaire

Une carte IMAGE supplémentaire est fournie aux porteurs pour lesquels les accès au système

informatique hors heures ouvrées pourraient être critiques et aux porteurs disposant de deux micro-ordinateurs.

La procédure d'établissement de la carte supplémentaire est décrite dans le document [PC-Personnes-Authentification].

Lorsque le porteur d'une carte supplémentaire est concerné par la confidentialité, son certificat de chiffrement peut être chargé aussi dans cette carte.

Le porteur, déjà enregistré, s'identifie à l'opérateur d'enregistrement en présentant une pièce d'identité.

3.6. Identification et validation d'une demande de certificat de secours

Suite à l'oubli de sa carte IMAGE, il est nécessaire de permettre au porteur d'obtenir un certificat de secours à usage provisoire.

Le certificat de chiffrement n'est pas importé dans les cartes de secours.

3.7. Identification et validation pour débloquer une carte IMAGE

La procédure est décrite dans le document [PC-Personnes-Authentification].

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1. Demande de certificat

4.1.1. Origine de la demande

Les personnes concernées par la confidentialité sont identifiées par l'AEL.

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

La demande de certificat est établie par l'opérateur d'enregistrement, exclusivement pour les personnes identifiées par l'AEL comme des personnes concernées par la confidentialité.

4.2. Traitement d'une demande de certificat

4.2.1. Processus d'identification et de validation

Les personnes concernées doivent être préalablement porteurs d'une carte IMAGE, établie suivant les exigences décrites dans le document [PC-Personnes-Authentification]. L'opérateur d'enregistrement recherche le nom de la personne dans la liste des personnes internes déjà enregistrées et valide la demande.

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

4.2.2. Acceptation ou rejet de la demande

La demande ne fait pas d'objet de validation.

4.2.3. Durée d'établissement du certificat

Les certificats de chiffrement sont valables pour une durée de six ans.

4.3. Délivrance du certificat

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

Suite à la demande de l'opérateur d'enregistrement, l'AC déclenche les processus de génération du certificat.

Le bi-clé et le certificat de chiffrement sont générés en central et conservés de manière protégée au sein de l'IGC et mis à disposition dans l'entité de publication. Le bi-clé de chiffrement est également conservé dans la base de séquestre de l'IGC (cf. 4.12.1).

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

Lorsque la génération est terminée, un courriel est envoyé automatiquement à l'utilisateur pour l'informer que son certificat de chiffrement est disponible. Ce courriel contient une url qui l'envoie vers la page Web de l'entité de publication pour la récupération du bi-clé et du certificat.

En général, l'opérateur d'enregistrement se met en contact avec le porteur pour l'assister à charger le certificat et bi-clé dans sa carte, ou ses cartes, IMAGE.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

L'utilisateur est guidé dans l'opération de mise à jour de sa carte IMAGE. Il doit saisir son code-pin pour s'authentifier et autoriser l'importation du bi-clé et du certificat dans sa carte.

La même opération peut être effectuée pour importer ce certificat de chiffrement dans sa carte IMAGE

supplémentaire, si pertinent.

4.4.2. Publication du certificat

L'opération de retrait du certificat de chiffrement reste possible autant de fois que le porteur souhaite et sans limitation de temps soit à partir de l'url du courriel, soit en accédant directement à l'entité de publication de l'IGC IMAGE.

4.5. Usages de la bi-clé et du certificat

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

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de confidentialité.

Les certificats de chiffrement sont ajoutés sur les cartes IMAGE des utilisateurs concernés.

Pour pouvoir accéder à une zone chiffrée, l'utilisateur concerné par la confidentialité doit être préalablement enregistré dans une liste d'accès pour la zone chiffrée en question auprès du logiciel de chiffrement. Cet enregistrement s'effectue avec le certificat de chiffrement du porteur concerné par la confidentialité.

L'autorisation de l'accès à la zone chiffrée se fait avec le certificat de chiffrement après saisie du code-pin. L'accès est contrôlé par le logiciel de chiffrement en se basant sur la liste d'accès à la zone.

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

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

Les utilisateurs des certificats de chiffrement sont les porteurs des mêmes certificats.

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

4.6. 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, conformément aux exigences de la PRIS V 2.1.

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

Les certificats et les bi-clés de chiffrement sont renouvelés tous les six ans.

Nota - Par la suite, le terme « renouvellement du certificat » recouvre également le changement de bi-clé du porteur.

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

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques.

Par ailleurs, une bi-clé et un certificat peuvent être fournis de nouveau à un porteur par anticipation, suite à la révocation du certificat du porteur.

4.7.2. Origine d'une demande de renouvellement de certificat

Les opérateurs d'enregistrement sont informés par courriel de la prochaine expiration de certificats de chiffrement.

Peu avant la date d'expiration de leur certificat, les porteurs internes sont également avertis par courriel.

Les demandes des porteurs externes sur site sont effectuées par le Directeur de leur direction d'accueil.

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

L'AEL confirme que le porteur est toujours concerné par la confidentialité.

L'opérateur d'enregistrement effectue la demande de renouvellement.

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

La procédure de notification du nouveau certificat au porteur est identique à celle de la demande initiale.

4.7.5. Démarche d'acceptation du nouveau certificat

La démarche d'acceptation du nouveau certificat est identique à celle de la demande initiale.

4.7.6. Publication du nouveau certificat

Le dispositif de publication du nouveau certificat est identique à celui de la demande initiale.

4.8. Modification du certificat

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

4.9. Révocation et suspension des certificats

4.9.1. Causes possibles d'une révocation

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

- l'une des informations nominatives du porteur figurant dans son certificat de chiffrement est périmée, ceci avant l'expiration normale du certificat[2] ;

[2] Il appartient au porteur de signaler tout changement dans celles-ci.

- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur ;
- la clé privée du porteur est suspectée de compromission, est compromise, ou la carte IMAGE est perdue ou est volée ;
- le porteur ne fait plus partie du personnel du Ministère ;
- dans le cas d'un porteur externe sur site : le porteur quitte le Ministère ;
- le porteur lors d'une mutation, d'une évolution de ses fonctions, ou pour une autre raison, n'est plus concerné par la confidentialité ;

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

4.9.2. Origine d'une demande de révocation

Les personnes qui peuvent effectuer la révocation d'un certificat de porteur sont les suivantes :

- le porteur au nom duquel le certificat a été émis,
- l'opérateur d'enregistrement.

L'AEL peut également émettre une demande administrative de révocation d'un certificat de chiffrement de ce porteur à destination de l'opérateur d'enregistrement.

4.9.3. Procédure de traitement d'une demande de révocation faite par le porteur

Pour révoquer son certificat, le porteur peut :

- se rendre auprès de son opérateur d'enregistrement pour demander la révocation de son certificat,

- effectuer lui-même cette opération en ligne. Pour cela, il doit se connecter à l'adresse suivante : http://igc.sante.gouv.fr. Le porteur est identifié en fournissant son adresse de messagerie, puis est authentifié à l'aide du jeu de questions/ réponses qu'il avait fourni lors de l'enregistrement initial.

Dans les deux cas, le porteur peut préciser la cause de la révocation, à l'aide d'un commentaire libre.

Une fois la demande authentifiée 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.

4.9.4. Délai accordé au porteur pour effectuer la révocation

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

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

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 porteur est effective dans un délai inférieur à 24 heures, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs de certificat.

4.9.6. Exigences de vérification de la révocation par les utilisateurs de certificat

Les tiers utilisateurs de certificat 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 certificat selon les contraintes liées à leur application.

Dans le cas du système de confidentialité du Ministère, la vérification s'effectue lors de chaque nouvelle déclaration de droits.

4.9.7. 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.

4.9.8. Délai maximum de publication d'une LCR

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

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

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

4.9.10. Autres moyens disponibles d'information sur les révocations

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

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

La clé privée 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 du porteur,
- 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, le porteur est tenu d'effectuer une demande de révocation dans les meilleurs délais.

En cas de suspicion de compromission de son code d'activation, le porteur est tenu de le changer lui-même sans tarder, en se rendant auprès de la cellule informatique qui dispose de l'outil adéquat.

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

4.9.12. Causes possibles d'une suspension

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

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

4.10.1. 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 d'un porteur, c'est-à-dire :

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

via la consultation libre de la LCR.

La LCR émise par l'AC Personnes 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 Personnes relèvent de la responsabilité de l'AC Racine et peuvent donc être obtenues auprès de celle-ci.

4.10.2. 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.

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

Ce cas est couvert par le paragraphe §4.9.1.

4.12.Séquestre de clé et recouvrement

Les clés privées de chiffrement des porteurs sont générées en central dans le HSM et séquestrées.

Dans le cas où le porteur a perdu sa carte à puce, ou bien celle-ci n'est plus opérationnelle, le porteur peut réimporter son certificat et ses clés de chiffrement dans une nouvelle carte à puce par le biais de la fonction de retrait de certificat. Dans ce cas la fonction de recouvrement n'est pas utile.

Dans le cas où le porteur est absent du Ministère, a quitté le Ministère, ou est décédé, il peut être nécessaire d'utiliser la fonction de recouvrement afin de récupérer le certificat et la clé privée de chiffrement afin de déchiffrer des données chiffrées avec le certificat du porteur en question. Ce cas

peut arriver si les données sont enregistrées dans une zone que seul le porteur en question peut accéder.

La fonction de recouvrement consiste à restituer à une personne autorisée l'ancienne clé privée. Cette restitution se fait au moyen d'un fichier PKCS#12, protégé par une phrase de passe, obtenus lors d'une opération de recouvrement des clés.

Les différentes étapes de séquestre et de recouvrement de clés privées de porteurs respectent les exigences des paragraphes qui suivent.

4.12.1. Demande de séquestre

Pour les clés privées de chiffrement la demande de séquestre est automatiquement véhiculée dans l'IGC par la demande de certificat.

La durée de conservation de la clé privée séquestrée est supérieure à la durée de validité du certificat correspondant.

4.12.2. Traitement d'une demande de séquestre

La demande de séquestre de la clé privée étant véhiculée par la demande de certificat correspondant, le processus d'identification et de validation correspond à celui de la demande de certificat.

L'AC génère la bi-clé du porteur et le certificat associé et transmet la clé privée et le certificat associé à la fonction de séquestre suivant un processus qui assure, de bout en bout, la confidentialité, l'intégrité et l'authentification d'origine.

L'intégrité des clés privées séquestrées et des certificats associés ainsi que la confidentialité des clés privées séquestrées sont assurées en permanence, y compris lors d'éventuels échanges internes à l'IGC. La conservation de ces clés et des certificats associés se fait sous forme chiffrée, la clé de déchiffrement étant conservée dans un module cryptographique. Les mécanismes assurant la sécurité des clés séquestrées sont adaptés à la durée de conservation de ces clés.

Chaque clé privée séquestrée fait l'objet d'un « identifiant de séquestre » unique, généré de manière séquentielle. Le dossier correspondant à cet identifiant de séquestre contient la référence du dossier

qui a permis la création de la clé. Il est ainsi possible de connaitre toutes les caractéristiques de la clé privée séquestrée et du certificat associé.

La mise en séquestre est enregistrée dans les journaux d'évènements de l'IGC.

4.12.3. Origine d'une demande de recouvrement

Le besoin de recouvrement de clé privée de chiffrement est constaté par la nécessité de récupérer des données chiffrées et que le seul porteur en mesure de les accéder est absent (départ du Ministère, absence prolongée,…).

4.12.4. Identification et validation d'une demande de recouvrement

La demande de recouvrement porte sur un dossier relatif à un certificat du porteur. L'identifiant de séquestre (cf §4.12.2) permet d'identifier précisément la clé privée à recouvrer. Le motif du recouvrement peut être renseigné[3].

L'opération de recouvrement nécessite l'authentification de deux personnes dans des rôles de confiance dans l'IGC : ces personnes doivent être dans un rôle d'opérateur d'enregistrement.

Il n'est pas requis que ces 2 administrateurs soient physiquement présents au même endroit. Ils doivent par contre agir dans un intervalle de temps limité.

Le premier opérateur d'enregistrement initialise la demande de recouvrement dans l'IGC, le deuxième doit confirmer la demande dans l'IGC.

4.12.5. Traitement d'une demande de recouvrement

Le deuxième demandeur est invité à saisir une passe-phrase dont la longueur ne peut être inférieure à 8 caractères.

[3] sous forme d'un texte libre.

La demande de recouvrement et la passe-phrase associée sont protégées en intégrité et en confidentialité. De cette façon l'opération de recouvrement garantit que seule la clé privée sur laquelle porte le recouvrement sera divulguée.

La fonction de recouvrement remet au demandeur du recouvrement à la fois la clé privée recouvrée et le certificat associé, sous la forme d'un fichier au format PKCS#12 protégé par la phrase de passe initialement communiquée.

Les opérations relatives au recouvrement sont journalisées dans l'IGC.

4.12.6. Destruction des clés séquestrées

Dès la fin de la période de conservation d'une clé séquestrée, tout exemplaire de cette clé détenue par l'AC est détruit de manière fiable afin de ne pouvoir être ni recouvrée ni reconstituée.

4.12.7. Disponibilité des fonctions liées au séquestre et au recouvrement

La fonction de séquestre étant liée aux demandes de certificat, est disponible dans les mêmes conditions que celles-ci.

La fonction de recouvrement ne sera rendue qu'en fonction des heures de service des opérateurs d'enregistrement concernés.

Le délai de traitement maximal d'une demande de recouvrement, entre l'enregistrement de la demande du premier opérateur d'enregistrement et la remise de la clé privée recouvrée au deuxième demandeur sous la forme d'un fichier PKCS#12 chiffré par la passe-phrase fournie par ce deuxième demandeur est d'une heure maximum.

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.

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.

Opérateur d'enregistrement : Personne ayant reçu délégation de l'AEL, de la part des administrateurs centraux et réalisant les différentes opérations de gestion des certificats des porteurs.

Opérateur d'enregistrement délégué : Personne ayant reçu délégation de l'AEL de la part d'un opérateur d'enregistrement, et assurant les mêmes fonctions que celui-ci.

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 décrites 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.

Cellules informatiques : Services chargés de fournir aux porteurs le support technique relatif à leur environnement informatique, bureautique et réseau. Dans le cadre de l'IGC ils peuvent effectuer notamment les déblocages de carte IMAGE.

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.

Guichet Unique de Services (GUS) : Centre d'appels chargé du support technique à des porteurs référencés.

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 de l'AC 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 associée à cette PC

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, exception faite des opérateurs d'enregistrement.

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.

Les opérateurs d'enregistrement sont informés de leurs responsabilités et des procédures en vigueur par une lettre de mission signée par l'AEL.

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 sanctions disciplinaires s'il y a lieu.

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

Le personnel des prestataires externes intervenant dans les locaux et/ou sur la plate-forme hébergeant l'IGC doit également respecter les exigences du présent chapitre. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

5.3.8. 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, exception faite des opérateurs d'enregistrement ;
- 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 porteur 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 dans le cadre des dispositions de la présente PC :

- acceptation ou refus de connexion à l'application IGC ;
- demande de certificat de chiffrement ;
- demande de renouvellement de certificat de chiffrement ;
- génération de bi-clé et de certificat de chiffrement ;
- importation de bi-clé et de certificat chiffrement dans la carte IMAGE du porteur ;
- demande de révocation de certificat de chiffrement ;
- révocation de certificat de certificat de chiffrement ;
- 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, dont les opérateurs d'enregistrement ;
- 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 papier ou 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 quotidiennement afin de vérifier le fonctionnement normal de l'AC, et de mettre en évidence les tentatives d'intrusion au niveau de l'application.

Son contenu est également surveillé chaque semaine afin de vérifier le fonctionnement normal de l'AC,

et la cohérence entre les différents types d'évènement au niveau de l'infrastructure d'IGC.

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 sur papier ou bureautique

Les enregistrements papier 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 sur papier ou bureautique

Les journaux sous forme papier sont conservés en lieu sûr par leur dépositaire.

Les journaux sous forme de document bureautique 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 sur papier ou bureautique

Les enregistrements papier ne sont pas sauvegardés.

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 journaux d'événements tels qu'identifiés dans la section ci-dessus.

Les données conservées sous forme de document bureautique 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, les « Conditions d'Utilisation des certificats et des cartes IMAGE »…). 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 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 6.8.

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. En particulier, chaque opérateur d'enregistrement accède à ses données d'enregistrement.

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 porteurs qu'elle a émis et de façon à pouvoir émettre des certificats porteurs sans discontinuité.

La nouvelle bi-clé générée servira à signer les nouveaux certificats porteurs 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 composants 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 porteurs et 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 Personnes, 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, permettant le respect des exigences de la présente PC en matière de disponibilité des fonctions de l'IGC, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

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 cession d'activité affectant l'AEL

La mise en oeuvre 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'opérateurs d'enregistrement 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 et installation de bi-clés

6.1.1. Génération des bi-clés

6.1.1.1 Clés d'AC

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 Personnes 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.

6.1.1.2 Clés porteurs générées par l'AC

La génération de la bi-clé de chiffrement du porteur est effectuée par l'AC dans le boitier cryptographique qui répond aux exigences de l'annexe 2 du document [PRIS-PC].

6.1.2. Transmission de la clé privée à son propriétaire

La clé privée de chiffrement est transmise directement du boitier cryptographique à la carte IMAGE du porteur.

La transmission est réalisée d'une manière sécurisée par le guichet de retrait de l'IGC après authentification du porteur par la même carte à puce.

6.1.3. Transmission de la clé publique d'un porteur à l'AC

L'AC génère elle-même la bi-clé de chiffrement du porteur.

6.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificat et aux porteurs

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

6.1.5. Tailles des clés

Les clés d'AC et de porteurs respectent les exigences de caractéristiques (tailles, algorithmes, etc.) du document [PRIS-PC]. Les clés d'AC sont des clés RSA de 2048 bits. Les clés des porteurs sont des clés RSA de 2048 bits.

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

Les boîtiers cryptographiques qui génèrent les bi-clés utilisent des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

6.1.7. 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 de chiffrement du porteur et du certificat associé est strictement limitée au service de confidentialité tel que décrit dans la présente PC.

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

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 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+.

Les clés privées d'AC ne sont ni séquestrées ni archivées.

Les clés privées de chiffrement des porteurs sont générées dans le module cryptographique et séquestrées. Elles sont transmises dans la carte IMAGE d'une manière sécurisée.

6.2.1.2 Dispositifs de protection des clés privées des porteurs

Le boitier cryptographique utilisé pour générer et protéger les clés privées de chiffrement des porteurs répond aux exigences de l'annexe 2 du document [PRIS-PC].

6.2.2. Contrôle de la clé privée par plusieurs personnes

Ce paragraphe porte sur le contrôle de la clé privée d'AC pour l'exportation / importation hors / dans un module cryptographique.

La génération de la bi-clé est traitée dans §6.1.1, l'activation de la clé privée dans §6.2.8, et sa destruction dans §6.2.10.

Le contrôle des clés privées de signature de l'AC est assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets Shamir avec n=2.

6.2.3. Séquestre de la clé privée

Les clés privées des porteurs sont systématiquement séquestrées, conformément aux dispositions prévues dans la présente PC et la DPC de l'AC, et en respectant les exigences de séquestre et de recouvrement du §4.12.

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

6.2.4. Copie de secours de la clé privée

Les clés privées des porteurs séquestrées par l'AC peuvent faire l'objet de copies de secours par l'AC, moyennant le respect des exigences de sécurité pour le séquestre des clés.

Pour les clés privées d'AC, le Ministère s'est réservé le droit de faire des copies de secours :

- dans le module cryptographique redondé conforme aux exigences de l'annexe 2 du document [PRIS-PC],
- hors d'un module cryptographique sous la forme de clés chiffrées par la clé maître du module cryptographique (insérée sous forme de composant de clés lors de la phase d'initialisation). Toutes les opérations de chiffrement et de déchiffrement sont donc réalisées à l'intérieur du module cryptographique. Un mécanisme de contrôle d'intégrité est également mis en place.

Cette copie hors module permet de réinitialiser avec les clés de l'IGC :

- le module primaire ou le module redondé,
- un nouveau module dans le cas d'une défaillance matérielle.

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

6.2.5. Archivage de la clé privée

Les clés privées de l'AC ne sont en aucun cas archivées.

Les clés privées des porteurs ne sont archivées ni par l'AC, ni par aucune composante de l'IGC.

Les clés privées de chiffrement des porteurs sont par contre séquestrées par l'AC.

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

Pour les clés privées des porteurs, le transfert se fait conformément aux exigences de §6.1.1.2 ci-dessus.

Pour les clés privées d'AC, tout transfert se fait sous forme chiffrée, conformément aux exigences du chapitre 6.2.4.

6.2.7. Stockage de la clé privée dans un module cryptographique

Les clés privées de l'AC sont stockées dans un module cryptographique répondant aux exigences de l'annexe 2 du document [PRIS-PC] pour le niveau de sécurité **.

Le stockage des clés privées de l'AC est effectué en dehors d'un module cryptographique moyennant le respect des exigences de §6.2.4.

6.2.8. Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'AC

La méthode d'activation des clés privées d'AC dans le module cryptographique permet de répondre aux exigences définies dans l'annexe 2 du document [PRIS-PC] pour le niveau de sécurité **.

L'activation des clés privées d'AC dans un module cryptographique est contrôlée via des données d'activation (cf. §**Erreur ! Source du renvoi introuvable.**) et fait intervenir au moins deux personnes dans des rôles de confiance.

6.2.8.2 Clés privées des porteurs

L'activation de la clé privée du porteur est contrôlée via un code PIN (cf. §**Erreur ! Source du renvoi introuvable.**) et permet de répondre aux exigences définies dans le chapitre **Erreur ! Source du renvoi introuvable.** pour le niveau de sécurité **.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'AC

La désactivation des clés privées d'AC dans le module cryptographique est automatique dès que l'environnement du module évolue :

- arrêt ou déconnexion du module,
- déconnexion de l'opérateur, etc.

Une clé privée d'AC peut également être désactivée après une certaine période d'inactivité.

Ces conditions de désactivation doivent permettre de répondre aux exigences définies dans l'annexe 2 du document [PRIS-PC] pour le niveau de sécurité **.

6.2.9.2 Clés privées des porteurs

La clé privée d'un porteur est désactivée dès que la carte à puce est déconnectée. Elle est aussi désactivée par logiciel après une période d'inactivité. Ceci permet de forcer une redemande du code PIN.

6.2.10. Méthode de destruction des clés privées

6.2.10.1 Clés privées d'AC

La méthode de destruction des clés privées d'AC permet de répondre aux exigences définies dans l'annexe 2 du document [PRIS-PC] pour le niveau de sécurité **.

En fin de vie d'une clé privée de l'AC, normale ou anticipée (révocation), cette clé est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.10.2 Clés privées des porteurs

Un certificat expiré ne peut plus être utilisé pour chiffrer des nouveaux messages, mais la clé privée correspondante peut continuer à être utilisée pour déchiffrer des messages qui ont été préalablement chiffrés à l'aide de la clé publique contenue dans ce certificat. A la fin de sa période de validité, un certificat expiré ne sera pas systématiquement détruit, afin que le porteur continue à accéder aux messages précédemment chiffrés avec l'ancienne clé publique.

La place étant limitée dans une carte à puce, seuls les couples, certificat de chiffrement et clé privée associée, courants et précédents seront conservés.

Pour exécuter une opération de destruction d'un couple certificat de chiffrement et clé privée associée, l'opérateur d'enregistrement dispose d'un outil logiciel. Lorsque qu'un couple, certificat de chiffrement et clé privée associée, est détruit dans la carte à puce, il l'est de manière définitive.

6.2.11. Niveau d'évaluation sécurité du module cryptographique

Les modules cryptographiques de l'AC sont évalués au niveau EAL4+ des critères communs correspondant à l'usage visé, tel que précisé dans l'annexe 2 du document [PRIS-PC].

Les cartes à puce des porteurs satisfont les exigences au niveau correspondant à l'usage visé, tel que précisé au chapitre **Erreur ! Source du renvoi introuvable.** ci-dessous.

6.3. Autres aspects de la gestion des bi-clés

6.3.1. Archivage des clés publiques

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

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

Les bi-clés et les certificats des porteurs couverts par la présente PC ont une durée de validité de six

ans.

La durée de validité des clés de signature d'AC et des certificats correspondants est de dix ans. Les certificats d'AC sont renouvelés après une période de 7 ans maximum, afin que toute la période de validité des certificats d'authentification émis pour les porteurs soit couverte.

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

6.4.1.1 Génération et installation des données d'activation correspondant à la clé privée de l'AC

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.

6.4.1.2 Génération et installation des données d'activation correspondant à la clé privée du porteur

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

6.4.2. Protection des données d'activation

6.4.2.1 Protection des données d'activation correspondant à la clé privée de l'AC

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.

6.4.2.2 Protection des données d'activation correspondant à la clé privée du porteur

Ces données d'activation sont choisies par les porteurs eux-mêmes.

6.5. 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 opérateurs d'enregistrement et 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 opérateurs d'enregistrement et 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.

6.6. Mesures de sécurité des systèmes durant leur cycle de

vie

6.6.1. 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.

6.6.2. 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.

6.7. Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires 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.

6.8. 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 de chiffrement émis par l'AC Personnes, ainsi que les profils de la LCR et des réponses OCSP correspondantes figurent dans le document [PC-Profils].

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 Personnes fait contrôler la conformité de 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 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 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 :

- le code d'activation de la carte IMAGE
- les jeux de questions /réponses de chaque porteur ;
- les causes de révocation des certificats des porteurs ;
- le dossier d'enregistrement du porteur.

9.4.3. Informations à caractère non personnel

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

- les adresses de messagerie professionnelles des porteurs.

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 :

- pouvoir démontrer aux utilisateurs de certificat qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, conformément aux exigences de la présente PC ;
- garantir et maintenir la cohérence de sa DPC avec la présente PC ;
- prendre toutes les mesures raisonnables pour s'assurer que les porteurs soient au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion du certificat de chiffrement ; ceux-ci sont résumés dans le document [Charte-Confidentialité] ;
- prendre toutes 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 de la présente PC 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 porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

Par ailleurs, 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 opérateurs d'enregistrement

Les opérateurs d'enregistrement ont 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 porteurs.

9.6.3. Obligations applicables aux porteurs

Les porteurs ont le devoir de respecter les exigences décrites dans le document [Charte-Confidentialité].

9.6.4. Obligations applicables aux utilisateurs de certificat

Les utilisateurs de certificat doivent :

- vérifier et respecter les conditions d'utilisation pour lesquelles un certificat a été émis et décrites dans le document « Conditions d'Utilisation des certificats et des cartes IMAGE applicables aux tiers utilisateurs »),
- Contrôler la validité du certificat de l'Autorité de Certification « Personnes » :
  - par contrôle de la signature par l'Autorité de Certification « 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'Autorité de Certification « Racine » ;
- Contrôler la validité de chaque certificat porteur :
  - par contrôle de la signature par l'Autorité de Certification « Personnes » ;
  - 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'Autorité de Certification « Personnes ».
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC,
- contrôler que le certificat émis par l'AC Personnes est référencé au niveau de sécurité requis par l'application.

Les « Conditions d'Utilisation des certificats et des cartes IMAGE applicables aux tiers utilisateurs »

constituent un document public auquel les utilisateurs de certificat ont accès.

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 de l'AC est valide jusqu'à :

- émission d'une mise à jour majeure du présent document, avec évolution du numéro de version,
- 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 ». 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 porteurs seront avertis des amendements au moyen de leur adresse de messagerie et/ou sur l'Intranet du Ministère.

Les amendements applicables seront également reportés sur la version mise à jour des différents documents « Conditions d'Utilisation des certificats et des cartes IMAGE » applicables aux porteurs et aux tiers utilisateurs de certificat.

Les porteurs et 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 distinguer quels certificats correspondent à quelles exigences.

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).