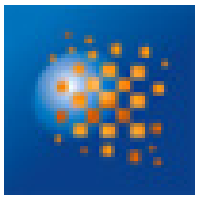
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'EUROPE ET DES
AFFAIRES ÉTRANGÈRES

# Politique de Certification des AC INFRASTRUCTURE

## Services applicatifs



**OID : 1.2.250.1.214.69.3.1.3.1.21.1**

**Cotation Archive : E.3.1.3.1**

**Version 1.0.5 du 06/09/2019**

**État : validé**

| Suivi des mises à jour | | | |
|---|---|---|---|
| **Version** | **Date** | **Auteur** | **Commentaire(s)** |
| 1.0.1 | 17/07/2015 | Solucom | Création au format RGSv2 |
| 1.0.2 | 26/05/2016 | Solucom | Renouvellement des AC |
| 1.0.3 | 10/10/2016 | MAEDI | Ajout des équipements DPHONE |
| 1.0.4 | 20/07/2018 | MAEDI | Mise à jour du document |
| 1.0.5 | 06/09/2019 | Wavestone | Renouvellement des AC |

# SOMMAIRE

# FIGURES



# TABLEAUX

# DOCUMENTS DE REFERENCE

| Renvoi | En ligne | Joint | Titre |
|---|---|---|---|
| [1] | ☑ | ☐ | Référentiel Général de Sécurité – version 2.0 - Politique de Certification Type «certificats électroniques de services applicatifs» version 3.0 |
| [2] | ☑ | ☐ | Politique de Certification de l'AC RACINE DIPLOMATIE |

# 1 INTRODUCTION

## 1.1 PRESENTATION GENERALE

### 1.1.1 OBJET DU DOCUMENT

Le Ministère des Affaires Étrangères dispose d'une infrastructure de gestion de clés (IGC DIPLOMATIE), qui assure la fourniture de certificats électroniques destinés à l'ensemble des agents ou les composants techniques du MINISTÈRE.

L'IGC DIPLOMATIE est constituée d'une hiérarchie d'Autorités de Certification :

- l'AC RACINE DIPLOMATIE ;
- trois AC Déléguées et leurs renouvellements en version 2 : AC UTILISATEURS, AC INFRASTRUCTURE et AC UTILISATEURS RENFORCÉE.

Chacune des AC émet plusieurs types de certificats.

L'AC INFRASTRUCTURE émet notamment des certificats :

- «Accès distant » : destinés aux postes de travail Itinéo, tablettes dPad, smartphones dPhone, passerelles ou boîtiers NETASQ auxquels se connectent les postes EOLE.
- « Serveur SSL » et « Client SSL » : destinés aux serveurs et aux ressources informatiques du Ministère ou d'autres entités. Ils sont de type logiciel.
- « Signature de configuration » : destinés à signer des configurations logicielles pour en assurer l'authenticité et l'intégrité.
- « Signature de code » : destinés à signer des codes logiciels pour en assurer l'authenticité et l'intégrité.
- « Signature de jetons d'horodatage » : destinés à la signature de jetons émis par l'Autorité d'Horodatage du Ministère.

Ces certificats sont de type logiciel.

Le présent document constitue la Politique de Certification (PC) de l'Autorité de Certification – AC INFRASTRUCTURE du Ministère conformément à la norme RGS v2.

Cette Politique de Certification a vocation à être consultée et examinée par les personnes qui utilisent ces certificats pour les aider à apprécier le degré de confiance qu'ils peuvent placer dans ces certificats.

Cette Politique de Certification est un document public et est mise à disposition du public sous format électronique sur le site web du Ministère.

Cette Politique de Certification s'appuie sur la Politique de Certification de l'AC RACINE DIPLOMATIE [2].

### 1.1.2 CONVENTION DE REDACTION

Sans Objet.

## 1.2 IDENTIFICATION DU DOCUMENT

La présente PC porte le titre suivant :

**Politique de certification de l'Autorité de Certification**
**AC INFRASTRUCTURE**

La PC relative aux certificats délivrés par l'AC INFRASTRUCTURE est identifiée par l'OID suivant : 1.2.250.1.214.69.3.1.3.1.21.1

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

Cette Politique de Certification traite des certificats identifiés dans plusieurs précédentes PC en version RGS 2.3. Les certificats tous issus de l'AC INFRASTRUCTURE sont toujours en vigueur à date de rédaction du présent document. Les OID des PC correspondantes sont les suivants :

| Gamme de certificats | OID |
|---|---|
| « Accès Distant » | 1.2.250.1.214.69.3.1.3.1.1.1 |
| « Client SSL » | 1.2.250.1.214.69.3.1.3.1.7.1 |
| « Serveur SSL » | 1.2.250.1.214.69.3.1.3.1.9.1 |
| « Signature de code » | 1.2.250.1.214.69.3.1.3.1.13.1 |
| « Signature de configuration » | 1.2.250.1.214.69.3.1.3.1.13.1 |
| « Signature de jetons d'horodatage » | 1.2.250.1.214.69.3.1.3.1.17.1. |

## 1.3 DEFINITIONS ET ACRONYMES

Cf. Annexe 3.

## 1.4 ENTITES INTERVENANT DANS L'IGC

Ce paragraphe présente les entités intervenant dans l'Infrastructure de Gestion de Clés (IGC), ainsi que les obligations auxquelles elles sont soumises.

Les obligations suivantes sont communes à toutes les entités de l'IGC :

- documenter et respecter les accords, conventions ou contrats qui lient le Ministère aux autres entités ;
- mettre en œuvre les moyens techniques et humains nécessaires à la réalisation des prestations auxquelles l'entité s'engage dans les conditions garantissant qualité et sécurité.

### 1.4.1 AUTORITES DE CERTIFICATION

L'IGC DIPLOMATIE est constituée des AC suivantes :

- L'Autorité de Certification racine, dite AC RACINE DIPLOMATIE.
- Les Autorités de Certification Déléguées :
    - AC UTILISATEURS
        - Elle délivre des certificats destinés aux Porteurs personnes physiques : agents du Ministère et externes.
        - Les usages des certificats délivrés sont divers : signature personnelle et chiffrement pour l'usage de messagerie sécurisée, et authentification pour l'authentification auprès de serveurs. Les certificats sont nominatifs, au nom du Porteur.
        - Les supports sont soit logiciels soit matériels (ex : carte à puce, clé USB).
    - AC INFRASTRUCTURE
        - Elle délivre des certificats destinés aux Porteurs éléments de l'infrastructure (composants de l'IGC, supports matériels, serveurs, routeurs, etc.).
        - Les usages des certificats délivrés sont divers : certificats d'authentification client/serveur, certificats SSL, certificats « accès distant », signature de configuration, signature de jetons d'horodatage etc.
        - Les supports sont logiciels.
    - AC UTILISATEURS RENFORCÉE
        - Elle délivre des certificats destinés à des personnes physiques : agents du MAE et externes (prestataires du MAE et agents d'autres Ministère ou de l'Élysée).
        - Les usages des certificats délivrés sont divers : signature personnelle forte (signature de documents…), confidentialité forte (chiffrement de la base locale sur le poste du porteur) et authentification forte (à des applications sensibles). Les certificats sont nominatifs.
        - Les supports sont matériels, sur carte à puce appelée « carte MAE ».

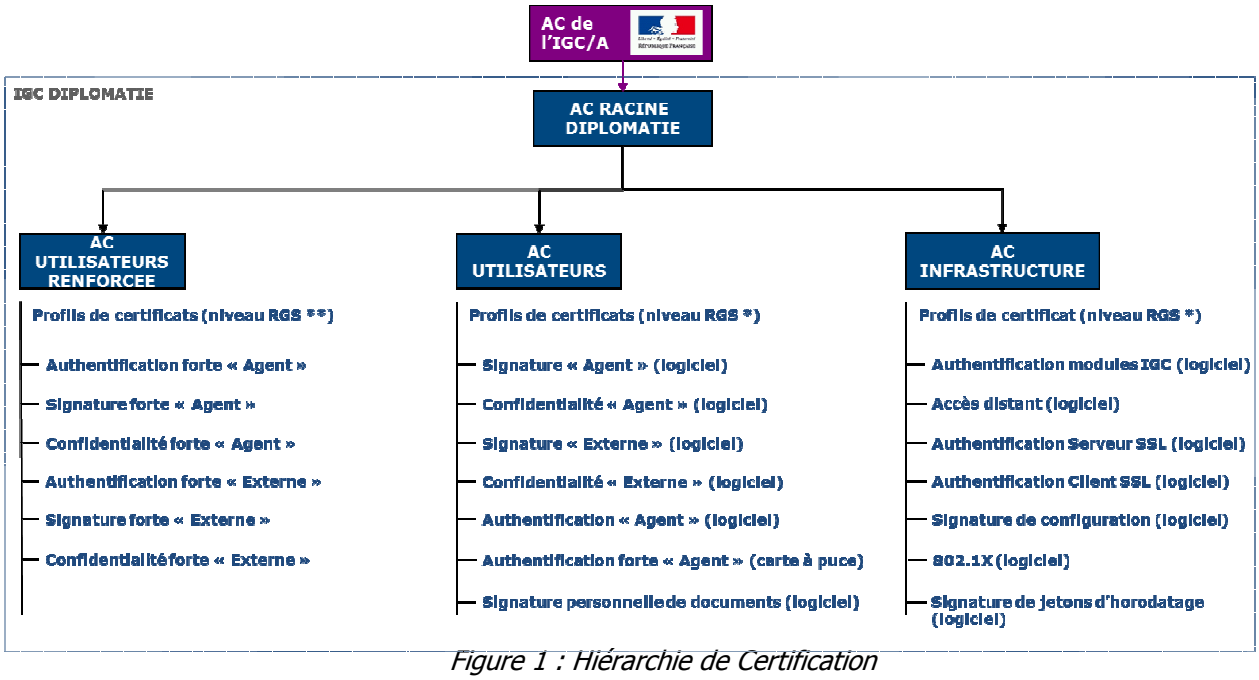



*Figure 1 : Hiérarchie de Certification*

Le rôle d'Autorité de Certification Déléguée est assuré par le Directeur des Systèmes d'Information, qui encadre l'ensemble des équipes de la DSI.

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

Les prestations de l'ACD 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.

**Fonction de remise au RC :**

Cette fonction remet au RC au minimum le certificat du service applicatif ainsi que, le cas échéant, les autres éléments fournis par l'IGC (dispositif de protection des éléments secrets, clé privée du service applicatif, codes d'activation…).

**Fonction de publication :**

Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux RC ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides des services applicatifs.

**Fonction de gestion des révocations :**

Dans le cadre de cette fonction, l'ACD 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 par la publication d'informations de révocation sous forme de LCR.

L'ACD doit également assurer les fonctions suivantes :

- 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 de certificat, de gestion des révocations et d'information sur l'état des certificats.

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

- Responsable du certificat (RC) - Personne physique responsable du certificat électronique du service applicatif, notamment de l'utilisation de ce certificat et de la bi-clé correspondante, pour le compte du service applicatif identifié dans le certificat ;
- Utilisateur de certificat - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une valeur de cachet ou d'authentification serveur provenant du service applicatif auquel le certificat est rattaché, ou pour établir une clé de session ;
- Personne autorisée- Il s'agit d'une personne autre que le RC et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du RC (demande de révocation, de renouvellement...).

### 1.4.2 AUTORITE D'ENREGISTREMENT

L'Autorité d'Enregistrement a pour rôle de vérifier l'identité du futur RC et les informations liées au serveur informatique (cf. chapitre 1.6.2). Pour cela, l'AE assure les tâches suivantes :

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

### 1.4.3 RESPONSABLE DE CERTIFICATS ELECTRONIQUES DE SERVICES APPLICATIFS

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

Le RC respecte les conditions qui lui incombent définies dans la présente PC.

Il est à noter que le certificat étant attaché à l'entité et non au RC, ce dernier peut être amené à changer en cours de validité du certificat : départ du RC de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.

L'entité doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RC de ses fonctions et lui désigner un successeur. L'AC doit révoquer un certificat électronique pour lequel il n'y a plus de RC explicitement identifié.

#### 1.4.3.1 CERTIFICAT DE PROFIL « ACCES DISTANT»

Les RC sont les responsables des boîtiers NetASQ (ESU SSI), les titulaires des postes Itinéo, l'équipe en charge de la préparation des tablettes dPad et des smartphones dPhone (service des ACSSI) et les responsables des composants techniques et des serveurs doivent respecter les conditions définies dans cette Politique de Certification.

Les RC sont chargés d'effectuer les actions suivantes auprès des interlocuteurs adéquats :

- demander un certificat ;
- demander le renouvellement d'un certificat ;
- demander la révocation d'un certificat.

#### 1.4.3.2 CERTIFICAT DE PROFIL « SERVEUR SSL » ET « CLIENT SSL »

Les Porteurs des certificats d'authentification émis par l'AC INFRASTRUCTURE N sont des composants techniques logiciels (applications, annuaires…) ou matériels (routeurs, boîtiers, proxy…) du Ministère.

Les responsables des composants techniques (ESU) doivent respecter les conditions définies dans cette Politique de Certification.

Les responsables des composants techniques sont chargés d'effectuer les actions suivantes :

- Demander un certificat à l'équipe chargée de la validation des demandes de certificats.
- Demander le renouvellement du certificat à l'équipe chargée de la validation des demandes de certificat.
- Demander la révocation du certificat à un opérateur d'AE.

#### 1.4.3.3 CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

Les Porteurs des certificats « Signature de configuration » émis par l'AC INFRASTRUCTURE N sont :

- Les entités du Ministère ou des entités partenaires ayant un besoin de certificat de signature de configuration

En particulier La MOA Hermès demandeur d'émission de certificat, de renouvellement et de révocation des certificats

- L'ANSSI signataire du logiciel SecDroïd et demandeur de révocation des certificats

L'ANSSI, doit respecter les conditions définies dans cette Politique de Certification.

Ils sont chargés d'effectuer les actions suivantes auprès des interlocuteurs adéquats :

- signer le logiciel SecDroïd
- demander la révocation d'un certificat.

La MOA Hermès doit respecter les conditions définies dans cette Politique de Certification.

Ils sont chargés d'effectuer l'action suivante auprès des interlocuteurs adéquats :

- demander la révocation d'un certificat.

#### 1.4.3.4 CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

Les Porteurs des certificats « Signature de code » émis par l'AC INFRASTRUCTURE N sont :

- Les entités du Ministère ou des entités partenaires ayant un besoin de certificat de signature de code

Le Responsable de Certificat doit respecter les conditions définies dans cette Politique de Certification qui lui incombent.

En particulier, il est chargé d'effectuer l'action suivante auprès des interlocuteurs adéquats :

- demander la révocation d'un certificat.

#### 1.4.3.5 CERTIFICAT DE PROFIL « SIGNATURE DE JETONS D'HORODATAGE »

Dans le cadre de la présente PC, le porteur est le serveur informatique tiers utilisé pour la signature des jetons émis par l'Autorité d'Horodatage.

### 1.4.4 UTILISATEURS DE CERTIFICATS

Un utilisateur (ou accepteur) de certificats électroniques d'authentification serveur peut être notamment :

- Une personne accédant à un serveur et qui utilise le certificat du serveur et un module de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat du serveur, afin d'établir une clé de session partagée entre son poste et le serveur.

- Un service applicatif accédant à un serveur informatique et qui utilise un certificat et un applicatif de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat, et afin d'établir une clé de session partagée entre les deux serveurs.

#### 1.4.4.1 CERTIFICAT DE PROFIL « ACCES DISTANT»

Les utilisateurs de type « service applicatif » des certificats émis par l'AC INFRASTRUCTURE sont :

- soit des postes Itinéo (postes EOLE destinés à des agents MAE en mobilité) ;

- soit des tablettes dPad ;

- soit des smartphones dPhone ;

- soit des boîtiers NetASQ.

- Soit les serveurs et ressources informatiques du ministère et d'autres entités

#### 1.4.4.2 CERTIFICAT DE PROFIL « SERVEUR SSL » ET « CLIENT SSL »

Sont appelés utilisateurs, les composants techniques qui utilisent les certificats émis par le Ministère.

Les domaines d'utilisation figurent dans la partie 1.4.1 de la présente Politique de Certification.

#### 1.4.4.3 CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

Sont appelés tiers utilisateurs, le serveur ou applications qui vérifient la configuration ou le logiciel signé par le certificat de signature de configuration.

Les domaines d'utilisation figurent dans la partie 1.4.1 de la présente Politique de Certification.

#### 1.4.4.4 CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

Sont appelés tiers utilisateurs, le serveur ou applications qui vérifient la signature du code ou du logiciel effectuée par le certificat de signature de code.

Les domaines d'utilisation figurent dans la partie 1.4.1 de la présente Politique de Certification.

#### 1.4.4.5 CERTIFICAT DE PROFIL « SIGNATURE DE JETONS D'HORODATAGE »

L'utilisateur des présents certificats de signature de jetons d'horodatage est le serveur identifié comme Porteur de certificats, ainsi que l'ensemble des personnes physiques (ou éléments d'infrastructure) dont le rôle est de vérifier la signature de jetons d'horodatage.

### 1.4.5 AUTRES PARTICIPANTS

#### 1.4.5.1 COMPOSANTE DE L'IGC

La décomposition en fonctions de l'IGC est présentée au chapitre 1.4.1« Autorités de certification ». Les composantes de l'IGC mettant en œuvre ces fonctions sont présentées dans la DPC de l'AC.

#### 1.4.5.2 MANDATAIRE DE CERTIFICATION

Sans objet.

## 1.5 USAGE DES CERTIFICATS

### 1.5.1 DOMAINES D'UTILISATION APPLICABLES

#### 1.5.1.1 BI-CLES ET CERTIFICATS DES SERVICES APPLICATIFS

Les certificats délivrés par l'AC INFRASTRUCTURE N permettent aux composants de s'authentifier entre eux dans le cadre de l'accès distant, et d'authentifier les éléments d'infrastructure du ministère ou d'autres structures en relation avec le ministère.

Ci-dessus l'utilisation faite en fonction du gabarit du certificat :

- « Accès distant » : Établir une authentification au tunnel IPsec
- « Client SSL » : Établir des connexions sécurisées SSL grâce au chiffrement
- « Serveur SSL » : Établir des connexions sécurisées SSL grâce au chiffrement
- «Signature de configuration » : permettre aux services applicatifs de signer des données de façon électronique et de s'authentifier entre eux.
- «Signature de code » permettre aux services applicatifs de signer des codes applicatifs de façon électronique, et de vérifier des signatures.
- « Signature de jetons d'horodatage » permettre à un service de signature de jetons d'horodatage tiers de signer les jetons émis par l'Autorité d'Horodatage du Ministère. Le service de signature de jetons d'horodatage tiers ne peut utiliser les certificats de signature de jetons d'horodatage que pour signer les jetons d'horodatage émis par l'Autorité d'Horodatage du Ministère.

#### 1.5.1.2 BI-CLES ET CERTIFICATS D'AC ET DE SES COMPOSANTES

La clé privée de l'Autorité de Certification – AC INFRASTRUCTURE N n'est utilisée que dans les cas suivants :

- signature des certificats des services applicatifs mis par l'Autorité de Certification – AC INFRASTRUCTURE N ;
- signature de la Liste des Certificats Révoqués (LCR) émise par l'Autorité de Certification – AC INFRASTRUCTURE N.

### 1.5.2 DOMAINES D'UTILISATION INTERDITS

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.5 ci-dessous, en fonction du niveau de sécurité. L'AC doit respecter ces restrictions et imposer leur respect par ses services applicatifs auxquels elle délivre des certificats et les utilisateurs de ces certificats.

À cette fin, elle doit communiquer à tous ses services applicatifs, et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

## 1.6 GESTION DE LA PC

### 1.6.1 ENTITE GERANT LA PC

La PC de l'Autorité de Certification AC INFRASTRUCTURE N est élaborée et mise à jour par le Responsable de la Sécurité de l'Information du Ministère.

Cette PC est soumise à l'approbation du Comité SSI (COSSI) notamment pour :

- valider les usages et restrictions d'usage des certificats émis par cette AC ;
- vérifier sa conformité aux évolutions technologiques et aux exigences fonctionnelles ou réglementaires.

La périodicité minimale de révision de cette PC est de deux (2) ans.

Un tableau indiquant les différentes versions de la PC, les dates de révisions et les principales modifications apportées par rapport à sa version antérieure est présenté en page 2 du présent document.

### 1.6.2 POINT DE CONTACT

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

**Ministère des Affaires Étrangères**
Direction des Systèmes d'Information
AC INFRASTRUCTURE
37 quai d'Orsay
75700 PARIS 07 SP

Le tableau suivant indique les coordonnées des entités responsables des PC des AC du Ministère.

| Rôle | Entité | Coordonnées |
|---|---|---|
| Entité juridique responsable | MAE - DSI | 37, quai d'Orsay<br>75007 Paris 07 SP |
| Personne physique responsable | Fabien FIESCHI - DSI | 37, quai d'Orsay<br>75007 Paris 07 SP |
| Entité gérant la conformité de la DPC avec la PC | COSSI | 37, quai d'Orsay<br>75007 Paris 07 SP |
| Entité représentant le Comité d'Approbation des Politiques de Certification | Nadir SOUABEG – RSSI | 37, quai d'Orsay<br>75007 Paris 07 SP |

*Tableau 1 : Points de contact de la Politique de Certification*

### 1.6.3 ENTITE DETERMINANT LA CONFORMITE D'UNE DPC AVEC CETTE PC

L'entité gérant la conformité de la DPC avec la présente politique de certification est le Comité SSI (COSSI).

### 1.6.4 PROCEDURES D'APPROBATION DE LA CONFORMITE DE LA DPC

L'entité approuvant la conformité de la DPC avec les PC Ministère est le Comité SSI (COSSI).

# 2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

## 2.1 ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

Le Directeur des Systèmes d'Information du Ministère est responsable de la mise à disposition des informations publiées.

Pour la mise à disposition des informations devant être publiées à destination des tiers utilisateurs de certificats, l'AC INFRASTRUCTURE N 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 DEVANT ETRE PUBLIEES

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

- la Politique de Certification de l'AC INFRASTRUCTURE N en cours de validité (le présent document) ;
- les versions antérieures de la présente Politique de Certification (PC « Client /Serveur SSL » et PC « Accès Distant »), tant que des certificats émis selon ces versions sont en cours de validité ;
- les gabarits des certificats des ACD, et des LCR émises par l'AC INFRASTRUCTURE N ;
- les certificats auto-signés de l'ACR, en cours de validité et les informations permettant aux tiers utilisateurs de certificats de s'assurer de l'origine de ces certificats (empreintes) ;
- la LCR en cours de validité, conforme au profil indiqué en partie 7 et accessible par le protocole http ;
- l'adresse (URL) permettant d'obtenir des informations concernant l'AC RACINE DIPLOMATIE à laquelle sont rattachées les ACD ;
- le certificat de l'AC RACINE DIPLOMATIE ;
- le certificat de l'AC INFRASTRUCTURE N.

| Information publiée | Emplacement de publication |
|---|---|
| PC | http://crl.diplomatie.gouv.fr |
| LCR | http://crl.diplomatie.gouv.fr |
| Certificat de l'AC INFRASTRUCTURE N | http://crl.diplomatie.gouv.fr |
| Certificat de l'AC RACINE DIPLOMATIE | http://crl.diplomatie.gouv.fr |
| Information permettant aux utilisateurs de s'assurer de l'origine du certificat de l'AC INFRASTRUCTURE N | http://crl.diplomatie.gouv.fr |

*Tableau 2 : Liste des informations publiées*

## 2.3 DELAIS ET FREQUENCES DE PUBLICATION

Les informations documentaires publiées sont mises à jour après chaque modification dans un délai de 24 heures après leur validation.

La fréquence de mise à jour des LCR est au minimum de 72 heures.

Les délais de publication et la disponibilité de l'information 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. |
| **Certificats des ACD** | |
| Délais de publication : | Ceux-ci sont diffusés préalablement à toute diffusion de certificats de service applicatif 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 : | Délai maximum de publication d'une LCR après génération : 30 minutes<br>Fréquence minimale de publication des LCR : 72 heures |
| Disponibilité de l'information : | Les exigences portant sur la fonction de publication de ces informations sont définies à la partie 6.10<br>La durée maximale d'indisponibilité par interruption de service (panne ou maintenance) est de 8 heures (jours ouvrés) et la durée totale maximale d'indisponibilité par mois est de 32 heures (jours ouvrés), ceci hors cas de force majeure. |

## 2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'ensemble des informations publiées à destination des services applicatifs et des utilisateurs de certificats est en accès libre. Le personnel chargé de la modification des données publiées est spécifiquement habilité à réaliser l'opération. L'attribution et la gestion de ces habilitations sont décrites dans la DPC.

L'information publiée est accessible avec accès en lecture seulement sur le site Internet du Ministère, aux adresses suivantes :

- pour la publication des LCR des AC : http://crl.diplomatie.gouv.fr ;
- pour les autres informations : http://crl.diplomatie.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, basé sur une politique de gestion stricte des mots de passe.

# 3 IDENTIFICATION ET AUTHENTIFICATION

## 3.1 NOMMAGE

### 3.1.1 TYPES DE NOMS

Dans chaque certificat conforme à la norme [X.509], l'AC émettrice (issuer) et le service applicatif de cachet ou d'authentification du serveur (subject) sont identifiés par un "Distinguished Name" (DN) répondant aux exigences de la norme [X.501].

### 3.1.2 NECESSITE D'UTILISATION DE NOMS EXPLICITES

Les noms choisis pour désigner les services applicatifs dans les certificats sont explicites. L'identification de l'entité à laquelle le service applicatif est rattaché est obligatoire.

#### 3.1.2.1 CERTIFICAT DE PROFIL « ACCES DISTANT»

Concernant les DN des services applicatifs, la composition du champ DN pour service applicatif du Ministère est décrite ci-dessous :

| Attribut | Valeur |
|---|---|
| **Nom du service applicatif (Attribut « CN »)** | objetldap@diplomatie.gouv.fr<br>• Dans le cas d'un poste Itinéo : itineoxxxx@diplomatie.gouv.fr avec xxx valant le numéro IMMO du poste Itinéo<br>• Dans le cas d'un boitier : boîtier XXXX où XXXX désigne l'identifiant du boitier<br>• Dans le cas d'une tablette dPad : Prénom NOM du détenteur de l'équipement.<br>• Dans le cas d'un smartphone dPhone : Prénom NOM du détenteur de l'équipement.<br>• Dans le cas d'un composant technique XXXX où XXXX désigne l'identifiant du composant<br>• Dans le cas d'un service applicatif « Serveur SSL » le FQDN du serveur> |
| **Nom de l'Unité Organisationnelle (Attribut « OU »)** | 0002 12000601000025 |
| | MINISTERE DES AFFAIRES ETRANGERES |

| | |
|---|---|
| **Nom de l'Organisation (Attribut « O »)** | |
| **Pays (Attribut « C »)** | FR |
| **Adresse électronique** | objetldap@diplomatie.gouv.fr* |

*Tableau 3 : Composition des champs du DN profil « Accès distant »*

** un Connecteur SMTP entre le CN et l'adresse du titulaire du poste sera fait à l'attribution du poste Itinéo à un agent.*

#### 3.1.2.2 CERTIFICAT DE PROFIL « SERVEUR SSL » ET « CLIENT SSL »

La composition du champ DN pour un service applicatif « Serveur SSL » du Ministère est décrite ci-dessous :

| Attribut | Valeur |
|---|---|
| **Nom du service applicatif (Attribut « CN »)** | <FQDN du serveur> |
| **Nom de l'Unité Organisationnelle (Attribut « OU »)** | 0002 12000601000025 |
| **Nom de l'Organisation (Attribut « O »)** | MINISTERE DES AFFAIRES ETRANGERES |
| **Pays (Attribut « C »)** | FR |

*Tableau 4 : Composition des champs du DN pour un agent « profils Serveur SSL »*

La composition du champ DN pour un service applicatif « Client SSL » est décrite ci-dessous :

| Attribut | Valeur |
|---|---|
| **Nom du service applicatif (Attribut « CN »)** | <NOM du composant technique> |
| **Nom de l'Unité Organisationnelle (Attribut « OU »)** | 0002 12000601000025 |
| **Nom de l'Organisation (Attribut « O »)** | Ministère DES AFFAIRES ETRANGERES |

| | |
|---|---|
| **Pays (Attribut « C »)** | FR |

*Tableau 5 : Composition des champs du DN pour un externe (prestataire) « profil client SSL »*

#### 3.1.2.3 CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

La composition du champ DN pour un service applicatif du Ministère est décrite ci-dessous :

| Attribut | Valeur |
|---|---|
| **Nom du service applicatif (Attribut « CN »)** | [Nom de l'organisme].[Nom du bureau responsable du serveur].[Nom du service applicatif]<br>• Par exemple dans le cas de la signature de code dPad : MAE.IDA.dPad |
| **Nom de l'Unité Organisationnelle (Attribut « OU »)** | 0002 12000601000025 |
| **Nom de l'Organisation (Attribut « O »)** | MINISTERE DES AFFAIRES ETRANGERES |
| **Pays (Attribut « C »)** | FR |

*Tableau 6 : Composition des champs du DN « profil signature de code »*

#### 3.1.2.4 CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

La composition du champ DN pour un service applicatif du Ministère est décrite ci-dessous :

| Attribut | Valeur |
|---|---|
| **Nom du service applicatif (Attribut « CN »)** | [Nom de l'organisme].[Nom du bureau responsable du serveur].[Nom du service applicatif] |
| **Nom de l'Unité Organisationnelle (Attribut « OU »)** | 0002 12000601000025 |
| **Nom de l'Organisation (Attribut « O »)** | MINISTERE DES AFFAIRES ETRANGERES |
| | FR |

| | |
|---|---|
| **Pays (Attribut « C »)** | |

*Tableau 7 : Composition des champs du DN « profil signature de configuration »*
** un Connecteur SMTP entre le CN et l'adresse du titulaire du poste sera fait à l'attribution du poste Itinéo à un agent.*

#### 3.1.2.5 CERTIFICAT DE PROFIL « SIGNATURE JETON D'HORODATAGE »

La composition du champ DN pour un serveur du Ministère est décrite ci-dessous :

| Attribut | Valeur |
|---|---|
| **Nom du serveur (Attribut « CN »)** | dtss.diplomatie.gouv.fr |
| **Nom de l'Unité Organisationnelle (Attribut « OU »)** | 0002 12000601000025 |
| **Nom de l'Organisation (Attribut « O »)** | MINISTERE DES AFFAIRES ETRANGERES |
| **Pays (Attribut « C »)** | FR |
| **Adresse électronique** | assistance.dsi@diplomatie.gouv.fr |

*Tableau 8 : Composition des champs du DN « profil signature jeton d'horodatage »*

### 3.1.3 PSEUDONYMISATION OU ANONYMISATION DES SERVICES APPLICATIFS

Sans objet.

### 3.1.4 REGLES D'INTERPRETATION DES DIFFERENTES FORMES DE NOM

- « Accès distant » : Sur la base de la demande de certificats, l'opérateur d'AE renseigne ces éléments via l'interface d'AE de l'IGC, en respectant les règles de composition du DN (pas d'accent, pas de caractères spéciaux, nomenclature des CN, etc.)
- « Serveur et Client SSL » : Le responsable du composant technique fournit un formulaire de demande de certification avec les éléments identifiant le service applicatif et qui composent le DN. Sur la base de ce formulaire, l'opérateur d'AE renseigne ces éléments via l'interface d'AE de l'IGC, en respectant les règles de composition du DN (pas d'accent, pas de caractères spéciaux).
- «Signature de configuration » : Le contenu du DN s'appuie sur le nom de l'organisation utilisatrice du certificat, du bureau responsable du service applicatif à faire signer ainsi que sur le nom de ce dernier.

- «Signature de code » : Le contenu du DN s'appuie sur le nom de l'organisation utilisatrice du certificat, du bureau responsable du service applicatif à faire signer et du nom de ce dernier.
- « Signature de jetons d'horodatage » : Le contenu du DN du certificat s'appuie le FQDN du serveur informatique tiers porteur de certificats.

### 3.1.5 UNICITE DES NOMS

Le champ DN est unique. La méthode mise en place pour assurer cette unicité est décrite dans la DPC.

### 3.1.6 IDENTIFICATION, AUTHENTIFICATION ET ROLE DE MARQUES DEPOSEES

Sans objet.

## 3.2 VALIDATION INITIALE DE L'IDENTITE

Focus sur les profils suivants :

- Certificat de profil « Accès distant» :

  Un certificat établit un lien de confiance entre le Porteur d'un certificat et la clé publique qui y figure. La bi-clé est générée par un dispositif technique opéré par l'Autorité d'Enregistrement. L'Autorité d'Enregistrement s'assure que le service applicatif identifié dans le certificat est bien en possession de la clé privée.

- Certificat de profil « Signature jeton d'horodatage » :

  L'enregistrement d'un service de création de signature de jetons d'horodatage d'une entité auquel un certificat doit être délivré se fait via l'enregistrement du RC correspondant.

  Un RC peut être amené à changer en cours de validité du certificat de signature de jetons d'horodatage correspondant (cf. chapitre 1.3.3), dans ce cas, tout nouveau RC doit également faire l'objet d'une procédure d'enregistrement.

  L'enregistrement d'un RC, et du serveur informatique correspondant se fait directement auprès de l'AE.

  La validation initiale de l'identité d'une entité ou d'une personne physique est ainsi réalisée dans les cas suivants :

  - Enregistrement d'un RC pour un certificat de signature de jeton d'horodatage : validation par l'AE de l'identité "personne morale" de l'entité de rattachement du RC, de l'identité "personne physique" du futur RC, de son habilitation à être RC pour le service de signature de jeton d'horodatage et pour l'entité considérée.
  - Enregistrement d'un nouveau RC pour un certificat de signature de jetons d'horodatage déjà émis : validation par l'AE de l'identité "personne physique" du futur RC et de son habilitation à être RC pour le service de création de jetons d'horodatage considéré et pour l'entité considérée.

  Pour des raisons de simplicité de présentation, ces différents cas sont regroupés dans le chapitre 3.2.3.

### 3.2.1 METHODES POUR PROUVER LA POSSESSION DE LA CLE PRIVEE

#### 3.2.1.1 CERTIFICAT DE PROFIL « ACCES DISTANT»

Un certificat établit un lien de confiance entre le Porteur d'un certificat et la clé publique qui y figure. La bi-clé est générée par un dispositif technique opéré par l'Autorité d'Enregistrement. L'Autorité d'Enregistrement s'assure que le service applicatif identifié dans le certificat est bien en possession de la clé privée.

#### 3.2.1.2 CERTIFICAT DE PROFIL « SERVEUR SSL » ET « CLIENT SSL »

Un certificat établit un lien de confiance entre le Porteur d'un certificat et la clé publique qui y figure. La bi-clé est générée par un dispositif technique opéré par l'Autorité d'Enregistrement. L'Autorité d'Enregistrement s'assure que le service applicatif identifié dans le certificat est bien en possession de la clé privée.

Dans le cas où la bi-clé n'est pas générée par l'AC, le responsable du composant technique doit alors fournir à l'AC, via l'équipe chargée de la validation des demandes de certificats, une preuve de possession de la clé privée correspondant à la clé publique contenue dans la demande de certificat d'authentification.

#### 3.2.1.3 CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

L'AC transmet au Responsable de Certificat identifié dans le dossier de demande le certificat le certificat et la bi-clé associée au format PKCS#12.

#### 3.2.1.4 CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

La bi-clé peut être générée par l'AC en central ou en local.

Dans le cas d'une génération en central, l'AC transmet au RC identifié dans le dossier de demande le certificat.

Dans la cas d'une génération en local, le RC fournit alors à l'AE un moyen de vérifier qu'il est bien en possession de la clé privée. La méthode utilisée est décrite dans la DPC.

#### 3.2.1.5 CERTIFICAT DE PROFIL « SIGNATURE JETON D'HORODATAGE »

Lorsque la bi-clé du serveur n'est pas générée par l'AC, le RC doit alors fournir à l'AC une preuve de possession de la clé privée correspondant à la clé publique contenue dans la demande de certificat de signature de jetons d'horodatage.

### 3.2.2 VALIDATION DE L'IDENTITE D'UNE ENTITE

Cf. chapitre 3.2.3

### 3.2.3 VALIDATION DE L'IDENTITE D'UN INDIVIDU

La validation initiale de l'identité d'un service applicatif ou d'un RC fonde la confiance portée aux certificats émis par le Ministère.

#### 3.2.3.1 CERTIFICAT DE PROFIL « ACCES DISTANT»

**Boîtiers NETASQ**

Le principe de validation repose sur l'IDA DCG si le boîtier est implémenté en administration centrale. Et il repose sur l'IDA DET si le boîtier est implémenté à l'étranger.

**Postes Itinéo, tablettes dPad et smartphones dPhone**

Le principe de validation repose sur une validation en amont par le responsable hiérarchique puis une validation en aval par l'IDA/DCG responsable de l'attribution du matériel

*3.2.3.1.1 Responsable d'un boîtier NETASQ*

Les demandeurs de boîtiers NetASQ (personnes ou entités) doivent être connus de l'IDA DCG/DET afin que celle-ci puisse vérifier leur habilitation à adresser des demandes.

Pour ce faire, l'IDA DCG/DET a pour responsabilité de :

- vérifier l'identité du demandeur ainsi que son habilitation à demander un certificat pour le composant technique ;
- vérifier le DN du boîtier auquel le certificat doit être rattaché (à minima, respect des politiques de nommage au sein du Ministère) ;
- vérifier la cohérence des justificatifs présentés ;
- s'assurer que le demandeur a pris connaissances des modalités applicables pour l'utilisation du certificat (Conditions Générales d'Utilisation).

Un formulaire les identifiant est remis à l'IDA DET/DCG.
La vérification d'identité peut se faire par la signature électronique via la messagerie sécurisée.

*3.2.3.1.2 Titulaire d'un poste Itinéo*

Le titulaire doit être connu par l'entité IDA DCG/DET afin que celle-ci puisse vérifier son habilitation à demander un certificat. Elle doit vérifier également que la demande a été validée en amont par le responsable hiérarchique du titulaire.

*3.2.3.1.3 Titulaire d'une tablette dPad*

Le titulaire doit être connu par le service de proximité (infogérant du Ministère) et par l'entité IDA DCG afin que celle-ci puisse valider l'attribution d'une tablette dPad. IDA/DCG doit également vérifier que la demande a été validée en amont par le responsable hiérarchique du titulaire avant de valider l'attribution d'une tablette dPad et de la carte microSD sur laquelle sera stocké le certificat.

*3.2.3.1.4 Titulaire d'un smartphone dPhone*

Le titulaire doit être connu par le service de proximité (infogérant du Ministère) et par l'entité IDA DCG afin que celle-ci puisse valider l'attribution d'un smartphone dPhone. IDA/DCG doit également vérifier que la demande a été validée en amont par le responsable hiérarchique du titulaire avant de valider l'attribution d'un smartPhone dPhone et de la carte microSD sur laquelle sera stocké le certificat.

### 3.2.3.2 CERTIFICAT DE PROFIL « SERVEUR SSL » ET « CLIENT SSL »

Le principe de validation repose sur l'équipe chargée de la validation des demandes de certificats.

Sont considérés comme individus les responsables des composants techniques et les membres de l'équipe chargée de la validation des demandes de certificats.

#### *3.2.3.2.1 Enregistrement d'un Responsable d'un composant technique*

Les responsables des composants techniques doivent être connus de l'équipe chargée de la validation des demandes de certificats afin que celle-ci puisse vérifier leur habilitation à adresser des demandes.

Pour ce faire, l'équipe chargée de la validation des demandes a pour responsabilité de :

- vérifier l'identité du demandeur ainsi que son habilitation à demander un certificat pour le composant technique ;
- vérifier le FQDN du serveur auquel le certificat doit être rattaché (à minima, respect des politiques de nommage au sein du Ministère) ;
- vérifier la cohérence des justificatifs présentés ;
- s'assurer que le demandeur a pris connaissances des modalités applicables pour l'utilisation du certificat (Conditions Générales d'Utilisation).

Un formulaire les identifiant est remis à l'équipe chargée de la validation des demandes.
La vérification d'identité peut se faire par la signature électronique via la messagerie sécurisée.

#### *3.2.3.2.2 Enregistrement d'un membre de l'équipe chargée de la validation des demandes*

Les membres de l'équipe chargée de la validation des demandes sont désignés par un responsable hiérarchique et renseignés dans un formulaire.

Ce formulaire est diffusé aux opérateurs d'AE.

### 3.2.3.3 CERTIFICAT DE PROFIL « SIGNATURE DE CODE » ET « SIGNATURE DE CONFIGURATION »

Sont considérés comme individus les responsables de certificats amenés à demander un certificat de signature de code.

#### *3.2.3.3.1 Enregistrement d'un responsable de certificat*

Un responsable de certificat représentant une entité nécessite l'identification de cette entité, l'identification du Responsable de certificat en tant que personne physique, ainsi que son habilitation à être responsable de certificat pour le service applicatif considéré.

Pour ce faire, l'AE ou l'équipe en charge de la validation des demandes a pour responsabilité de :

- vérifier l'identité du demandeur ainsi que son habilitation à demander un certificat de signature de code pour le service applicatif qu'il représente ;
- vérifier le service applicatif auquel le certificat de signature sera rattaché (à minima, respect des politiques de nommage au sein du Ministère) ;

- vérifier la cohérence des justificatifs présentés ;
- s'assurer que le demandeur a pris connaissances des modalités applicables pour l'utilisation du certificat (Conditions Générales d'Utilisation).

Un formulaire les identifiant est remis directement aux opérateurs d'Autorité d'Enregistrement en mettant a minima en copie l'équipe en charge de la validation.

La vérification d'identité peut se faire par la signature électronique via la messagerie sécurisée.

*3.2.3.3.2 Enregistrement de l'équipe chargée de la validation des demandes*

Les membres de l'équipe chargée de la validation des demandes sont désignés par un responsable hiérarchique et renseignés dans un formulaire.

Ce formulaire est diffusé aux opérateurs d'AE.

### 3.2.3.4 CERTIFICAT DE PROFIL « SIGNATURE JETON D'HORODATAGE »

*3.2.3.4.1 Enregistrement d'un RC pour un certificat de signature de jetons d'horodatage à émettre*

L'enregistrement du futur RC (personne physique) représentant une entité nécessite l'identification de cette entité et l'identification de la personne physique. S'agissant d'un certificat de signature de jetons d'horodatage, le RC est, de plus, habilité en tant que RC pour le service de création de signature de jetons d'horodatage considéré.
Le dossier d'enregistrement, déposé directement auprès de l'AE, doit au moins comprendre :

- une demande de certificat écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le nom du service de création de signature de jetons d'horodatage concerné par cette demande;
- un mandat, daté de moins de 3 mois, désignant le futur RC comme étant habilité à être RC pour le service de création de signature de jetons d'horodatage pour lequel le certificat de signature de jetons d'horodatage doit être délivré. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RC ;
- une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative ;
- un document officiel d'identité en cours de validité du futur RC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie ;
- les conditions générales d'utilisation signées.

*Nota* - Le RC est informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il est convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

L'authentification du RC se fait notamment :

- Soit par l'envoi du dossier papier à l'AE accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, RC) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original") ;
- Soit via une demande d'enregistrement dématérialisée signée électroniquement par le futur RC à l'aide du procédé de signature électronique du MAE et que la signature soit vérifiée et valide au moment de l'enregistrement ;

- Soit par la communication d'un élément propre au futur RC permettant de l'identifier au sein d'une base de données administrative préétablie.

*3.2.3.4.2 Enregistrement d'un nouveau RC pour un certificat de signature de jetons d'horodatage déjà émis*

Dans le cas de changement d'un RC en cours de validité d'un certificat de signature de jetons d'horodatage, le nouveau RC est enregistré en tant que tel par l'AC en remplacement de l'ancien RC.

L'enregistrement du nouveau RC (personne physique) représentant une entité nécessite l'identification de la personne physique et la vérification de son habilitation en tant que représentant de l'entité à laquelle le service de création de signature de jetons d'horodatage est rattaché et en tant que RC pour ce service.

Le dossier d'enregistrement, déposé directement auprès de l'AE, comprend au moins :

- un mandat, daté de moins de 3 mois, désignant le futur RC comme étant habilité à être le nouveau RC pour le service de création de signature de jetons d'horodatage auquel le certificat a été délivré, en remplacement du RC précédent. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RC ;
- une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative ;
- un document officiel d'identité en cours de validité du futur RC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie ;
- les conditions générales d'utilisation signées.

*Nota* - Le RC est informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

L'authentification du RC se fait :

- Soit par l'envoi du dossier papier à l'AE accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, RC) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original") ;
- Soit via une demande d'enregistrement dématérialisée signée électroniquement par le futur RC à l'aide du procédé de signature électronique du MAE et que la signature soit vérifiée et valide au moment de l'enregistrement ;
- Soit par la communication d'un élément propre au futur RC permettant de l'identifier au sein d'une base de données administrative préétablie.

### 3.2.4 INFORMATIONS NON VERIFIEES DU RC ET DU SERVICE APPLICATIF

Aucune information non vérifiée n'est enregistré dans le dossier du RC ni introduite dans les certificats.

### 3.2.5 VALIDATION DE L'AUTORITE DU DEMANDEUR

La validation de l'autorité du demandeur est effectuée par l'Autorité d'Enregistrement.

## 3.3 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DE CLES

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

### 3.3.1 IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT COURANT

Lors du premier renouvellement, la vérification de l'identité du RC et des informations du serveur informatique correspondant est optionnelle. Elle est laissée à l'appréciation de l'AC qui engage sa responsabilité quant à la validité des informations contenues dans le certificat renouvelé.

Lors du renouvellement suivant, l'AE, saisie de la demande, identifiera le RC et vérifiera les informations du serveur informatique selon la même procédure que pour l'enregistrement initial ou une procédure offrant un niveau de garantie équivalent.

### 3.3.2 IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT APRES REVOCATION

Le processus de renouvellement de certificat est le même que le processus de demande initiale de certificat.

## 3.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

Pour des raisons précisées dans la partie 4.9.1 les certificats des services applicatifs peuvent être révoqués.

#### 3.4.1.1 CERTIFICAT DE PROFIL « ACCES DISTANT»

**Boîtiers NETASQ**

Le responsable d'un boîtier adresse sa demande de révocation à l'ACSSI par téléphone ou par courriel signé.

**Postes Itinéo**

Le titulaire du poste ou son responsable hiérarchique peuvent appeler la hotline (pour signaler, une perte, un vol ou une casse notamment) et demander la révocation du certificat « accès distant » ou bien le Correspondant SI peut s'adresser par téléphone ou par courrier signé au Centre de Transmission Diplomatique (CTD) ou à l'ACSSI pour formuler une demande de révocation.

**Tablettes dPad**

Le titulaire de la tablette peut appeler le Service de proximité (infogérant) ou le Centre de Transmission Diplomatique en dehors des heures ouvrables pour demander la révocation du certificat « Accès Distant ». Le service de proximité est alors en charge d'effectuer la demande de révocation auprès de l'opérateur d'AE. Si le titulaire de la tablette dPad est à l'étranger, il peut se rapprocher du Correspondant SI qui adressera une demande de révocation par courriel signé ou téléphone au Centre de Transmission Diplomatique.

**Smartphones dPhone**

Le titulaire du smartphone peut appeler le Service de proximité (infogérant) ou le Centre de Transmission Diplomatique en dehors des heures ouvrables pour demander la révocation du certificat « Accès Distant ». Le service de proximité est alors en charge d'effectuer la demande de révocation auprès de l'opérateur d'AE. Si le titulaire du smartphone dPhone est à l'étranger, il peut se rapprocher du Correspondant SI qui adressera une demande de révocation par courriel signé ou téléphone au Centre de Transmission Diplomatique.

**Composants techniques et serveurs**

Le responsable d'un composant technique fait sa demande de révocation directement à l'AE ou via son l'équipe chargée de la validation des demandes. Dans ce cas, celle-ci est alors responsable de transmettre la demande à l'AE.

Les tableaux suivants présentent la façon dont sont identifiés les demandeurs autorisés à formuler cette demande de révocation, en fonction du moyen mis à disposition pour effectuer cette demande de révocation.

| Moyen | Demandeur autorisé | Authentification du demandeur | Opérateur de révocation |
|---|---|---|---|
| Appel téléphonique à la Hotline | Le titulaire du poste ou son responsable hiérarchique | Vérification du droit à demander la révocation | Hotline |
| Courriel signé adressé au CTD | Le correspondant SI | Vérification du droit à demander la révocation | CTD |
| Courriel signé adressé aux ACSSI | Le correspondant SI | Vérification du droit à demander la révocation | ACSSI |

Tableau 9 : Identification et validation d'une demande de révocation d'un certificat poste Itinéo

| Moyen | Demandeur autorisé | Authentification du demandeur | Opérateur de révocation |
|---|---|---|---|
| Appel téléphonique ou courriel signé adressé au CTD | Le titulaire de la tablette ou du smartphone ou son responsable hiérarchique | Vérification du droit à demander la révocation | CTD |
| Appel téléphonique ou courriel signé adressé aux ACSSI | Le titulaire de la tablette ou du smartphone ou son responsable hiérarchique ou le service de proximité | Vérification du droit à demander la révocation | ACSSI |

Tableau 10 : Identification et validation d'une demande de révocation d'un certificat tablette dPad ou smartphone dPhone

| Moyen | Demandeur autorisé | Authentification du demandeur | Opérateur de révocation |
|---|---|---|---|
| Courriel signé adressé aux ACSSI<br>Par téléphone | Le Responsable Boîtier | Vérification du droit à demander la révocation | ACSSI |

Tableau 11 : Identification et validation d'une demande de révocation d'un certificat boîtier

| Moyen | Demandeur autorisé | Authentification du demandeur | Opérateur de révocation |
|---|---|---|---|
| Appel téléphonique aux ACSSI | Le responsable d'un composant technique ou l'équipe chargée de la validation des demandes | Vérification du droit à demander la révocation | ACSSI |
| Fax / Formulaire adressé aux ACSSI | Le responsable d'un composant technique ou l'équipe chargée de la validation des demandes | Vérification du droit à demander la révocation | ACSSI |
| Courriel signé adressé aux ACSSI | Le responsable d'un composant technique ou l'équipe chargée de la validation des demandes | Vérification du droit à demander la révocation | ACSSI |

Tableau 12 : Identification et validation d'une demande de révocation d'un certificat client SSL et Serveur SSL

#### 3.4.1.2 CERTIFICAT DE PROFIL « SERVEUR SSL » ET « CLIENT SSL »

Le tableau suivant présente la façon dont sont identifiés les demandeurs autorisés à formuler cette demande de révocation, en fonction du moyen mis à disposition pour effectuer cette demande de révocation.

Le responsable d'un composant technique fait sa demande de révocation directement à l'AE ou via son l'équipe chargée de la validation des demandes. Dans ce cas, celle-ci est alors responsable de transmettre la demande à l'AE.

| Moyen | Demandeur autorisé | Authentification du demandeur | Opérateur de révocation |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Appel téléphonique aux ACSSI | Le responsable d'un composant technique ou l'équipe chargée de la validation des demandes | Vérification du droit à demander la révocation | ACSSI |
| Fax / Formulaire adressé aux ACSSI | Le responsable d'un composant technique ou l'équipe chargée de la validation des demandes | Vérification du droit à demander la révocation | ACSSI |
| Courriel signé adressé aux ACSSI | Le responsable d'un composant technique ou l'équipe chargée de la validation des demandes | Vérification du droit à demander la révocation | ACSSI |

Tableau 13 : Identification et validation d'une demande de révocation

#### 3.4.1.3 CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

Le responsable du certificat fait sa demande de révocation directement à l'AE en mettant en copie l'équipe chargée de la validation des demandes.

Les tableaux suivants présentent la façon dont sont identifiés les demandeurs autorisés à formuler cette demande de révocation, en fonction du moyen mis à disposition pour effectuer cette demande de révocation.

| Moyen | Demandeur autorisé | Authentification du demandeur | Opérateur de révocation |
|---|---|---|---|
| Fax / Formulaire adressé aux ACSSI | Le responsable du certificat ou l'équipe chargée de la validation des demandes | Vérification du droit à demander la révocation | ACSSI |
| Courriel signé adressé aux ACSSI | Le responsable du certificat ou l'équipe chargée de la validation des demandes | Vérification du droit à demander la révocation | ACSSI |

Tableau 14 : Identification et validation d'une demande de révocation d'un certificat Signature de Code

#### 3.4.1.4 CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

Le responsable du certificat fait sa demande de révocation directement à l'AE en mettant en copie l'équipe chargée de la validation des demandes.

Les tableaux suivants présentent la façon dont sont identifiés les demandeurs autorisés à formuler cette demande de révocation, en fonction du moyen mis à disposition pour effectuer cette demande de révocation.

| Moyen | Demandeur autorisé | Authentification du demandeur | Opérateur de révocation |
|---|---|---|---|
| Fax / Formulaire adressé aux ACSSI | Le responsable du certificat ou l'équipe chargée de la validation des demandes | Vérification du droit à demander la révocation | ACSSI |
| Courriel signé adressé aux ACSSI | Le responsable du certificat ou l'équipe chargée de la validation des demandes | Vérification du droit à demander la révocation | ACSSI |

Tableau 15 : Identification et validation d'une demande de révocation d'un certificat Signature de Configuration

#### 3.4.1.5 CERTIFICAT DE PROFIL « SIGNATURE JETON D'HORODATAGE »

Une demande de révocation doit être faite par courrier ou par télécopie. Elle doit alors être signée par le demandeur et le service de gestion des révocations doit s'assurer de l'identité du demandeur (vérification de la signature manuscrite par rapport à une signature préalablement enregistrée) et de son autorité par rapport au certificat à révoquer.

# 4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

## 4.1 DEMANDE DE CERTIFICAT

### 4.1.1 ORIGINE D'UNE DEMANDE DE CERTIFICAT

#### 4.1.1.1 CERTIFICAT DE PROFIL « ACCES DISTANT»

**Postes Itinéo**

Une demande de certificat ne peut être faite que par le titulaire du poste lui-même ou son responsable hiérarchique ou la secrétaire lorsque le titulaire est situé à l'administration centrale. Pour les titulaires situés à l'étranger, une demande de certificat ne peut être faite que par le correspondant SI.

**Tablettes dPad**

En amont de la demande de certificat, la demande d'équipement d'un agent du Ministère passe par IDA/DCG qui valide l'attribution d'une tablette et d'une carte microSD. Ces éléments sont alors fournis au service de proximité). La demande de certificat provient par la suite du service de proximité (infogérant) en charge des tablettes et est adressée à IDA/DCG qui la vérifie avant de la transmettre à l'opérateur d'AE.

**Smartphones dPhone**

En amont de la demande de certificat, la demande d'équipement d'un agent du Ministère passe par IDA/DCG qui valide l'attribution d'un smartphone et d'une carte microSD. Ces éléments sont alors fournis au service de proximité). La demande de certificat provient par la suite du service de proximité (infogérant) en charge des smartphones et est adressée à IDA/DCG qui la vérifie avant de la transmettre à l'opérateur d'AE.

**Boîtiers NETASQ**

Une demande de certificat ne peut être adressée à l'Autorité d'Enregistrement que via IDA/DCG/DET, cette ayant reçu la demande via une entité ou un poste demandeur à l'étranger ou en administration centrale.

**Composants techniques et serveurs**

Une demande de certificat ne peut être adressée à l'Autorité d'Enregistrement que via l'équipe chargée de la validation des demandes de certificats du futur Porteur.

#### 4.1.1.2 CERTIFICAT DE PROFIL « SERVEUR SSL » ET « CLIENT SSL »

Une demande de certificat ne peut être adressée à l'Autorité d'Enregistrement que via l'équipe chargée de la validation des demandes de certificats du futur Porteur.

#### 4.1.1.3 CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

Une demande de certificat est adressée par le Responsable de Certificat à l'Autorité d'Enregistrement en mettant en copie l'équipe en charge de la validation des demandes.

#### 4.1.1.4 CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

Une demande de certificat est adressée par le Responsable du certificat à l'Autorité d'Enregistrement en mettant en copie l'équipe d'habilitation en charge de la validation des demandes.

#### 4.1.1.5 CERTIFICAT DE PROFIL « SIGNATURE JETON D'HORODATAGE »

Un certificat peut être demandé par un représentant légal de l'entité dûment mandaté pour cette entité, avec dans tous les cas consentement préalable du futur RC.

### 4.1.2 PROCESSUS ET RESPONSABILITES POUR L'ETABLISSEMENT D'UNE DEMANDE DE CERTIFICAT

#### 4.1.2.1 CERTIFICAT DE PROFIL « ACCES DISTANT»

**Postes Itinéo**

Le demandeur de poste Itinéo contacte la hotline pour une demande de poste Itinéo qui transmet la demande via ITSM à l'IDA. Cette dernière se charge de valider la demande et de la transmettre à l'ACSSI (Opérateur d'AE).

**Tablettes dPad**

Le service de proximité transmet une demande de certificat pour la tablette dPad via ITSM à IDA/DCG. Cette dernière se charge de valider la demande et de la transmettre au service des ACSSI (Opérateur d'AE).

**Smartphones dPhone**

Le service de proximité transmet une demande de certificat pour le smartphone dPhone via ITSM à IDA/DCG. Cette dernière se charge de valider la demande et de la transmettre au service des ACSSI (Opérateur d'AE).

**Boîtiers NETASQ**

Le demandeur de boîtier NetASQ remplit une demande de certificat au format électronique qu'il transmet par courriel signé à l'IDA DET/DCG.
L'IDA valide la demande et notifie via ITSM l'opérateur d'AE (ACSSI).

Un opérateur d'AE se charge de l'authentifier et de valider la demande.

**Composants techniques et serveurs**

*4.1.2.1.1 GENERATION DE LA CLE PRIVEE EN CENTRAL, AU NIVEAU DE L'AC INFRASTRUCTURE N*

Le responsable du composant technique remplit une demande de certificat au format électronique qu'il transmet par courriel à l'équipe chargée de la validation des demandes, accepte les Conditions Générales d'Utilisation de certificats en joignant une reconnaissance de lecture des Conditions Générales d'Utilisation et signe le courriel à l'aide son certificat de signature.
Un membre de l'équipe chargée de la validation des demandes de certificats co-signe la demande en envoyant un courriel signé à la boîte aux lettres commune des opérateurs d'AE (en copie, un responsable de l'équipe chargée des validations).
Un opérateur d'AE se charge de l'authentifier et de valider la demande.

#### *4.1.2.1.2 GENERATION DE LA CLE PRIVEE EN LOCAL, SUR LE COMPOSANT TECHNIQUE*

Le responsable du composant technique génère la clé privée et la requête de certificat (PKCS#10) sur le composant technique. Il effectue ensuite une demande auprès de l'équipe chargée de la validation des demandes par courriel signé contenant les documents justificatifs et le fichier PKCS#10 accompagnés d'une reconnaissance de lecture des Conditions Générales d'Utilisation signée.
L'équipe chargée de la validation des demandes de certificats co-signe la demande en envoyant un courriel signé à la boîte aux lettres commune des opérateurs d'AE qui se charge de l'authentifier et de valider la demande.

### 4.1.2.2 CERTIFICAT DE PROFIL « SERVEUR SSL » ET « CLIENT SSL »

#### *4.1.2.2.1 Génération de la clé privée en central, au niveau de l'AC INFRASTRUCTURE N*

Le responsable du composant technique remplit une demande de certificat au format électronique qu'il transmet par courriel à l'équipe chargée de la validation des demandes, accepte les Conditions Générales d'Utilisation de certificats en joignant une reconnaissance de lecture des Conditions Générales d'Utilisation et signe le courriel à l'aide son certificat de signature.

Un membre de l'équipe chargée de la validation des demandes de certificats co-signe la demande en envoyant un courriel signé à la boîte aux lettres commune des opérateurs d'AE (en copie, un responsable de l'équipe chargée des validations).

Un opérateur d'AE se charge de l'authentifier et de valider la demande.

#### *4.1.2.2.2 Génération de la clé privée en local, sur le composant technique*

Le responsable du composant technique génère la clé privée et la requête de certificat (PKCS#10) sur le composant technique. Il effectue ensuite une demande auprès de l'équipe chargée de la validation des demandes par courriel signé contenant les documents justificatifs et le fichier PKCS#10 accompagnés d'une reconnaissance de lecture des Conditions Générales d'Utilisation signée.

L'équipe chargée de la validation des demandes de certificats co-signe la demande en envoyant un courriel signé à la boîte aux lettres commune des opérateurs d'AE qui se charge de l'authentifier et de valider la demande.

#### 4.1.2.3 CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

Le responsable du certificat remplit une demande de certificat qu'il transmet par courriel à l'Autorité d'Enregistrement (via la boîte aux lettres commune des opérateurs d'AE) en mettant en copie l'équipe chargée de la validation des demandes, accepte les Conditions Générales d'Utilisation de certificats en joignant une reconnaissance de lecture des CGU et signe le courriel à l'aide son certificat de signature.

Un opérateur d'AE se charge d'authentifier et de valider la demande.

#### 4.1.2.4 CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

##### *4.1.2.4.1 Génération de la clé privée en central, au niveau de l'AC INFRASTRUCTURE N*

Le responsable du certificat remplit une demande de certificat au format électronique qu'il transmet par courriel à l'Autorité d'Enregistrement (via la boîte aux lettres commune des opérateurs d'AE) en mettant en copie l'équipe chargée de la validation des demandes, accepte les Conditions Générales d'Utilisation de certificats en joignant une reconnaissance de lecture des CGU et signe le courriel à l'aide son certificat de signature.

Un opérateur d'AE se charge d'authentifier et de valider la demande.

##### *4.1.2.4.2 Génération de la clé privée en local, sur le composant technique*

Le responsable du certificat génère la clé privée et la requête de certificat (PKCS#10) via un utilitaire prévu à cet effet. Il effectue ensuite une demande auprès de l'Autorité d'enregistrement (via la boite mail des opérateurs d'AE) ou auprès de l'équipe chargée de la validation des demandes. Ce courriel est signé, contient les documents justificatifs et le fichier PKCS#10 accompagnés d'une reconnaissance de lecture des Conditions Générales d'Utilisation signée.

#### 4.1.2.5 CERTIFICAT DE PROFIL « SIGNATURE JETON D'HORODATAGE »

Les informations suivantes doivent au moins faire partie de la demande de certificat (cf. chapitre 3.2 ci-dessus) :

- le nom du service de création de signature de jetons d'horodatage à utiliser dans le certificat ;
- les données personnelles d'identification du RC ;
- les données d'identification de l'entité ;
- La CSR (Certificate Signing Request) signé par la bi-clé privée du serveur de signature.

Le dossier de demande est établi soit directement par le futur RC à partir des éléments fournis par son entité, soit par son entité et signé par le futur RC.

Par ailleurs, l'AE doit s'assurer de disposer d'une information permettant de contacter le futur RC du certificat.

## 4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

### 4.2.1 EXECUTION DES PROCESSUS D'IDENTIFICATION ET DE VALIDATION DE LA DEMANDE

#### 4.2.1.1 CERTIFICAT DE PROFIL « ACCES DISTANT»

**Postes Itinéo**

Pour les postes Itinéo, ce processus s'appuie sur la validation par l'entité IDA de la demande et de la légitimité du demandeur.

IDA vérifie que le poste Itinéo ne dispose pas de certificat valide (un seul certificat par poste par personne) puis déclenche le processus de demande via ITSM.

**Tablettes dPad et smartphones dPhone**

Pour les tablettes dPad et smartphones dPhone, ce processus s'appuie sur la validation par l'entité IDA/DCG de la demande et de la légitimité du demandeur.

IDA/DCG vérifie que le carte microSD associée ne dispose pas de certificat valide (un seul certificat par terminal), que l'identifiant de la carte microSD considérée est unique au sein du Ministère, puis déclenche le processus de demande via ITSM.

**Boîtiers NETASQ**

Une fois en possession de la demande de certificats, l'opérateur d'AE vérifie qu'elle provient de l'IDA et la renseigne dans l'interface d'AE de l'IGC.

L'AC INFRASTRUCTURE N émet alors le certificat.

#### 4.2.1.2 CERTIFICAT DE PROFIL « SERVEUR SSL » ET « CLIENT SSL »

Ce processus s'appuie sur la connaissance préalable par l'opérateur d'AE des membres de l'équipe chargée de la validation des demandes de certificats autorisés à transmettre les demandes pour les profils « Authentification Serveur / Client SSL ».

Une fois en possession de la demande de certificats (au format papier ou électronique), l'opérateur d'AE vérifie qu'elle provient de l'équipe chargée de la validation des demandes et la renseigne dans l'interface d'AE de l'IGC.

L'AC INFRASTRUCTURE N émet alors le certificat.

#### 4.2.1.3 CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

L'ACSSI s'assure que la demande de certificat provient bien d'un Responsable de Certificat dument authentifié et qui a autorité à effectuer une demande de certificat de profil signature de code.

#### 4.2.1.4 CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

L'ACSSI s'assure que la demande de certificat provient bien du RC.

#### 4.2.1.5 CERTIFICAT DE PROFIL « SIGNATURE JETON D'HORODATAGE »

Les identités "personne physique" et "personne morale" sont vérifiées conformément aux exigences du chapitre 3.2.

L'AE doit effectuer les opérations suivantes :

- valider l'identité du futur RC ;
- vérifier la cohérence des justificatifs présentés ;
- s'assurer que le futur RC a pris connaissance des modalités applicables pour l'utilisation du certificat (voir les conditions générales d'utilisation).

Une fois ces opérations effectuées, l'AE émet la demande de signature de la CSR transmise par le RC.

L'AE conserve ensuite une trace des justificatifs présentés :

- si le dossier est au format papier, sous la forme d'une photocopie signée à la fois par le futur RC et par l'AE les signatures étant précédées de la mention "copie certifiée conforme à l'original" ;

si le dossier est au format électronique, les différents justificatifs sous une forme électronique ayant valeur légale

### 4.2.2 ACCEPTATION OU REJET DE LA DEMANDE

#### 4.2.2.1 CERTIFICAT DE PROFIL « ACCES DISTANT»

L'IDA accepte les demandes émanant de demandeurs dûment autorisés, ayant fourni l'ensemble des éléments valides, cohérents et nécessaires à la demande.

Si l'une des informations fournie est erronée, l'IDA renvoie le dossier au demandeur pour mise à jour. Ils se réservent le droit de rejeter toute demande incomplète ou non conforme.

L'opérateur d'AE accepte uniquement les demandes émanant de l'IDA.

#### 4.2.2.2 CERTIFICAT DE PROFIL « SERVEUR SSL » ET « CLIENT SSL »

L'équipe chargée de la validation des demandes accepte les demandes émanant de demandeurs dûment autorisés, ayant fourni l'ensemble des éléments valides, cohérents et nécessaires à la demande et accepté les Conditions Générales d'Utilisation.

Si l'une des informations fournie est erronée, l'équipe chargée de la validation des demandes renvoie le dossier au demandeur pour mise à jour.

L'équipe chargée de la validation des demandes se réserve le droit de rejeter toute demande incomplète ou non conforme.

L'opérateur d'AE accepte les demandes émanant de l'équipe chargée de la validation des demandes.

#### 4.2.2.3 CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

L'AE accepte les demandes émanant de demandeurs dûment autorisés, ayant fourni l'ensemble des éléments valides, cohérents et nécessaires à la demande et accepté les Conditions Générales d'Utilisation.

#### 4.2.2.4 CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

L'AE accepte les demandes émanant de demandeurs dûment autorisés, ayant fourni l'ensemble des éléments valides, cohérents et nécessaires à la demande et accepté les Conditions Générales d'Utilisation.

#### 4.2.2.5 CERTIFICAT DE PROFIL « SIGNATURE JETON D'HORODATAGE »

En cas de rejet de la demande, l'AE en informe le RC en justifiant le rejet.

### 4.2.3 DUREE D'ETABLISSEMENT D'UN CERTIFICAT

#### 4.2.3.1 CERTIFICAT DE PROFIL « ACCES DISTANT»

La demande n'est pas traitée immédiatement en raison des divers intermédiaires de confiance.

Après validation de la demande par IDA, l'opérateur de l'AE (ACSSI) est notifié via ITSM.

L'établissement d'un certificat peut prendre quelques jours.

#### 4.2.3.2 CERTIFICAT DE PROFIL « SERVEUR SSL » ET « CLIENT SSL »

La demande passant par l'équipe chargée de la validation des demandes de certificats, puis par un opérateur d'AE, n'est pas faite de façon immédiate. L'établissement d'un certificat peut prendre quelques jours.

#### 4.2.3.3 CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

La demande passant par un opérateur d'AE, n'est pas faite de façon immédiate. L'établissement d'un certificat peut prendre quelques jours.

#### 4.2.3.4 CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

La demande passant par un opérateur d'AE, n'est pas faite de façon immédiate. L'établissement d'un certificat peut prendre quelques jours.

#### 4.2.3.5 CERTIFICAT DE PROFIL « SIGNATURE JETON D'HORODATAGE »

La présente PC ne formule pas d'exigence spécifique sur le sujet. À préciser par l'AC dans sa PC, en visant une durée d'établissement la plus courte possible.

## 4.3 DELIVRANCE DU CERTIFICAT

### 4.3.1 ACTIONS DE L'AC CONCERNANT LA DELIVRANCE DU CERTIFICAT

#### 4.3.1.1 CERTIFICAT DE GABARIT « ACCES DISTANT »

À chaque demande de certificat, l'AC effectue les opérations suivantes :

- authentification du demandeur (Autorité d'Enregistrement);
- vérification de l'intégrité de la demande;
- vérification technique de la demande;
    - création du certificat et de la bi-clé du futur Porteur;

- signature du certificat à l'aide de la clé privée de l'AC;

- envoi du certificat et de la bi-clé au format PKCS#12 protégé par un mot de passe en pièce jointe d'un courriel envoyé
  - Poste Itinéo : à la boîte commune des opérateurs d'AE (ACSSI) qui se chargent d'installer la clé et le certificat sur le poste Itinéo ;
  - Tablette dPad et smartphone dPhone : à la boîte commune des opérateurs d'AE (ACSSI) qui se chargent ensuite de transmettre le PKCS#12 et le mot de passe associé au service de déploiement (infogérant) qui lui, se chargera d'installer la clé et le certificat sur la carte microSD qui sera insérée dans la tablette dPad ou le smartphone dPhone ;
  - Boîtier NETASQ : à la boîte aux lettres commune des opérateurs d'AE (ACSSI) qui se chargent de transférer le PKCS#12 à l'ESU SSI responsable de l'installation de la clé et du certificat sur le boîtier par courriel chiffré et signé.
- envoi du mot de passe protégeant l'accès au PKCS#12 à :
  - Poste Itinéo, tablette dPad et smartphone dPhone : à la boîte commune des opérateurs d'AE (ACSSI) ;
  - Boîtier NETASQ : à la boîte aux lettres commune des opérateurs d'AE (l'ACSSI). Ces derniers sont en charge de transmettre le mot de passe à l'ESU SSI par courriel chiffré et signé.

Actions supplémentaires (ne relevant pas directement de l'AC) :

- Remise du poste :
  - Poste Itinéo : après installation du certificat et de la clé privée, le poste est remis à l'info-gérant en administration centrale pour accompagner le titulaire du poste lors du déploiement et à l'IDA\DET à l'étranger qui remettra le poste au correspondant SI responsable d'accompagner le titulaire au déploiement de son poste ;
  - tablette dPad et smartphone dPhone : le PKCS#12 et le mot de passe nécessaire à son installation sont envoyés par messagerie sécurisée au service de proximité (infogérant) qui se charge de l'installation du certificat dans la carte microSD. Le service de proximité se charge alors d'accompagner le titulaire du Smartphone lors du déploiement ;
  - Boîtier NETASQ : après installation du certificat et de la clé privée, le boîtier NetASQ est remis à l'info-gérant puis à l'IDA qui se charge du déploiement du boîtier à la boîte.

L'ensemble de ces opérations est détaillé dans la DPC.

Les conditions de génération des clés et des certificats, les mesures de sécurité à respecter, sont précisées dans les parties 5 et 6, notamment la séparation des rôles de confiance.

#### 4.3.1.2 CERTIFICAT DE GABARIT « CLIENT SSL » ET « SERVEUR SSL » : COMPOSANTS TECHNIQUES ET SERVEURS

- Dans le cas d'une génération de la clé privée en central :
  - création du certificat et de la bi-clé du futur Porteur; signature du certificat à l'aide de la clé privée de l'AC;
  - envoi du certificat et de la bi-clé au format PKCS#12 protégé par un mot de passe en pièce jointe d'un courriel envoyé à la boîte aux lettres commune des ESU (en copie, un responsable de l'équipe chargée des validations) ;

- envoi du mot de passe protégeant l'accès au PKCS#12 à la boîte aux lettres commune des opérateurs d'AE (en copie, un responsable de l'ACSSI). Ces derniers sont en charge de transmettre le mot de passe au demandeur par courriel chiffré et signé (en copie, le responsable hiérarchique du demandeur).

- Dans le cas d'une génération de la clé privée en local :
  - certification du PKCS#10 ;
  - envoi du certificat au demandeur (en copie, le responsable hiérarchique du demandeur).

L'ensemble de ces opérations est détaillé dans la DPC.

Les conditions de génération des clés et des certificats, les mesures de sécurité à respecter, sont précisées dans les parties 5 et 6, notamment la séparation des rôles de confiance.

#### 4.3.1.3 CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

À chaque demande de certificat, l'AC effectue les opérations suivantes :

- authentification du demandeur (Autorité d'Enregistrement);
- vérification de l'intégrité de la demande;
- vérification technique de la demande;
- création du certificat et de la bi-clé du futur Porteur;
- signature du certificat à l'aide de la clé privée de l'AC;
- envoi du certificat et de la bi-clé au format PKCS#12 protégé par un mot de passe en pièce jointe d'un courriel envoyé au Responsable de certificat ;
- envoi du mot de passe protégeant l'accès au PKCS#12 à la boîte aux lettres commune des opérateurs d'AE (en copie, un responsable de l'ACSSI). Ces derniers sont en charge de transmettre le mot de passe au Responsable de Certificat par courriel chiffré et signé (en copie, le responsable hiérarchique du demandeur).

L'ensemble de ces opérations est détaillé dans la DPC.

Les conditions de génération des clés et des certificats, les mesures de sécurité à respecter, sont précisées dans les parties 5 et 6, notamment la séparation des rôles de confiance.

#### 4.3.1.4 CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

À chaque demande de certificat, l'AC effectue les opérations suivantes :

- authentification du demandeur (Autorité d'Enregistrement);
- vérification de l'intégrité de la demande;
- vérification technique de la demande;
- **Dans le cas d'une génération de la clé privée en central** :
  - création du certificat et de la bi-clé du futur Porteur;
  - signature du certificat à l'aide de la clé privée de l'AC;
  - envoi du certificat et de la bi-clé au format PKCS#12 protégé par un mot de passe en pièce jointe d'un courriel envoyé au Responsable de certificat ;

- envoi du mot de passe protégeant l'accès au PKCS#12 à la boîte aux lettres commune des opérateurs d'AE (en copie, un responsable de l'ACSSI). Ces derniers sont en charge de transmettre le mot de passe au demandeur par courriel chiffré et signé (en copie, le responsable hiérarchique du demandeur).

- **Dans le cas d'une génération de la clé privée en local** :
  - certification du PKCS#10 ;
  - envoi du certificat au demandeur (en copie, le responsable hiérarchique du demandeur).

L'ensemble de ces opérations est détaillé dans la DPC.

Les conditions de génération des clés et des certificats, les mesures de sécurité à respecter, sont précisées dans les parties 5 et 6, notamment la séparation des rôles de confiance.

#### 4.3.1.5 CERTIFICAT DE PROFIL « SIGNATURE JETON D'HORODATAGE »

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération et de préparation des différents éléments destinés au RC : au minimum, le certificat, et, selon les cas, la bi-clé du serveur, son dispositif de création de signature de jetons d'horodatage, les codes d'activation, etc. (cf. chapitre 1.3.1).

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

### 4.3.2 NOTIFICATION PAR L'AC DE LA DELIVRANCE DU CERTIFICAT AU SERVICE APPLICATIF

#### 1.1. CERTIFICAT DE PROFIL « ACCES DISTANT»

L'AC notifie directement les opérateurs d'AE (l'ACSSI) par 2 courriels distincts contenant respectivement les clés et certificats au format PKCS#12 et le mot de passe associé.

#### 1.2. CERTIFICAT DE PROFIL « SERVEUR SSL » ET « CLIENT SSL »

L'AC notifie directement les responsables des composants techniques par courriel pour les informer du retrait effectif des clés et certificats.

#### 1.3. CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

L'AC notifie le Responsable du Certificat par courriel pour l'informer du retrait effectif des clés et certificats.

#### 1.4. CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

L'AC notifie le responsable du Certificat par courriel pour l'informer du retrait effectif des clés et certificats.

#### 1.5. CERTIFICAT DE PROFIL « SIGNATURE JETON D'HORODATAGE »

Le certificat est transmis par message électronique à une adresse fournie par le RC. Le certificat complet et exact est mis à la disposition du RC.

*Nota – Si la remise du certificat doit se faire en main propre auprès de l'AE, le RC sera également tributaire des modalités d'accueil de l'AE.*

## 4.4 ACCEPTATION DU CERTIFICAT

### 4.4.1 DEMARCHE D'ACCEPTATION DU CERTIFICAT

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

L'acceptation d'un certificat vaut acceptation de la PC de l'Autorité de Certification AC INFRASTRUCTURE N.

### 4.4.2 PUBLICATION DU CERTIFICAT

Le certificat de l'AC INFRASTRUCTURE N est publié tel que défini au paragraphe 2.2.

### 4.4.3 NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU CERTIFICAT

Les opérations réalisées par L'AC lors de la délivrance d'un certificat sont tracées dans un module dédié de l'IGC.

## 4.5 USAGE DE LA BI-CLE ET DU CERTIFICAT

### 4.5.1 UTILISATION DE LA CLE PRIVEE ET DU CERTIFICAT PAR LE RC

Les porteurs de certificats ne doivent les utiliser que dans les domaines d'utilisation spécifiés à la partie 1.4.1 de la présente PC.

Les responsables des composants techniques s'engagent à respecter strictement ces domaines d'utilisation. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la clé privée et du certificat associé est indiqué dans le certificat dans les extensions concernant les usages des clés.

### 4.5.2 UTILISATION DE LA CLE PUBLIQUE ET DU CERTIFICAT PAR L'UTILISATEUR DU CERTIFICAT

Les services applicatifs ne doivent utiliser le certificat et la clé publique associée que dans les domaines d'utilisation spécifiés à la partie 1.4.1.

L'usage autorisé du certificat est indiqué dans le certificat dans les extensions concernant les usages des clés.

## 4.6 RENOUVELLEMENT D'UN CERTIFICAT

Pour l'ACI la notion de renouvellement correspond à la délivrance d'un nouveau certificat sans modification de la bi-clé et pour lequel seules les dates sont modifiées, toutes les autres informations restant identiques au certificat précédent (y compris la clé publique du service applicatif).
La présente PC exige qu'un certificat et sa bi-clé aient la même durée de vie ; le renouvellement d'un certificat sans modification de la bi-clé est donc interdit.

## 4.7 DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE

Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat électronique liée à la génération d'une nouvelle bi-clé. L'AC exige que la bi-clé soit renouvelée en cas de renouvellement de certificat.

### 4.7.1 CAUSES POSSIBLES DE CHANGEMENT D'UNE BI-CLE

La délivrance d'un nouveau certificat peut résulter de l'expiration du certificat courant dans le cadre d'un renouvellement de bi-clé. Dans ce cas, le renouvellement ne peut avoir lieu que pendant la période de renouvellement du certificat associé à la bi-clé changée.

La délivrance d'un nouveau certificat peut également résulter d'une nouvelle demande suite à une révocation ou suite à un oubli de renouvellement (délivrance en dehors de la période de renouvellement).

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des services applicatifs, et les certificats correspondants, sont renouvelés à une fréquence définie au point 6.3.2..

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du service applicatif.

### 4.7.2 ORIGINE D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

Dans le cas d'une demande de certificat pour un renouvellement, l'Autorité de Certification notifie automatiquement par courriel, à l'adresse renseignée dans l'interface d'AE (pendant l'enregistrement initial ou par la suite), de l'expiration prochaine du certificat. Tant que le certificat n'a pas été renouvelé, les notifications continuent d'être envoyées aux dates suivantes à la même adresse courriel :

- 6 mois avant l'expiration du certificat ;
- 3 mois avant l'expiration du certificat ;
- 1 mois avant l'expiration du certificat.

L'adresse de destination de ces notifications peut être une adresse de boîte aux lettres commune.

**Profil « serveur SSSL » et « Client SLL » :**

- Cas d'un renouvellement : Le responsable du composant technique est notifié par courriel de l'expiration prochaine de son certificat (Cf Déclaration des Pratiques de Certification). La demande de renouvellement s'effectue à l'identique d'une demande initiale de certificat.
- Cas d'une nouvelle demande : La demande de certificat s'effectue à l'identique d'une demande initiale de certificat.

**Profil « jeton d'horodatage » :**

Le déclenchement de la fourniture d'un nouveau certificat de signature de jetons d'horodatage est à l'initiative du RC. L'entité peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un serveur qui lui est rattaché.

### 4.7.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

La procédure de demande d'un nouveau certificat est identique à la procédure de demande initiale.

### 4.7.4 NOTIFICATION AU RC DE L'ETABLISSEMENT D'UN NOUVEAU CERTIFICAT

Cf chapitre 4.3.2

### 4.7.5 DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT

La démarche d'acceptation du nouveau certificat est identique à la démarche à l'enregistrement initial.

### 4.7.6 PUBLICATION DU NOUVEAU CERTIFICAT

La publication du nouveau certificat se fera de la même façon qu'à l'enregistrement initial.

### 4.7.7 NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU NOUVEAU CERTIFICAT

La notification se fera de la même façon qu'à l'enregistrement initial.

## 4.8 MODIFICATION DU CERTIFICAT

La modification de certificat n'est pas autorisée. Toute demande de modification se traduit par une demande de nouveau certificat, détaillée dans les parties 4.1 et 4.2.

## 4.9 REVOCATION ET SUSPENSION DES CERTIFICATS

### 4.9.1 CAUSES POSSIBLES D'UNE REVOCATION

#### 4.9.1.1 CERTIFICATS DE SERVICE APPLICATIF

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

- les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du nom du serveur), ceci avant l'expiration normale du certificat ;
- le RC n'a pas respecté les modalités applicables d'utilisation du certificat ;

- le RC / l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- la clé privée du serveur est suspectée de compromission, est compromise, est perdue ou est volée, (éventuellement les données d'activation associées) ;
- le RC ou une entité autorisée (représentant légal de l'entité par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du serveur et/ou de son support) ;
- l'arrêt définitif du serveur ou la cessation d'activité de l'entité du RC de rattachement du serveur.

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

Lorsque l'une des circonstances ci-dessus se réalise, le certificat concerné est révoqué et son numéro de série placé dans la Liste de Certificats Révoqués (LCR) tant que la date d'expiration du certificat n'est pas dépassée.

Toute demande de révocation doit être accompagnée d'une cause de révocation.

#### 4.9.1.2 CERTIFICATS D'UN COMPOSANT D'IGC

Les circonstances suivantes doivent être à l'origine de la révocation du certificat de l'ACI

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

### 4.9.2 ORIGINE D'UNE DEMANDE DE REVOCATION

#### 4.9.2.1 CERTIFICAT DE GABARIT « ACCES DISTANT »

**Postes Itinéo**

Les personnes habilitées à demander une révocation de certificat sont :

- L'IDA/DCG qui reçoit la demande via le titulaire du poste ou son responsable hiérarchique, ou l'info gérant ;
- le Correspondant SI ;
- l'ACSSI.

**Tablettes dPad et smartphones dPhone**

Les personnes habilitées à demander une révocation de certificat sont :

- L'IDA/DCG qui reçoit la demande via le titulaire du poste ou son responsable hiérarchique, ou l'info gérant ;
- le Correspondant SI ;
- l'ACSSI.

**Boîtiers NETASQ**

Les personnes habilitées à demander une révocation de certificat sont :

- le responsable du composant technique ;
- un opérateur de l'Autorité d'Enregistrement.

L'authentification du demandeur et la vérification de la validité de la demande se font selon les modalités définies dans la partie 3.4.

En cas de compromission, la demande peut également émaner de la voie SSI (FSSI/RSSI venant éventuellement de CERTA/ANSSI).

En cas de décision du Ministère, la demande peut émaner de l'autorité administrative (HFCDS/SDD) ou de l'autorité d'enregistrement (DSI/ACSSI).

Dans ces deux cas, la justification est à la diligence de l'AC ou de l'AE dont font partie les membres de la voie fonctionnelle SSI.

#### 4.9.2.2 CERTIFICAT DE GABARIT « CLIENT SSL » ET « SERVEUR SSL »

**Composants techniques et serveurs**

Les personnes habilitées à demander une révocation de certificat sont :

- le responsable du composant technique ;
- l'équipe chargée de la validation des demandes de certificats ;
- un opérateur de l'Autorité d'Enregistrement.

L'authentification du demandeur et la vérification de la validité de la demande se font selon les modalités définies dans la partie 3.4.
En cas de compromission, la demande peut également émaner de la voie SSI (FSSI/RSSI venant éventuellement de CERTA/ANSSI).

Dans ces deux cas, la justification est à la diligence de l'AC ou de l'AE dont font partie les membres de la voie fonctionnelle SSI.

#### 4.9.2.3 CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

Les personnes habilitées à demander une révocation de certificat sont :

- le responsable du certificat ;
- un représentant légal de l'entité ;

- l'AC émettrice du certificat ou l'une de ses composantes (opérateur d'AE).

En cas de compromission, la demande peut également émaner de la voie SSI (FSSI/RSSI venant éventuellement de CERTA/ANSSI).

En cas de décision du Ministère, la demande peut émaner de l'autorité administrative (HFCDS/SDD) ou de l'autorité d'enregistrement (DSI/ACSSI).

Dans ces deux cas, la justification est à la diligence de l'AC ou de l'AE dont font partie les membres de la voie fonctionnelle SSI.

#### 4.9.2.4 CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

Les personnes habilitées à demander une révocation de certificat sont :

- le responsable du certificat (MOA Hermès) ;
- un représentant légal de l'entité ;
- l'AC émettrice du certificat ou l'une de ses composantes (opérateur d'AE).

En cas de compromission, la demande peut également émaner de la voie SSI (FSSI/RSSI venant éventuellement de CERTA/ANSSI).

En cas de décision du Ministère, la demande peut émaner de l'autorité administrative (HFCDS/SDD) ou de l'autorité d'enregistrement (DSI/ACSSI).

Dans ces deux cas, la justification est à la diligence de l'AC ou de l'AE dont font partie les membres de la voie fonctionnelle SSI.

#### 4.9.2.5 CERTIFICAT DE PROFIL « SIGNATURE JETON D'HORODATAGE »

Les personnes / entités qui peuvent demander la révocation d'un certificat de signature de jetons d'horodatage sont les suivantes :

- le RC pour le serveur considéré ;
- un représentant légal de l'entité ;
- l'AC émettrice du certificat ou l'une de ses composantes (AE).

*Nota* : Le RC doit être informé des personnes / entités susceptibles d'effectuer une demande de révocation pour le certificat dont il a la responsabilité.

### 4.9.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE REVOCATION

#### 4.9.3.1 CERTIFICAT DE GABARIT « ACCES DISTANT »

Il existe plusieurs moyens pour le demandeur de révoquer les certificats d'un service applicatif :

- par courriel signé;
- par téléphone.

La demande de révocation doit contenir à minima :

- le CN du composant technique ;
- le nom du demandeur ;
- toute information permettant de retrouver le certificat (numéro de série, raison de révocation, etc.).

La demande de révocation est envoyée à la boîte aux lettres commune des opérateurs d'AE. Un opérateur d'AE va alors vérifier l'identité du demandeur et son droit à demander la révocation d'un certificat. Une fois la vérification effectuée, l'opérateur d'AE renseigne la demande à l'interface d'AE de l'IGC.

**Postes Itinéo, tablettes dPad et smartphones dPhone**

Des notifications automatiques sont envoyées aux opérateurs de révocation pour les informer de la révocation du certificat. Ensuite, ces opérateurs se chargent d'informer le demandeur de la révocation.

**Boîtiers NETASQ**

Une notification est envoyée aux ACSSI en tant qu'opérateurs de révocation et une notification est envoyée à l'ESU SSI en tant que responsable du boîtier.

#### 4.9.3.2 CERTIFICAT DE GABARIT « CLIENT / SERVEUR SSL »

**Composants techniques et serveurs**

Il existe plusieurs moyens pour le demandeur de révoquer les certificats d'un service applicatif :

- par courriel signé (en copie, l'équipe chargée de la validation des demandes) ;
- par téléphone ;
- par fax ou écrit (en joignant le formulaire d'habilitation signé).

La demande de révocation doit contenir à minima :

- Le FQDN du serveur ou le nom du composant technique ;
- Le nom du demandeur ;
- Toute information permettant de retrouver le certificat (numéro de série, raison de révocation, etc.).

La demande de révocation est envoyée à la boîte aux lettres commune des opérateurs d'AE. Un opérateur d'AE va alors vérifier l'identité du demandeur et son droit à demander la révocation d'un certificat. Une fois la vérification effectuée, l'opérateur d'AE renseigne la demande à l'interface d'AE de l'IGC.

Dans le cas où le Responsable du composant technique n'est pas le demandeur de la révocation, une notification par courriel lui est envoyée l'informant de la révocation de son certificat.

Ce processus est valable pour les demandes de révocation des certificats pour les profils « Authentification Serveur / Client SSL ».

#### 4.9.3.3 CERTIFICAT DE PROFIL « SIGNATURE DE CODE »

Il existe plusieurs moyens pour le demandeur de révoquer les certificats d'un Responsable de Certificat :

- par courriel signé (en copie, l'équipe d'habilitation chargée de la validation des demandes);
- par téléphone ;
- par fax ou écrit (en joignant le formulaire d'habilitation signé).

La demande de révocation doit contenir à minima :

- le nom du service applicatif figurant dans le certificat (nom de l'application ou du service applicatif)
- le nom du demandeur ;
- toute information permettant de retrouver le certificat (numéro de série, raison de révocation, etc.) ;
- éventuellement la cause de la révocation.

La demande de révocation est envoyée à la boîte aux lettres commune des opérateurs d'AE. Un opérateur d'AE va alors vérifier l'identité du demandeur et son droit à demander la révocation d'un certificat. Une fois la vérification effectuée, l'opérateur d'AE renseigne la demande à l'interface d'AE de l'IGC.

Une notification par courriel est envoyée au Responsable de Certificat pour l'informer de la révocation de son certificat.

#### 4.9.3.4 CERTIFICAT DE PROFIL « SIGNATURE DE CONFIGURATION »

Il existe plusieurs moyens pour le demandeur de révoquer les certificats d'un RC :

- par courriel signé (en copie, l'équipe d'habilitation chargée de la validation des demandes);
- par téléphone ;
- par fax ou écrit (en joignant le formulaire d'habilitation signé).

La demande de révocation doit contenir à minima :

- le nom du service applicatif figurant dans le certificat (nom de l'application ou du service applicatif)
- le nom du demandeur ;
- toute information permettant de retrouver le certificat (numéro de série, raison de révocation, etc.) ;
- éventuellement la cause de la révocation.

La demande de révocation est envoyée à la boîte aux lettres commune des opérateurs d'AE. Un opérateur d'AE va alors vérifier l'identité du demandeur et son droit à demander la révocation d'un certificat. Une fois la vérification effectuée, l'opérateur d'AE renseigne la demande à l'interface d'AE de l'IGC.

Dans le cas où le Responsable du Certificat n'est pas le demandeur de la révocation, une notification par courriel lui est envoyée l'informant de la révocation de son certificat.

#### 4.9.3.5 CERTIFICAT DE PROFIL « SIGNATURE JETON D'HORODATAGE »

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

Les informations suivantes doivent au moins figurer dans la demande de révocation de certificat :

- le nom du serveur utilisé dans le certificat ;
- le nom du demandeur de la révocation ;
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série,...) ;

- la cause de révocation.

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 doit être diffusée au minimum via une LCR signée par une entité désignée par l'AC. D'autres moyens de diffusion complémentaires peuvent également être utilisés par l'AC (cf. chapitre 4.9.9).

Le demandeur de la révocation doit être informé du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si le RC n'est pas le demandeur, il doit également être informé de la révocation effective de ce certificat.

L'entité doit être informée de la révocation de tout certificat de signature de jetons d'horodatage qui lui sont rattachés.

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

#### 4.9.3.6 REVOCATION D'UN CERTIFICAT D'UNE COMPOSANTE DE L'IGC

L'AC précise dans sa DPC les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des RC concernés que leurs certificats de services applicatifs correspondants ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE. Ces derniers devront informer les RC en leur indiquant explicitement que leurs certificats de services applicatifs ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Le point de contact identifié sur le site http://ssi.gouv.fr doit être immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification. L'ANSSI se réserve le droit de diffuser par tout moyen l'information auprès des promoteurs d'applications au sein des autorités administratives et auprès des usagers.

### 4.9.4 DELAI ACCORDE AU DEMANDEUR POUR FORMULER LA DEMANDE DE REVOCATION

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

### 4.9.5 DELAI DE TRAITEMENT PAR L'AC D'UNE DEMANDE DE REVOCATION

#### 4.9.5.1 REVOCATION D'UN CERTIFICAT ELECTRONIQUE

Par nature, une demande de révocation doit être traitée en urgence.

#### 4.9.5.2 DISPONIBILITE DU SYSTEME DE TRAITEMENT DES DEMANDES DE REVOCATION

La fonction de gestion des révocations est disponible aux heures ouvrées. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2h (jours ouvrées). Cette fonction a une durée maximale totale d'indisponibilité par mois de 16h (jours ouvrées)

L'AE traite les demandes qui lui parviennent au plus tard 72 heures après réception. 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.
Une fois la demande de révocation envoyées par l'AE à l'AC, la Liste des Certificats Révoquées est mise à jour et générée.

#### 4.9.5.3 REVOCATION D'UN CERTIFICAT D'UNE COMPOSANTE DE L'IGC

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat, et que cette liste est accessible au téléchargement.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR ou de réponses OCSP) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

### 4.9.6 EXIGENCES DE VERIFICATION DE LA REVOCATION PAR UTILISATEURS DE CERTIFICATS

L'utilisateur d'un certificat électronique est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée (LCR, dLCR, OCSP…) est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.
Le Ministère met à disposition des utilisateurs des Listes de Certificats Révoqués (LCR) et un répondeur OCSP.

### 4.9.7 FREQUENCE D'ETABLISSEMENT DES LCR

Les Listes des Certificats Révoqués sont générées au minimum toutes les 72 heures.

### 4.9.8 DELAI MAXIMUM DE PUBLICATION D'UNE LCR

La Liste des Certificats Révoqués est publiée au plus tard 30 minutes après sa génération.

### 4.9.9 EXIGENCES SUR LA VERIFICATION EN LIGNE DE LA REVOCATION ET DE L'ETAT DES CERTIFICATS

La validité du certificat est vérifiée par composants techniques en consultant les LCR valides et le serveur OCSP.

### 4.9.10 AUTRES MOYENS DISPONIBLES D'INFORMATION SUR LES REVOCATIONS

Sans objet.

### 4.9.11 EXIGENCES SPECIFIQUES EN CAS DE COMPROMISSION DE LA CLE PRIVEE

Les entités (cf. partie 4.9.2) autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Dans certains cas, l'information de révocation de certificat devra pouvoir être communiquée à l'ANSSI et/ou à tout ou partie de l'ensemble des opérateurs d'AE du Ministère.

### 4.9.12 CAUSES POSSIBLES D'UNE SUSPENSION

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

### 4.9.13 ORIGINE D'UNE DEMANDE DE SUSPENSION

Sans objet.

### 4.9.14 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE SUSPENSION

Sans objet.

### 4.9.15 LIMITES DE LA PERIODE DE SUSPENSION D'UN CERTIFICAT

Sans objet.

## 4.10 FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS

### 4.10.1 CARACTERISTIQUES OPERATIONNELLES

La fonction d'information sur l'état des certificats a pour but de permettre aux RC de vérifier le statut d'un certificat et de sa chaîne de certification, c'est à dire de vérifier également les signatures des certificats de la chaîne de certification et les signatures garantissant l'origine et l'intégrité des LCR.
La fonction d'information sur l'état des certificats met à la disposition des services applicatifs un mécanisme de consultation libre de LCR. Ces LCR sont au format LCRv2, publiées électroniquement aux URL définies à la partie 2.2. Ces adresses figurent également dans le champ « Point de Distribution des LCR » de chaque certificat.

### 4.10.2 DISPONIBILITE DE LA FONCTION

Le tableau suivant présente les engagements en termes de disponibilité de la fonction d'information sur l'état des certificats.

| | |
|---|---|
| Accessibilité du service | 24h/24h, 7j/7j |
| Taux de disponibilité du service de publication (base mensuelle hors maintenance préventive) | 96 % |
| Durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats | 32h (jours ouvrés) |

Tableau 16 : Disponibilité de la fonction d'information sur l'état des certificats

### 4.10.3 DISPOSITIFS OPTIONNELS

Sans objet.

## 4.11 FIN DE LA RELATION ENTRE LE SERVICE APPLICATIF ET L'AC

En cas de fin de vie de la relation entre le service applicatif et l'AC avant la fin de validité du certificat, l'Autorité d'Enregistrement procède à la révocation du certificat du service applicatif.

## 4.12 SEQUESTRE DE CLE ET RECOUVREMENT

Ce document ne traite pas de chiffrement de données et interdit donc le séquestre des clés privées des Porteurs.

Les clés privées d'AC ne doivent pas non plus être séquestrées.

### 4.12.1 POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR SEQUESTRE DES CLES

Sans objet.

### 4.12.2 POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR ENCAPSULATION DES CLES DE SESSION

Sans objet.

# 5 MESURES DE SECURITE NON TECHNIQUES

## 5.1 MESURES DE SECURITE PHYSIQUE

### 5.1.1 SITUATION GEOGRAPHIQUE 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.

### 5.1.2ACCES PHYSIQUE

Les zones hébergeant les systèmes informatiques de l'ACD sont physiquement protégées. L'accès doit être strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être 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.

### 5.1.3ALIMENTATION ELECTRIQUE ET CLIMATISATION

Le serveur hébergeant l'ACD sur le site nominal ainsi que son module cryptographique sont branchés électriquement en permanence.
Les locaux hébergeant l'ACD sont climatisés.
Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'ACD telles que fixées par leurs fournisseurs.

### 5.1.4 VULNERABILITE AUX DEGATS DES EAUX

Les locaux hébergeant l'ACD sont protégés contre les dégâts des eaux par le plan de prévention des inondations.

### 5.1.5 PREVENTION ET PROTECTION INCENDIE

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

### 5.1.6 CONSERVATION DES SUPPORTS

Les sauvegardes des données et de l'application opérant l'ACD sont conservées dans une enceinte sécurisée, accessible aux seules personnes habilitées, autorisées et désignées à ces fins.
Les supports papier de l'ACD sont également être 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'ACD, 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'ACD 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'ACD ne sont pas utilisés à d'autres fins avant destruction complète des informations liées à l'ACD qu'ils sont susceptibles de contenir.

### 5.1.8 SAUVEGARDE HORS SITE

La procédure de sauvegarde des données et logiciels appliquée permet de garantir la continuité d'activité de l'ACD, y compris en cas de destruction des sauvegardes situées sur le site nominal, dans un délai inférieur à 3 jours ouvrés.

## 5.2 MESURES DE SECURITE PROCEDURALES

### 5.2.1 ROLES DE CONFIANCE

Les rôles de confiance définis au niveau des AC Déléguées sont les suivantes :

- **Administrateur central -** Personne chargée de la configuration applicative et du maintien en conditions opérationnelles de l'application IGC, ainsi que de l'analyse régulière des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission.
- **Administrateur local –** Personne chargée des opérations de gestion du cycle de vie des certificats émis par les AC Déléguées (demande initiale, révocation, renouvellement recouvrement des certificats).
- **Auditeur -** Personne désignée par l'Autorité de Certification dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par les AC Déléguées par rapport aux Politiques de Certification et Déclarations des Pratiques de Certification correspondantes.
- **Autorité Qualifiée -** Personne chargée de la Sécurité de l'application IGC pour le compte de l'Autorité de Certification.
- **Responsable de l'application IGC -** Personne chargée de la mise en œuvre des Politiques de Certification et des Déclarations des Pratiques de Certification des AC Déléguées, 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 chargée de la vérification de la cohérence des actions des différents rôles décrits précédemment et de la qualité des processus des AC Déléguées.

#### 5.2.1.1 ROLES DE CONFIANCE MUTUALISES

Les rôles de confiance mutualisés et définis au niveau des AC Déléguées sont les suivantes :

- **Administrateur sécurité** - Personne chargée d'assurer la gestion de la sécurité au niveau des systèmes, ainsi que de l'habilitation des administrateurs centraux et locaux.
- **Responsable de salle** - Personne chargée de la gestion des accès physiques aux salles informatiques hébergeant l'infrastructure et aux équipements.
- **Exploitant -** Personne chargée d'assurer l'exploitation, la surveillance et la maintenance des systèmes et des réseaux. Cette personne est également 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 système afin de détecter tout incident, anomalie, tentative de compromission, etc.
- **Fonctionnaire de Sécurité des Systèmes d'Informations (FSSI) -** Personne chargée de la Politique de Sécurité du SI du Ministère.
- **Responsable de production -** Personne chargée du maintien en conditions opérationnelles du système d'information du Ministère.

En plus de ces rôles de confiance, l'AC peut être amenée à distinguer également en tant que rôle de confiance, les rôles de Porteur de parts de secrets d'IGC. Les rôles de confiance spécifiques aux Cérémonies des Clés sont décrits dans le document de Cérémonie des Clés. Ce document n'est pas public.

### 5.2.2 NOMBRE DE PERSONNES REQUISES PAR TACHES

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 doivent être assurés par des personnes distinctes.
Par ailleurs, toute opération impliquant les secrets principaux de l'ACD nécessite l'intervention de trois personnes. La DPC précise les opérations nécessitant l'intervention de plusieurs personnes ainsi que les contraintes que ces personnes doivent respecter.

### 5.2.3 IDENTIFICATION ET AUTHENTIFICATION POUR CHAQUE ROLE

Tout accès à l'application IGC est soumis à authentification (éventuellement 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 enregistrée dans l'application IGC et disposer d'un certificat d'authentification.
Pour les autres rôles en relation avec l'IGC, l'AC 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.

### 5.2.4 ROLES EXIGEANT UNE SEPARATION 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 partie 5.2.2.
Les attributions associées à chaque rôle doivent être 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 SECURITE VIS-A-VIS DU PERSONNEL

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

### 5.3.1 QUALIFICATIONS, COMPETENCES 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 rôles de confiance correspondent à leurs compétences professionnelles et tient à jour la liste des personnels intervenants sur l'IGC.
Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier des procédures de sécurité en vigueur au sein de l'ACD.
L'AC informe toute personne intervenant dans des rôles de confiance de l'AC :

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

par une lettre de mission signée par l'AC.

### 5.3.2PROCEDURES DE VERIFICATION DES ANTECEDENTS

Le personnel amené à assurer un rôle de confiance vis-à-vis de l'ACD fait l'objet lors de son entrée en fonction, d'une vérification de ses antécédents par les services du Ministère.
Ces personnels ne doivent notamment pas avoir de condamnation incompatible avec leurs attributions.
Les personnes ayant un rôle de confiance ne souffrent pas 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 subissent pas de pression hiérarchique les incitants à se dessaisir de leur secret.

### 5.3.3 EXIGENCES EN MATIERE DE FORMATION INITIALE

En préalable à leur entrée en fonction, les administrateurs centraux sont formés aux concepts et objectifs de l'ACD, ainsi qu'aux procédures à mettre en œuvre.
Les exploitants et administrateurs système sont formés aux concepts et objectifs de l'ACD, ainsi qu'aux logiciels, matériels et procédures d'exploitation applicables.
Les administrateurs centraux sont formés aux concepts et objectifs de l'ACD, aux diverses procédures à mettre en œuvre au niveau de l'application IGC, notamment en terme de gestion des secrets et de délégation des droits.

### 5.3.4 EXIGENCES ET FREQUENCE EN MATIERE DE FORMATION CONTINUE

Avant toute évolution majeure de l'infrastructure de l'ACD 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 FREQUENCE ET SEQUENCE DE ROTATION ENTRE DIFFERENTES ATTRIBUTIONS

Aucune rotation programmée des attributions n'est prévue.

### 5.3.6 SANCTIONS EN CAS D'ACTIONS NON AUTORISEES

En cas d'actions non autorisées par le personnel, sont applicables les actions disciplinaires s'il y a lieu.

### 5.3.7 EXIGENCES VIS-A-VIS DU PERSONNEL DES PRESTATAIRES EXTERNES

Le personnel des prestataires externes intervenant dans les locaux et/ou sur la plate-forme hébergeant l'ACD respecte également les exigences du présent chapitre. Ceci est 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 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

Cette section s'applique exclusivement aux événements liés aux certificats objets de la présente PC.

### 5.4.1 TYPES D'EVENEMENTS A ENREGISTRER

#### 5.4.1.1 ENREGISTREMENTS SUR PAPIER OU BUREAUTIQUE

Sont enregistrés sur papier :

- Les opérations et événements survenant à l'occasion des Cérémonies des Clés. Ces enregistrements sont décrits dans le document de Cérémonie des Clés. Ce document n'est pas public.
- Les demandes de certificat lors d'une demande initiale ainsi que l'éventuel acceptation ou refus de la demande.
- Les demandes de renouvellement de certificat, ainsi que l'éventuelle acceptation ou refus de la demande.
- Les demandes de révocation.

Doivent être 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 ;
- les mises à jour de la présente PC, au sein du présent document.

#### 5.4.1.2 ENREGISTREMENTS ELECTRONIQUES PAR L'APPLICATION IGC

Toute action sur un dossier lié à un certificat émis par l'ACD est enregistrée, et un historique complet du dossier doit être conservé dans la base de données de l'ACD.
De plus, les événements suivants font l'objet d'un enregistrement électronique de type log par l'application IGC :

- acceptation ou refus de connexion à l'application IGC ;
- génération des certificats ;
- révocation de certificat ;
- génération de la LCR ;
- modification des droits des personnels autorisés à intervenir auprès de l'application IGC ;
- modification des paramètres de configuration de l'application IGC.

#### 5.4.1.3 AUTRES ENREGISTREMENTS ELECTRONIQUES

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'ACD, 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.

Les évènements suivants doivent également faire l'objet d'un enregistrement électronique :

- publication de la LCR.

#### 5.4.1.4 CARACTERISTIQUES COMMUNES

Pour tous les types d'enregistrements présentés ci-dessus : chaque enregistrement d'événement doit contenir 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 doit être responsable de sa journalisation.
Les opérations de journalisation électronique doivent être effectuées au cours du processus ou à la fin de celui-ci.
En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement.

### 5.4.2 FREQUENCE DE TRAITEMENT DES JOURNAUX D'EVENEMENTS

Cf. chapitre **Erreur ! Source du renvoi introuvable.** « Évaluation des vulnérabilités » ci-dessous.

### 5.4.3 PERIODE DE CONSERVATION DES JOURNAUX D'EVENEMENTS

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

#### 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 ELECTRONIQUES PAR L'APPLICATION IGC

Les enregistrements des journaux doivent être conservés au sein de l'application IGC pendant 5 ans.

#### 5.4.3.3 AUTRES ENREGISTREMENTS ELECTRONIQUES

Les autres journaux d'enregistrement sous forme électronique doivent être sauvegardés puis purgés suivant une fréquence prévue par les procédures internes du MINISTÈRE, hormis ceux situés sur la plate-forme des ACD, non purgés.

### 5.4.4 PROTECTION DES JOURNAUX D'EVENEMENTS

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.
Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

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

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

#### 5.4.4.1 ENREGISTREMENTS SUR PAPIER OU BUREAUTIQUE

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

#### 5.4.4.2 ENREGISTREMENTS ELECTRONIQUES 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 ELECTRONIQUES

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

### 5.4.5 PROCEDURE DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS

L'AC mets en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC.

#### 5.4.5.1 ENREGISTREMENTS SUR PAPIER OU BUREAUTIQUE

Les enregistrements papier font l'objet d'une archive, ce qui est précisé dans la partie 5.5.
Les enregistrements sous forme de documents bureautiques sont sauvegardés selon les procédures applicables à ce type de documents.

#### 5.4.5.2 ENREGISTREMENTS ELECTRONIQUES 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 doivent être protégés en intégrité par le même mécanisme qu'au sein de l'application IGC.

#### 5.4.5.3 AUTRES ENREGISTREMENTS ELECTRONIQUES

Les autres journaux sous forme électroniques sont sauvegardés par un système centralisé de sauvegardes, hormis ceux hébergés sur la plate-forme de l'ACD, non sauvegardés.

### 5.4.6 SYSTEME DE COLLECTE DES JOURNAUX D'EVENEMENTS

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 EVENEMENT AU RESPONSABLE DE L'EVENEMENT

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

### 5.4.8 ÉVALUATION DES VULNERABILITES

Chaque entité opérant une composante de l'IGC est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.
Les journaux d'évènements sont contrôlés une (1) fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.
Les journaux sont analysés dans leur totalité au minimum 1 fois toutes les 2 semaines et dès la détection d'une anomalie.
Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.
Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) est effectué à une fréquence d'une fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

## 5.5 ARCHIVAGE DES DONNEES

### 5.5.1 TYPES DE DONNEES A ARCHIVER

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

Les données archivées sont au minimum les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC ;
- les DPC ;
- les conditions générales d'utilisation ;
- les accords contractuels avec d'autres AC ;
- les certificats, LCR ou réponses OCSP tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les engagements signés des MC ;
- les justificatifs d'identité des RC et, le cas échéant, de leur entité de rattachement ;
- les journaux d'évènements des différentes entités de l'IGC.

#### 5.5.1.1 DONNEES 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'ACD (i.e. la présente Politique de Certification, la DPC et ses annexes…). L'archivage est sous la responsabilité du responsable de l'application IGC ;
- les dossiers de demande de certificat (demande initiale, renouvellement, révocation) pour les services applicatifs.

#### 5.5.1.2 DONNEES DE L'APPLICATION IGC (SOUS FORME ELECTRONIQUE) :

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

#### 5.5.1.3 AUTRES DONNEES SOUS FORME ELECTRONIQUE :

Les logiciels et fichiers de configuration doivent être sauvegardés périodiquement mais non archivés.
Les journaux d'événements autres que ceux de l'application IGC et tels que définis dans la section précédente peuvent éventuellement être sauvegardés selon la procédure définie ci-dessus, mais non archivés.

### 5.5.2 PERIODE DE CONSERVATION DES ARCHIVES

#### 5.5.2.1 DOSSIERS D'ENREGISTREMENT

**Certificats d'Autorités Déléguées et des services applicatifs émis par l'ACD :**
Les dossiers électroniques, les dossiers papier d'enregistrement et les certificats attachés sont conservés par l'application IGC pendant toute la vie de l'ACD sans être purgés.
La durée de conservation des dossiers d'enregistrement doit être portée à la connaissance du RC ou du MC.
Les dossiers d'enregistrement et les certificats attachés peuvent être présentés par l'ACD lors de toute sollicitation par les Autorités habilitées.
Ces dossiers doivent permettre de retrouver :

- l'identité des personnes physiques désignées dans le certificat émis ;
- la dénomination de l'Autorité pour laquelle le certificat a été émis.

**Certificats des composantes de l'IGC :**
Les certificats de composantes sont générés ou renouvelés parallèlement à la génération ou au renouvellement de la clé de l'Autorité correspondante. Il n'est donc pas constitué de dossiers d'enregistrement relatifs à ces certificats.

#### 5.5.2.2 LCR EMISES PAR L'AC

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

#### 5.5.2.3 JOURNAUX D'EVENEMENTS

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.

#### 5.5.2.4 DONNEES SOUS FORME PAPIER ET BUREAUTIQUE

Les données sont archivées durant au moins 7 ans ; hormis l'ensemble des documents référencés applicables à l'ACD archivés sans limitation de durée.

### 5.5.3 PROTECTION DES ARCHIVES

Pendant tout le temps de leur conservation, les archives :

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

Les moyens mis en œuvre pour archiver les pièces en toute sécurité doivent être indiqués dans la DPC.

### 5.5.4 PROCEDURES DE SAUVEGARDE DES ARCHIVES

Le niveau de protection des sauvegardes est équivalent au niveau de protection des archives. Les procédures de sauvegarde et le niveau de protection sont décrits dans la DPC. Données sous forme papier ou bureautique.

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

#### 5.5.4.1 DONNEES DE L'APPLICATION IGC (SOUS FORME ELECTRONIQUE)

Les données de l'application IGC doivent être archivées par l'application IGC elle-même et doivent donc faire l'objet de sauvegardes régulières selon les modalités définies dans la partie 5.4.5.

### 5.5.5 EXIGENCES D'HORODATAGE DES DONNEES

#### 5.5.5.1 DONNEES 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 30 minutes.

#### 5.5.5.2 DONNEES DE L'APPLICATION IGC (SOUS FORME ELECTRONIQUE)

La datation des données est réalisée selon les modalités définies dans la partie 6.8.

### 5.5.6 SYSTEME DE COLLECTE DES ARCHIVES

Le système de collecte des archives respecte les exigences de protection des archives concernées, définies dans les §5.5.2, §5.5.3, §5.5.4 et §5.5.5.

#### 5.5.6.1 DONNEES SOUS FORME PAPIER OU BUREAUTIQUE

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

#### 5.5.6.2 DONNEES DE L'APPLICATION IGC (SOUS FORME ELECTRONIQUE)

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

### 5.5.7 PROCEDURES DE RECUPERATION ET DE VERIFICATION DES ARCHIVES

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

#### 5.5.7.1 DONNEES 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 DONNEES DE L'APPLICATION IGC (SOUS FORME ELECTRONIQUE)

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

## 5.6 CHANGEMENT DE CLE D'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité de ce certificat de l'AC doit être supérieure à celle des certificats des services applicatifs qu'elle signe.
Les durées de vie maximales pour chaque type du certificat sont spécifiées au chapitre 6.3.2.

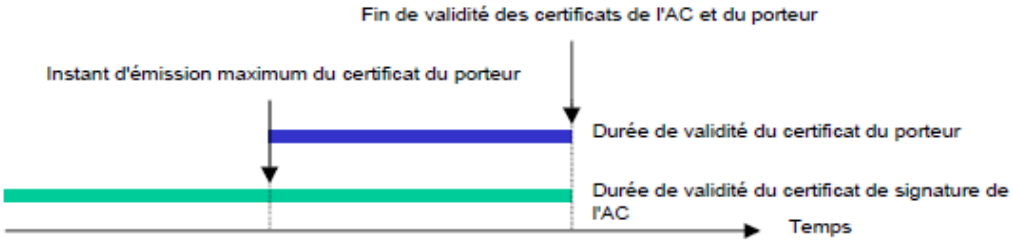



Figure 2 : Changement de clé d'AC

Au regard de la date de fin de validité d'un certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.
Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats.
Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

Le nommage utilisé pour distinguer les clés successives de l'autorité de certification répond aux règles suivantes.

- Dans le champ « Subject DN » du certificat AC INFRASTRUCTURE, la valeur « CN » est construite comme suit :
  - Pour la première clé cette valeur est « AC INFRASTRUCTURE » ;
  - Pour les clés suivantes, cette valeur est «AC INFRASTRUCTURE N » où N est un entier incrémenté par pas de 1 à chaque changement de clé d'AC, à partir de la valeur « 2 » pour le premier changement (le deuxième jeu de clés).
- Dans le champ « Issuer DN » des certificats porteurs, la valeur « CN » prend la valeur du champ « Subject DN » du certificat d'AC INFRASTRUCTURE ayant servi à les signer.

Le nommage des URL des CRL correspondant aux clés successives de l'autorité de certification répond aux règles suivantes :

- Pour la première clé cette valeur est « http://crl.diplomatie.gouv.fr/AC_Infrastructure/Crl/AC_INFRASTRUCTURE.crl »
- Pour les clés suivantes, cette valeur est « http://crl.diplomatie.gouv.fr/AC_Infrastructure_N/Crl/AC_INFRASTRUCTURE_N.crl », où N est un entier incrémenté par pas de 1 à chaque changement de clé d'AC, à partir de la valeur « 2 » pour le premier changement (le deuxième jeu de clés).

## 5.7 REPRISE SUITE A COMPROMISSION ET SINISTRE

### 5.7.1 PROCEDURES DE REMONTEE ET DE TRAITEMENT DES INCIDENTS ET DES COMPROMISSIONS

Ponctuellement, les administrateurs centraux de l'ACD peuvent mettre 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, par exemple avant utilisation de l'ACD.
Les procédures de traitement des incidents et des compromissions doivent faire l'objet du Plan de Reprise d'Activité de l'IGC. Ce document n'est pas public.
En cas d'incident impactant durablement ses services, l'ACD s'engage à Informer en utilisant tout moyen à sa convenance (messagerie, appel téléphonique, affichage, site Web, ...). :

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

### 5.7.2 PROCEDURES DE REPRISE EN CAS DE CORRUPTION DES RESSOURCES INFORMATIQUES (MATERIELS, LOGICIELS ET/OU DONNEES)

L'ACD 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 doit être testé au minimum une fois tous les deux ans.

### 5.7.3 PROCEDURES DE REPRISE EN CAS DE COMPROMISSION DE LA CLE PRIVEE D'UNE COMPOSANTE

Dans le cas de la compromission de sa clé privée, l'ACD doit procéder à sa cessation d'activité, et en informe selon tout moyen à sa disposition, les RC et utilisateurs des certificats émis par cette ACD.

### 5.7.4 CAPACITES DE CONTINUITE D'ACTIVITE SUITE A UN SINISTRE

En cas d'incident impactant l'infrastructure de l'ACD, les services de l'ACD doivent être restaurés sur une infrastructure semblable dans un délai inférieur à 8 heures en période ouvrée, permettant le respect des exigences de la présente PC en matière de disponibilité des fonctions de l'application IGC, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

## 5.8 FIN DE VIE DE L'IGC

Dans l'hypothèse d'une cessation d'activité totale, l'ACD 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'ACD :

1) doit s'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
2) doit prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
3) doit demander la révocation de son certificat auprès de l'AC RACINE DIPLOMATIE si cette dernière a certifié sa clé ;

4) doit révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
5) doit publier cette information sur les sites web *http://crl.diplomatie.gouv.fr* (dédié aux LCR des AC et aux autres informations).

# 6 MESURES DE SECURITE TECHNIQUES

## 6.1 GENERATION ET INSTALLATION DE BI-CLES

### 6.1.1 GENERATION DE BI-CLES

#### 6.1.1.1 CLES D'AC

La génération des clés des Autorités de Certification Déléguées est effectuée dans un environnement sécurisé.

Les clés sont générées et mises en œuvre dans un module cryptographique de type HSM (*Hardware Security Module*).
La génération de la clé des ACD 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. Ces documents ne sont pas publics.
La génération des clés des 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 des AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés des ACD.
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. 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 œuvre par son Porteur.
La cérémonie des clés se déroule sous le contrôle d'au moins une personne ayant au moins un rôle de confiance et en présence de plusieurs témoins.

Les détails de la méthode utilisée pour la génération des parts de secrets sont fournis dans la DPC.

#### 6.1.1.2 CLES DES SERVICES APPLICATIFS GENEREES PAR L'AC

Les bi-clés sont générées soit en central par l'AC soit en local directement sur le composant technique (dans le cas des certificats « Serveur et client SSL » et « signature de configuration ». Elles ne sont pas séquestrées par l'AC.

#### 6.1.1.3 CLES DE SERVICES APPLICATIFS GENEREES PAR LE SERVICE APPLICATIF

Dans le cas où la bi-clé est générée au niveau du service applicatif, cette génération doit être effectuée dans un dispositif répondant aux exigences de sécurité pour le niveau de sécurité considéré. L'AC s'assure auprès du RC, au minimum au travers d'un engagement contractuel clair et explicite du RC vis-à-vis de l'AC.

### 6.1.2 TRANSMISSION DE LA CLE PRIVEE AU SERVICE APPLICATIF

Quand l'AC génère la bi-clé du service applicatif (cf. chapitre 6.1.1.2), la clé privée est transmise au service applicatif de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. Les réponses OCSP produites sont archivées pendant au moins trois mois après leur expiration.

### 6.1.3 TRANSMISSION DE LA CLE PUBLIQUE A L'AC

Sans objet.

### 6.1.4 TRANSMISSION DE LA CLE PUBLIQUE DE L'AC AUX UTILISATEURS DE CERTIFICATS

Les clés publiques des AC Déléguées sont publiées et accessibles aux tiers utilisateurs de certificats.

### 6.1.5 TAILLE DE CLES

La longueur des clés d'AC est de 4096 bits.

La longueur des clés des RC émises par l'AC INFRASTRUCTURE N est 2048 bits.

### 6.1.6 VERIFICATION DE LA GENERATION DES PARAMETRES DES BI-CLES ET DE LEUR QUALITE

Les gabarits de certificats de l'AC INFRASTRUCTURE N sont préconfigurés dans la console de configuration de l'IGC. Seul un nombre restreint de personnes identifiées sont habilitées à accéder à la console de configuration pour édition. De plus, toute modification effectuée sur les gabarits figure dans les rapports d'audit.

### 6.1.7 OBJECTIFS D'USAGE DE LA CLE

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR et/ou de réponses OCSP (cf. chapitre 1.4.1.2).

L'utilisation de la clé privée du service applicatif et du certificat associé est strictement limitée à la fonction de sécurité concernée (cf. chapitres 1.5.1.1, 4.5).

## 6.2 MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES

### 6.2.1 STANDARDS ET MESURES DE SECURITE POUR LES MODULES CRYPTOGRAPHIQUES

#### 6.2.1.1 MODULES CRYPTOGRAPHIQUES DE L'AC

Les modules cryptographiques, utilisés par les ACD, pour la génération et la mise en œuvre de leurs clés, sont des modules cryptographiques de type HSM (*Hardware Security Module*) répondant au minimum aux exigences du chapitre 10 ci-dessous pour le niveau de sécurité considéré.

Les clés et certificats des administrateurs des HSM sont stockés au sein de cartes d'authentification administrateur, fournies aux administrateurs lors de la Cérémonie des Clés.

#### 6.2.1.2 DISPOSITIFS DE PROTECTION DES ELEMENTS SECRETS DU SERVICE APPLICATIF

Les dispositifs d'authentification des RC, pour la mise en œuvre de leurs clés privées d'authentification, respectent les exigences décrites ci-dessous :

- garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée
- garantir la confidentialité et l'intégrité de la clé privée
- assurer la correspondance entre la clé privée et la clé publique
- générer une authentification qui ne peut être falsifiée sans la connaissance de la clé privée
- assurer la fonction d'authentification pour le service applicatif légitime uniquement et protéger la clé privée contre toute utilisation par des tiers
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

### 6.2.2 CONTROLE DE LA CLE PRIVEE PAR PLUSIEURS PERSONNES

Ce chapitre porte sur le contrôle de la clé privée de l'AC pour l'exportation / l'importation hors / dans le module cryptographique HSM. La génération de la bi-clé est traitée à la partie 6.1.1.1, l'activation de la clé privée à la partie 6.2.8 et sa destruction à la partie 6.2.10.

Le contrôle des clés privées des AC est assuré par du personnel de confiance (Porteurs de secrets d'IGC) défini dans le cadre de la « Cérémonie des Clés ».

### 6.2.3 SEQUESTRE DE LA CLE PRIVEE

Ni les clés privées d'AC, ni les clés privées des services applicatifs s ne sont séquestrées.

### 6.2.4 COPIE DE SECOURS DE LA CLE PRIVEE

L'architecture réseau de l'IGC assure la haute-disponibilité. Les clés privées des AC font l'objet d'une copie de secours dans des modules cryptographiques identiques à ceux utilisés nominalement.

Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne sont à aucun moment en clair en dehors du module cryptographique. Le contrôle des opérations de chiffrement et de déchiffrement est conforme aux exigences de la partie 6.2.2.

### 6.2.5 ARCHIVAGE DE LA CLE PRIVEE

Sans objet. Ni les clés privées des AC, ni celles des services applicatifs ne sont pas archivée.

### 6.2.6 TRANSFERT DE LA CLE PRIVEE VERS / DEPUIS LE MODULE CRYPTOGRAPHIQUE

Le transfert de la clé privée d'AC depuis le module cryptographique est soumis à un dispositif mettant en œuvre le partage de secrets.

### 6.2.7 STOCKAGE DE LA CLE PRIVEE DANS UN MODULE CRYPTOGRAPHIQUE

Un module cryptographique est utilisé par l'AC pour stocker sa clé privée comme énoncé en 6.2.1.1.

## 6.2.8 METHODE D'ACTIVATION DE LA CLE PRIVEE

### 6.2.8.1 CLE PRIVEE D'AC

L'activation des clés privées d'AC dans les modules cryptographiques est contrôlée via des données d'activation et nécessite l'intervention de plusieurs conservateurs de secrets, ayant un rôle de confiance.

### 6.2.8.2 CLE PRIVEE DES SERVICES APPLICATIFS

La méthode d'activation de la clé privée du serveur dépend du dispositif utilisé. L'activation de la clé privée du serveur doit au minimum être contrôlée via des données d'activation (cf. chapitre 6.4) et doit permettre de répondre aux exigences définies pour le niveau de sécurité considéré.

Les clés privées des Porteurs ne disposent pas de données d'activation. Néanmoins, dans le cas de la génération de bi-clés en central, la clé privée est transmise au responsable du composant technique au format PKCS#12 protégée par un mot de passe. Ce mot de passe est utilisé lors de l'installation de la clé privée sur le composant technique. Il est réutilisé lors de la réinstallation de la clé privée.

Certificat « Serveur SSL et client SSL » : Dans le cas des tablettes dPad et smartphones dPhone, la clé privée est stockée et protégée dans une carte microSD cryptographique. L'accès aux informations contenues dans cette carte ne peut se faire que par l'utilisation d'un code d'authentification au démarrage du smartphone.

## 6.2.9 METHODE DE DESACTIVATION DE LA CLE PRIVEE

### 6.2.9.1 CLE PRIVEE D'AC

La désactivation des clés privées d'AC dans le module cryptographique HSM peut être réalisée dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

### 6.2.9.2 CLE PRIVEE DES SERVICES APPLICATIFS

Les conditions de désactivation de la clé privée d'un serveur doivent permettre de répondre aux exigences définies pour le niveau de sécurité considéré.

## 6.2.10 METHODE DE DESTRUCTION DES CLES PRIVEES

### 6.2.10.1 CLE PRIVEE D'AC

La méthode de destruction des clés privées d'AC permet de répondre aux exigences de sécurité pour le niveau de sécurité considéré. En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé doit être systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

#### 6.2.10.2 CLE PRIVEE DES SERVICES APPLICATIFS

*6.2.10.2.1 Certificat de profil « Accès distant»*

Les clés privées des services applicatifs sont stockées et gérées dans les postes Itinéo, les tablettes dPad, les smartphones dPhone et les boîtiers. La destruction de la clé privée est à la charge du responsable du composant technique selon les moyens mis à sa disposition par le composant technique.

*6.2.10.2.2 Certificat de profil « Serveur SSL » et « Client SSL »*

Les clés privées des services applicatifs sont stockées et gérées dans les composants techniques. La destruction de la clé privée est à la charge du responsable du composant technique selon les moyens mis à sa disposition par le composant technique.

*6.2.10.2.3 Certificat de profil « Signature de code »*

Les clés privées des services applicatifs sont stockées et gérées dans les postes de travail. La destruction de la clé privée est à la charge du responsable de certificat selon les moyens mis à sa disposition par les postes de travail.

*6.2.10.2.4 Certificat de profil « Signature de configuration »*

Les clés privées des services applicatifs sont stockées et gérées dans les postes de travail. La destruction de la clé privée est à la charge du responsable du composant technique selon les moyens mis à sa disposition par le composant technique.

*6.2.10.2.5 Certificat de profil « Signature jeton d'horodatage »*

En fin de vie de la clé privée d'un serveur, la méthode de destruction de cette clé privée permet de répondre aux exigences de sécurité pour le niveau de sécurité considéré.

### 6.2.11 NIVEAU DE QUALIFICATION DU MODULE CRYPTOGRAPHIQUE ET DES DISPOSITIFS D'AUTHENTIFICATION

Les modules HSM utilisés sont certifiés Critères Communs EAL 4+.

## 6.3 AUTRES ASPECTS DE LA GESTION DES BI-CLES

### 6.3.1 ARCHIVAGE DES CLES PUBLIQUES

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

### 6.3.2 DUREES DE VIE DES BI-CLES ET DES CERTIFICATS

La bi-clé et le certificat d'AC couvert par la présente PC a une durée de vie de :

- 9 ans pour AC INFRASTRUCTURE
- 2082 jours pour AC INFRASTRUCTURE 2
- 9 ans pour AC INFRASTRUCTURE 3

Les bi-clés et les certificats des services applicatifs couverts par la présente PC ont une durée de vie de 3 ans.

La fin de validité du certificat d'AC doit être postérieure à la fin de vie des certificats de services applicatifs qu'elle émet.

## 6.4 DONNEES D'ACTIVATION

### 6.4.1 GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION

#### 6.4.1.1 GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION CORRESPONDANT A LA CLE PRIVEE DE L'AC

La génération et l'installation des données d'activation des modules cryptographiques de l'IGC, au sein desquels sont mises en œuvre les clés des AC, 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 GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION CORRESPONDANT A LA CLE PRIVEE DES SERVICES APPLICATIFS

Le certificat et la bi-clé associée est envoyée à l'opérateur d'AE sous format PKCS#12 protégé par un mot de passe généré aléatoirement. Ces PKCS#12 et mot de passe sont envoyés aux opérateurs d'AE qui les transmettent au Responsable de Certificat.

Sans objet pour les certificats « signature de configuration » et « jeton d'horodatage ».

### 6.4.2 PROTECTION DES DONNEES D'ACTIVATION

#### 6.4.2.1 PROTECTION DES DONNEES D'ACTIVATION CORRESPONDANT A LA CLE PRIVEE 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 (lors de la Cérémonie des Clés).

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 DONNEES D'ACTIVATION CORRESPONDANT AUX CLES PRIVEES DES SERVICES APPLICATIFS

Quand les données d'activation des dispositifs de protection des clés privées des serveurs sont générées par l'AC, elles sont protégées en intégrité et en confidentialité jusqu'à la remise aux RC. Si ces données d'activation sont également sauvegardées par l'AC, elles sont protégées en intégrité et en confidentialité.

Le cas échéant mot de passe protégeant le PKCS#12 doit être conservé dans un endroit sécurisé dont l'accès est protégé.

Pour le certificat « Accès distant » : le code d'authentification utilisé pour accéder aux informations contenues dans la carte microSD de la tablette dPad ou du smartphone dPhone ne doit rester connu que du titulaire de la tablette.

### 6.4.3 AUTRES ASPECTS LIES AUX DONNEES D'ACTIVATION

Sans objet.

## 6.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

### 6.5.1 EXIGENCES DE SECURITE TECHNIQUE SPECIFIQUES AUX SYSTEMES 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 aux serveurs hébergeant les AC Déléguées,
- identification et authentification forte des administrateurs centraux pour l'accès à l'IGC,
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels,
- gestion des comptes des administrateurs centraux au niveau de l'application IGC,
- gestion des comptes des détenteurs de rôles de confiance au niveau des systèmes des serveurs des AC Déléguées,
- 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 des ACD,
- fonctions d'audits (imputabilité des actions effectuées),
- gestion des incidents,
- protection en confidentialité, en intégrité et en disponibilité des clés nécessaires au fonctionnement des ACD.

### 6.5.2 NIVEAU DE QUALIFICATION DES SYSTEMES INFORMATIQUES

Sans objet.

## 6.6 MESURES DE SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES

### 6.6.1 MESURES LIEES A LA GESTION DE LA SECURITE

L'Autorité Qualifiée est tenue informée de toute évolution majeure sur les systèmes des serveurs des ACD. Celle-ci est documentée et apparaît dans les procédures d'exploitation des ACD (document non public).

La configuration des systèmes des serveurs des ACD (systèmes d'exploitation, application IGC…), ainsi que toute modification et mise à niveau, sont documentées et contrôlées

### 6.6.2 NIVEAU D'EVALUATION SECURITE DU CYCLE DE VIE DES SYSTEMES

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

## 6.7 MESURES DE SECURITE RESEAU

L'Autorité de Certification s'engage à ce que les réseaux utilisés dans le cadre de l'IGC respectent les objectifs de sécurité informatique définis dans la DPC.

## 6.8 HORODATAGE / SYSTEME DE DATATION

La datation des évènements enregistrés par les différentes fonctions des ACD dans les journaux est basée sur l'heure système des serveurs hébergeant les AC et vérifiée avant toute utilisation avec une précision inférieure à 5 minutes. Il n'est pas mis en œuvre de mécanisme de synchronisation.

# 7 PROFIL DES CERTIFICATS, OCSP ET DES LCR

## 7.1 PROFIL DES CERTIFICATS

### 7.1.1 GABARIT DU CERTIFICAT « ACCES DISTANT »

#### 7.1.1.1 GÉNÉRALITÉS

Les certificats « Accès distant » respectent le format de base des certificats définis dans la recommandation x.509v3 et incluent au minimum les champs de base suivants :

| Champ | Valeur |
|---|---|
| Version | V3 |
| Serial number | Défini par Opentrust PKI |
| Issuer DN | CN= AC INFRASTRUCTURE N<br>OU= 0002 12000601000025<br>O= MINISTERE DES AFFAIRES ETRANGERES<br>C = FR |
| Subject DN | CN= <objetLDAP@diplomatie.gouv.fr><br>OU= 0002 12000601000025<br>O= MINISTERE DES AFFAIRES ETRANGERES<br>C = FR<br>Cf. partie 3.2 pour plus de précisions |
| NotBefore | YYMMDDHHMMSS |
| NotAfter | YYMMDDHHMMSS + 3 ans |
| Public Key Algorithm | sha2WithRSAEncryption (1.2.840.113549.1.1.13) |

Tableau 17 : Certificat « accès distant » - Champs de base - AC INFRASTRUCTURE

*Nota : La règle d'évolution de la valeur « CN » dans le champ « Issuer DN » est décrite dans la partie 5.6*

#### 7.1.1.2 EXTENSIONS DE CERTIFICAT

Les certificats « accès distant » émis pour les services applicatifs comprendront les extensions suivantes :

| Champ | Obligatoire (O/N) | Critique (O/N) | Valeur |
|---|---|---|---|
| Subject Key Identifier | O | N | <Valeur de Hachage> |

| | | | |
|---|---|---|---|
| Authority Key Identifier | O | N | <Valeur de Hachage> |
| Key Usage | O | O | digital signature |
| Certificate Policies | O | N | 1.2.250.1.214.69.3.1.3.1.21.1 |
| CRL Distribution Points | O | N | URL=http://crl.diplomatie.gouv.fr/AC_Infrastructure_N /Crl/AC_INFRASTRUCTURE_N.crl |
| Extended Key Usage | O | N | |

Tableau 18 : Certificat « accès distant » - Extensions standards - AC INFRASTRUCTURE

*Nota : La règle d'évolution de N dans le champ «CRL Distribution Points » est décrite dans la partie 5.6*

### 7.1.2 GABARIT DU CERTIFICAT « SERVEUR SSL » ET « CLIENT SSL »

#### 7.1.2.1 GÉNÉRALITÉS

Les certificats d'authentification « **Serveur SSL** » respectent le format de base des certificats définis dans la recommandation x.509v3 et incluent au minimum les champs de base suivants :

| Champ | Valeur |
|---|---|
| Version | V3 |
| Serial number | Défini par Opentrust PKI |
| Issuer DN | CN= AC INFRASTRUCTURE N<br>OU= 0002 12000601000025<br>O= MINISTERE DES AFFAIRES ETRANGERES<br>C = FR |
| Subject DN | CN= <FQDN du serveur><br>OU= 0002 12000601000025<br>O= MINISTERE DES AFFAIRES ETRANGERES<br>C = FR |
| NotBefore | YYMMDDHHMMSS |
| NotAfter | YYMMDDHHMMSS + 3 ans |
| Public Key Algorithm | sha2WithRSAEncryption (1.2.840.113549.1.1.13) |

Tableau 19 : Certificat Serveur SSL - Champs de base - AC INFRASTRUCTURE

*Nota : La règle d'évolution de la valeur « CN » dans le champ « Issuer DN » est décrite dans la partie 5.6*

Les certificats d'authentification « **Client SSL** » respectent le format de base des certificats définis dans la recommandation x.509v3 et incluent au minimum les champs de base suivants :

| Champ | Valeur |
|---|---|
| Version | V3 |
| Serial number | Défini par Opentrust PKI |
| Issuer DN | CN= AC INFRASTRUCTURE N<br>OU= 0002 12000601000025<br>O= MINISTERE DES AFFAIRES ETRANGERES<br>C = FR |
| Subject DN | CN= <Nom du composant technique><br>OU= 0002 12000601000025<br>O= MINISTERE DES AFFAIRES ETRANGERES<br>C = FR |
| NotBefore | YYMMDDHHMMSS |
| NotAfter | YYMMDDHHMMSS + 3 ans |
| Public Key Algorithm | sha2WithRSAEncryption (1.2.840.113549.1.1.13) |

Tableau 20 : Certificat Client SSL - Champs de base - AC INFRASTRUCTURE

*Nota : La règle d'évolution de la valeur « CN » dans le champ « Issuer DN » est décrite dans la partie 5.6*

#### 7.1.2.2 EXTENSIONS DE CERTIFICAT

Les certificats d'authentification « **Serveur SSL** » émis pour les services applicatifs comprendront les extensions suivantes :

| Champ | Obligatoire (O/N) | Critique (O/N) | Valeur |
|---|---|---|---|
| Subject Key Identifier | O | N | <Valeur de Hachage> |
| Authority Key Identifier | O | N | <Valeur de Hachage> |
| Key Usage | O | O | digitalSignature, keyEnciphrement |
| Certificate Policies | O | N | 1.2.250.1.214.69.3.1.3.1.21.1 |
| CRL Distribution Points | O | N | URL=http://crl.diplomatie.gouv.fr/AC_Infrastructure_N/Crl/AC_INFRASTRUCTURE_N.crl |
| Extended Key Usage | O | N | id-kp-serverAuth |

*Nota : La règle d'évolution de N dans le champ «CRL Distribution Points » est décrite dans la partie 5.6*

Les certificats d'authentification « **Client SSL** » émis pour les services applicatifs comprendront les extensions suivantes :

| Champ | Obligatoire (O/N) | Critique (O/N) | Valeur |
|---|---|---|---|
| Subject Key Identifier | O | N | <Valeur de Hachage> |
| Authority Key Identifier | O | N | <Valeur de Hachage> |
| Key Usage | O | O | DigitalSignature |
| Certificate Policies | O | N | 1.2.250.1.214.69.3.1.3.1.21.1 |
| CRL Distribution Points | O | N | URL=http://crl.diplomatie.gouv.fr/AC_Infrastructure_N /Crl/AC_INFRASTRUCTURE_N.crl |
| Extended Key Usage | O | N | id-kp-clientAuth |

Tableau 21 : Certificat Client SSL - Extensions standards - AC INFRASTRUCTURE

*Nota : La règle d'évolution de N dans le champ «CRL Distribution Points » est décrite dans la partie 5.6*

## 7.1.3 GABARIT DU CERTIFICAT « SIGNATURE DE CODE »

### 7.1.3.1 GÉNÉRALITÉS

Les certificats « Signature de code » respectent le format de base des certificats définis dans la recommandation x.509v3 et incluent au minimum les champs de base suivants :

| Champ | Valeur |
|---|---|
| Version | V3 |
| Serial number | Défini par Opentrust PKI |
| Issuer DN | CN= AC INFRASTRUCTURE N<br>OU= 0002 12000601000025<br>O= MINISTERE DES AFFAIRES ETRANGERES<br>C = FR |
| Subject DN | CN= [Nom de l'organisme].[Nom du bureau responsable du serveur].[Nom du service applicatif]<br>OU= 0002 12000601000025 |

| | |
|---|---|
| | O= MINISTERE DES AFFAIRES ETRANGERES<br>C = FR |
| NotBefore | YYMMDDHHMMSS |
| NotAfter | YYMMDDHHMMSS + 3 ans |
| Public Key Algorithm | sha2WithRSAEncryption (1.2.840.113549.1.1.13) |

Tableau 22 : Certificat « signature de code » - Champs de base - AC INFRASTRUCTURE

*Nota : La règle d'évolution de la valeur « CN » dans le champ « Issuer DN » est décrite dans la partie 5.6*

#### 7.1.3.2 EXTENSIONS DE CERTIFICAT

Les certificats « Signature de code » émis pour les services applicatifs comprendront les extensions suivantes :

| Champ | Obligatoire (O/N) | Critique (O/N) | Valeur |
|---|---|---|---|
| Subject Key Identifier | O | N | <Valeur de Hachage> |
| Authority Key Identifier | O | N | <Valeur de Hachage> |
| Key Usage | O | O | digital signature |
| Certificate Policies | O | N | 1.2.250.1.214.69.3.1.3.1.21.1 |
| CRL Distribution Points | O | N | URL=http://crl.diplomatie.gouv.fr/AC_Infrastructure_N/Crl/AC_INFRASTRUCTURE_N.crl |
| Extended Key Usage | O | N | 1.3.6.1.5.5.7.3.3 - id_kp_codeSigning |

Tableau 23 : Certificat « signature de code » - Extensions standards - AC INFRASTRUCTURE

*Nota : La règle d'évolution de N dans le champ «CRL Distribution Points » est décrite dans la partie 5.6*

### 7.1.4 GABARIT DU CERTIFICAT « SIGNATURE DE CONFIGURATION »

#### 7.1.4.1 GÉNÉRALITÉS

Les certificats « Signature de configuration » respectent le format de base des certificats définis dans la recommandation x.509v3 et incluent au minimum les champs de base suivants :

| Champ | Valeur |
|---|---|

| | |
|---|---|
| Version | V3 |
| Serial number | Défini par Opentrust PKI |
| Issuer DN | CN= AC INFRASTRUCTURE N<br>OU= 0002 12000601000025<br>O= MINISTERE DES AFFAIRES ETRANGERES<br>C = FR |
| Subject DN | CN= <objetLDAP@diplomatie.gouv.fr><br>OU= 0002 12000601000025<br>O= MINISTERE DES AFFAIRES ETRANGERES<br>C = FR |
| NotBefore | YYMMDDHHMMSS |
| NotAfter | YYMMDDHHMMSS + 3 ans |
| Public Key Algorithm | sha2WithRSAEncryption (1.2.840.113549.1.1.13) |

Tableau 24 : Certificat « signature de configuration » - Champs de base - AC INFRASTRUCTURE

*Nota : La règle d'évolution de la valeur « CN » dans le champ « Issuer DN » est décrite dans la partie 5.6*

#### 7.1.4.2 EXTENSIONS DE CERTIFICAT

Les certificats « Signature de configuration » émis pour les services applicatifs comprendront les extensions suivantes :

| Champ | Obligatoire (O/N) | Critique (O/N) | Valeur |
|---|---|---|---|
| Subject Key Identifier | O | N | <Valeur de Hachage> |
| Authority Key Identifier | O | N | <Valeur de Hachage> |
| Key Usage | O | O | digital signature |
| Certificate Policies | O | N | 1.2.250.1.214.69.3.1.3.1.21.1 |
| CRL Distribution Points | O | N | URL=http://crl.diplomatie.gouv.fr/AC_Infrastructure_N/Crl/AC_INFRASTRUCTURE_N.crl |
| Extended Key Usage | O | N | 1.3.6.1.5.5.7.3.3 - id_kp_codeSigning |

Tableau 25 : Certificat « signature de configuration » - Extensions standards - AC INFRASTRUCTURE

*Nota : La règle d'évolution de N dans le champ «CRL Distribution Points » est décrite dans la partie 5.6*

### 7.1.5 GABARIT DU CERTIFICAT « SIGNATURE JETON D'HORODATAGE »

#### 7.1.5.1 GÉNÉRALITÉS

Les certificats « Signature de jetons d'horodatage » respectent le format de base des certificats définis dans la recommandation X.509v3 et incluent au minimum les champs de base suivants :

| Champ | Valeur |
|---|---|
| Version | V3 |
| Serial number | Défini par Opentrust PKI |
| Issuer DN | CN= AC INFRASTRUCTURE N<br>OU= 0002 12000601000025<br>O= MINISTERE DES AFFAIRES ETRANGERES<br>C = FR |
| Subject DN | CN= FQDN du serveur<br>OU= 0002 12000601000025<br>O= MINISTERE DES AFFAIRES ETRANGERES<br>C = FR<br>Subject Serial Number= <nom du VLAN><br>Adresse électronique = <assistance.dsi@diplomatie.gouv.fr> |
| NotBefore | YYMMDDHHMMSS |
| NotAfter | YYMMDDHHMMSS + 3 ans |
| Public Key Algorithm | sha2WithRSAEncryption (1.2.840.113549.1.1.13) |

Tableau 26 : Certificat « Signature de jetons d'horodatage » - Champs de base - AC INFRASTRUCTURE

*Nota : La règle d'évolution de la valeur « CN » dans le champ « Issuer DN » est décrite dans la partie 5.6*

#### 7.1.5.2 EXTENSIONS DE CERTIFICAT

Les certificats « Signature de jetons d'horodatage » émis pour les serveurs comprendront les extensions suivantes :

| Champ | Obligatoire (O/N) | Critique (O/N) | Valeur |
|---|---|---|---|
| Subject Key Identifier | O | N | <Valeur de Hachage> |
| Authority Key Identifier | O | N | <Valeur de Hachage> |
| Key Usage | O | O | Les bits « digitalSignature » et « nonRepudiation » doivent être à "1", tous les autres bits à "0". |
| Certificate Policies | O | N | 1.2.250.1.214.69.3.1.3.1.21.1 |
| CRL Distribution Points | O | N | URL=http://crl.diplomatie.gouv.fr/AC_Infrastructure_N/Crl/AC_INFRASTRUCTURE_N.crl |
| Extended Key Usage | O | N | id-kp-timeStamping |

Tableau 27 : Certificat « Signature de jetons d'horodatage » - Extensions standards - AC INFRASTRUCTURE

*Nota : La règle d'évolution de N dans le champ «CRL Distribution Points » est décrite dans la partie 5.6*

## 7.2 PROFIL DES LCR / LAR

### 7.2.1 NUMEROS DE VERSIONS

Les LCR émises par l'AC INFRASTRUCTURE utilisent la version 2 du format défini dans la norme [9594-8], le passage éventuel en version 3 sera notifié par une mise à jour de la présente PC sans changement de son OID.

Les champs de base sont les suivants :

| Champ | Description |
|---|---|
| Version | Version 2 |
| Signature | Sha256WithRSAEncryption |
| Issuer | CN= AC INFRASTRUCTURE N<br>OU= 0002 12000601000025<br>O= MINISTERE DES AFFAIRES ETRANGERES<br>C = FR |

| | |
|---|---|
| thisUpdate | Date d'émission de la LCR |
| nextUpdate | Date limite d'émission de cette LCR |
| revokedCertificates | Pour chaque certificat révoqué :<br>- Numéro de série du certificat<br>- Date de révocation du certificat |

Tableau 28 : Profil des LCR - Champs de base - AC INFRASTRUCTURE

*Nota : La règle d'évolution de la valeur « CN » dans le champ « Issuer DN » est décrite dans la partie 5.6*

La LCR dans sa forme finale est l'ensemble des éléments suivants :

| Champ | Description |
|---|---|
| signatureAlgorithm | Sha256WithRSAEncryption |
| Authority Key Identifier | L'identifiant de la clé publique de l'AC INFRASTRUCTURE N |
| CRL Number | Numéro de la liste de révocation |

Tableau 29 : LCR - Forme finale - AC INFRASTRUCTURE

### 7.2.2 LCR ET EXTENSION DES LCR

Sans objet.

## 7.3 PROFIL DES OCSP

### 7.3.1 DEFINITION DES OCSP

OCSP est un protocole en ligne pour valider un certificat numérique X.509. Ce protocole est standardisé par l'IETF dans la RFC 2560.

Ce protocole est une alternative à certains problèmes posés par les LCR dans un PKI. Le client n'a plus à communiquer qu'avec une seule entité : le répondeur OCSP afin de valider un certificat. Suite à l'envoi de la requête par le client, le répondeur OCSP constituera une réponse parmi les suivantes : bon, révoqué, inconnu.

### 7.3.2 PROFIL DE LA REQUETE OCSP

La requête OCSP émise par l'utilisateur de certificat, est codée en ASN.1 et peut être transportée par différents protocoles applicatifs (http, SMTP…).

Les champs de base sont les suivants :

| Champ | Description |
|---|---|
| Version | V1 |
| Requester Name | Optionnel : DN du demandeur |
| Request List | Liste des certificats spécifiés dans le RFC 2560 |
| Signature | Optionnelle : sha256 |
| Extensions | Optionnelles à préciser |

Tableau 30 : Profil des requêtes OCSP - Champs de base

### 7.3.3 PROFIL DE LA REPONSE OCSP

La réponse OCSP est émise par le répondeur OCSP.

Les champs de base sont les suivants :

| Champ | Description |
|---|---|
| Response Statuts | Spécifiée dans le RFC 2560 |
| Response Type | Id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1} |
| Version | V1 |
| Responder ID | DN du répondeur OCSP |
| Product At | Temps universel coordonné |
| List of Responses | Chaque réponse contiendra une identification du certificat :<br>- Statut des certificats (GOOD, REVOKED, UNKNOW)<br>- Date d'émission de la réponse OCSP<br>- Date limite d'émission de la réponse OCSP |
| Extensions | Optionnelles |
| Signature Algorithm | Sha256 |
| Signature | Présente |
| Certificates | Certificats applicables émis par le répondeur OCSP |

Tableau 31 : Profil des réponses OCSP - Champs de base

# 8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Ce chapitre ne concerne que les audits et évaluation de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

## 8.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

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, un audit interne global ou limité au périmètre de l'impact de la modification est réalisé.

Le Responsable des AC Déléguées fait aussi procéder régulièrement à un contrôle de conformité de l'ensemble de son IGC, a minima une fois tous les trois ans

## 8.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

Le contrôle d'un périmètre particulier de l'IGC (procédure, application, fonction, rôle) est assigné par 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 EVALUATEURS ET ENTITES EVALUEES

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

## 8.4 SUJETS COUVERTS PAR LES EVALUATIONS

Les audits internes portent sur un rôle, une procédure, une fonction des ACD, sur l'application IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques 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 EVALUATIONS

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : "réussite", "échec", "à confirmer". Selon l'avis rendu, les conséquences du contrôle sont les suivantes:

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

- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

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

## 8.6 COMMUNICATION DES RESULTATS

Les résultats des audits internes ne sont communiqués qu'à la discrétion des ACD.

# 9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

## 9.1 TARIFS

### 9.1.1 TARIFS POUR LA FOURNITURE OU LE RENOUVELLEMENT DE CERTIFICATS

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

### 9.1.2 TARIFS POUR ACCEDER AUX CERTIFICATS

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

### 9.1.3 TARIFS POUR ACCEDER AUX INFORMATIONS D'ETAT ET DE REVOCATION DES CERTIFICATS

L'accès aux LCR est libre en lecture.

### 9.1.4 TARIFS POUR D'AUTRES SERVICES

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

### 9.1.5 POLITIQUE DE REMBOURSEMENT

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

## 9.2 RESPONSABILITE FINANCIERE

Conformément à ses obligations, l'AC doit prendre les dispositions nécessaires pour couvrir, éventuellement financièrement, ses responsabilités liées à ses opérations et/ou activités.

### 9.2.1 COUVERTURE PAR LES ASSURANCES

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

### 9.2.2 AUTRES RESSOURCES

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

### 9.2.3 COUVERTURE ET GARANTIE CONCERNANT LES ENTITES UTILISATRICES

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

## 9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

### 9.3.1 PERIMETRE 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 INFORMATIONS HORS DU PERIMETRE DES INFORMATIONS CONFIDENTIELLES

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

### 9.3.3 RESPONSABILITES EN TERMES DE PROTECTION DES INFORMATIONS CONFIDENTIELLES

La présente PC ne formule pas d'exigence supplémentaire au respect de la législation et de la réglementation en vigueur sur le territoire français relatives à la protection des informations confidentielles.

## 9.4 PROTECTION DES DONNEES PERSONNELLES

### 9.4.1 POLITIQUE DE PROTECTION DES DONNEES 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'IGC 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 Libertés ».
Le récépissé de cette déclaration porte le numéro : 1245693.

### 9.4.2 INFORMATIONS A CARACTERE PERSONNEL

Les informations considérées comme personnelles sont les suivantes :

- les codes d'activation des cartes d'authentification administrateur des administrateurs de l'ACD ;
- les causes de révocation des certificats des services applicatifs ;
- le dossier d'enregistrement des RC.

### 9.4.3INFORMATIONS A CARACTERE NON PERSONNEL

Sont considérées comme non personnelles l'ensemble des informations n'étant pas identifiées comme personnelles.

### 9.4.4 RESPONSABILITE EN TERMES DE PROTECTION DES DONNEES PERSONNELLES

La présente PC ne formule pas d'exigence supplémentaire au respect de la législation et de la réglementation en vigueur sur le territoire français relatives à la protection des données personnelles.

### 9.4.5 NOTIFICATION ET CONSENTEMENT D'UTILISATION DES DONNEES PERSONNELLES

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

### 9.4.6 CONDITIONS DE DIVULGATION D'INFORMATIONS PERSONNELLES AUX AUTORITES 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 d'un administrateur peut faire l'objet d'une divulgation auprès de la hiérarchie de cet administrateur.

## 9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

La présente PC ne formule pas d'exigence supplémentaire au respect de la législation et la réglementation en vigueur sur le territoire français.

## 9.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

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

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ;
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent ;
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante) ;
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. partie 8) et l'organisme de qualification ;
- respecter les accords ou contrats qui les lient entre elles ou aux services applicatifs ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

### 9.6.1 AUTORITES DE CERTIFICATION

L'AC a pour obligation de :

- pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un service applicatif donné et que ce service applicatif a accepté le certificat, conformément aux exigences de la partie 4.4 ci-dessus ;
- garantir et maintenir la cohérence de sa DPC avec sa PC ;
- prendre toutes les mesures raisonnables pour s'assurer que ses services applicatifs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un service applicatif et l'AC est formalisée par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC est responsable de la conformité de sa Politique de Certification, avec les exigences émises dans la présente PC pour le niveau de sécurité considéré. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la présente PC, par elle-même ou l'une de ses composantes. Elle doit prendre les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique.

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

Par ailleurs, 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 ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de l'AC.

En cas de non-respect ponctuel des obligations décrites dans la présente PC, l'Administration se réserve le droit de refuser temporairement ou définitivement les certificats de l'AC conformément à la réglementation en vigueur.

### 9.6.2SERVICE D'ENREGISTREMENT

Cf. les obligations pertinentes du chapitre 9.6.1.

### 9.6.3RC

Le RC a le devoir de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- protéger sa clé privée par des moyens appropriés à son environnement ;
- protéger l'accès à sa base de certificats ;
- respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- informer l'AC de toute modification concernant les informations contenues dans son certificat ;
- faire, sans délai, une demande de révocation de son certificat auprès de l'AE, du MC de son entreprise ou de l'AC en cas de compromission ou de suspicion de compromission de sa clé privée (ou de ses données d'activation).

La relation entre le RC et l'AC ou ses composantes est formalisée par un engagement du RC visant à certifier l'exactitude des renseignements et des documents fournis. Ces informations s'appliquent également aux MC.

### 9.6.4 UTILISATEURS DE CERTIFICATS

Les utilisateurs de certificats doivent :

- vérifier et respecter l'usage pour lequel un certificat a été émis ;
- contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application ;
- pour chaque certificat de la chaîne de certification, du certificat du service applicatif jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

L'AC ne doit pas émettre dans sa propre PC d'obligations supplémentaires, par rapport aux obligations de la présente PC, à l'encontre des utilisateurs de la sphère publique.

### 9.6.5 AUTRES PARTICIPANTS

Sans objet.

## 9.7 LIMITE DE GARANTIE

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

## 9.8 LIMITE DE RESPONSABILITE

L'objectif de l'AC INFRASTRUCTURE N est d'émettre des certificats à destination services applicatifs du MINISTÈRE.
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 un de ses rôles de confiance 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.

## 9.9 INDEMNITES

Les indemnités sont à l'appréciation des tribunaux compétents.

## 9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

### 9.10.1 DUREE DE VALIDITE

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

### 9.10.2 FIN ANTICIPEE DE LA VALIDITE

La publication d'une nouvelle version du RGS peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC correspondante.
En fonction de la nature et de l'importance des évolutions apportées au RGS, le délai de mise en conformité sera arrêté conformément aux modalités prévues par la réglementation en vigueur.
De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

### 9.10.3 EFFETS DE LA FIN DE VALIDITE ET CLAUSES RESTANT APPLICABLES

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

## 9.11 NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

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 de qualification.

## 9.12 AMENDEMENTS A LA PC

### 9.12.1 PROCEDURES D'AMENDEMENTS

La procédure d'amendement à la PC est initiée par l'AC INFRASTRUCTURE.
En cas de changement important, l'AC s'engage à faire appel à un auditeur pour en contrôler l'impact.

### 9.12.2 MECANISME ET PERIODE D'INFORMATION SUR LES AMENDEMENTS

Les tiers utilisateurs de certificat peuvent prendre connaissance des amendements au moyen du site web *http://crl.diplomatie.gouv.fr*. Les ACD seront également informées de ces amendements.

### 9.12.3 CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE

L'OID de la présente 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, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) ou du document décrivant les profils associés se traduira par une évolution de l'OID. En particulier, des modifications de forme n'entraîneront pas une modification de l'OID.
Le nouvel OID, si nouvel OID il y a, apparaîtra dans tout nouveau certificat émis par l'ACD. Ainsi, les tiers utilisateurs de certificat pourront clairement distinguer quels certificats correspondent à quelles exigences.

## 9.13 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

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

## 9.14 JURIDICTIONS COMPETENTES

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

## 9.15 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

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).

Les textes législatifs et réglementaires applicables à la présente PC sont les suivants :

| | |
|---|---|
| [CNIL] | Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 |
| [ORDONNANCE] | Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives |
| [DécretRGS] | Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 |
| [LSQ] | Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne. |
| [DIRSIG] | Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques. |
| [LCEN] | Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés. |
| [SIG] | Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique |

L'AC est notamment soumise aux dispositions prévues par l'article 31 de la [LSQ] concernant la remise des clés privées des porteurs, si celles-ci sont séquestrées par l'AC

## 9.16 DISPOSITIONS DIVERSES

### 9.16.1 ACCORD GLOBAL

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

### 9.16.2 TRANSFERT D'ACTIVITES

Cf. partie 5.8.

### 9.16.3 CONSEQUENCES D'UNE CLAUSE NON VALIDE

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

### 9.16.4 APPLICATION ET RENONCIATION

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

### 9.16.5 FORCE MAJEURE

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

## 9.17 AUTRES DISPOSITIONS

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

# 10 ANNEXE 1 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC

## 10.1 EXIGENCES SUR LES OBJECTIFS DE SECURITE

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

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

## 10.2 EXIGENCES SUR LA QUALIFICATION

Sans objet.

# 11 ANNEXE 2 : EXIGENCES DE SECURITE DU DISPOSITIF D'AUTHENTIFICATION

## 11.1 EXIGENCES SUR LES OBJECTIFS DE SECURITE

Le dispositif « accès distant », utilisé par le responsable du composant technique pour stocker et mettre en œuvre la clé privée doit répondre aux exigences de sécurité suivantes :

- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une authentification qui ne peut être falsifiée sans la connaissance de la clé privée ;
- assurer la fonction d'authentification pour le Porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

## 11.2 EXIGENCES SUR LA QUALIFICATION

Sans objet.

# 12 ANNEXE 3 : DEFINITIONS ET ACRONYMES

## 12.1 LISTE DES ACRONYMES UTILISES

Le tableau qui suit recense des acronymes susceptibles d'être utilisés pendant le déroulement du projet :

| Acronyme | Signification |
|---|---|
| **AC** | Autorité de Certification |
| **ACR** | Autorité de Certification Racine |
| **ACI** | Autorité de Certification Intermédiaire |
| **AE** | Autorité d'Enregistrement |
| **ANSSI (ex-DCSSI)** | Agence Nationale de la Sécurité des Systèmes d'Information (ex-Direction Centrale de la Sécurité des Systèmes d'Information) |
| **ARL (voir LAR)** | *Authority Revocation List* |
| **CAS** | *Central Authentication Service* |
| **CEN** | Comité Européen de Normalisation |
| **CERTA** | Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques |
| **CGU** | Conditions Générales d'Utilisation |
| **CMC** | *Certificate Management over CMS* |
| **CMS** | *Card Management System* |
| **CNIL** | Commission Nationale de l'Informatique et des Libertés |
| **CRL (voir LCR)** | *Certificate Revocation List* |
| **CSR** | *Certificate Signing Request* |
| **DCOM** | *Distributed Component Object Model* |
| **DN** | *Distinguished Name* |
| **DPC** | Déclaration des Pratiques de Certification |
| **EAL** | *Evaluation Assurance Level* |
| **ETSI** | *European Telecommunications Standards Institute* |
| **FQDN** | *Fully Qualified Distinguished Name* |
| **http** | *Hypertext Transfer Protocol* |
| **HTTPS** | *Hypertext Transfer Protocol Secure* |
| **HSM** | *Hardware Security Module* |
| **IETF** | *Internet Engineering Task Force* |
| **IGC** | Infrastructure de Gestion de Clés |
| **IGC/A** | Infrastructure de Gestion de Clés de l'Administration de l'État français |
| **IHM** | Interface Homme-Machine |
| **KC** | *Key Ceremony* (ou Cérémonie des Clés) |
| **LAR** | Liste des Autorités Révoquées (ARL – *Authority Revocation List*) |
| **LCR** | Liste des Certificats Révoqués (CRL – *Certificate Revocation List*) |

| Acronyme | Signification |
|---|---|
| **LDAP** | *Lightweight Directory Access Protocol* |
| **MAE** | Ministère des Affaires Étrangères |
| **OC** | Opérateur de Certification |
| **OID** | *Object Identifier* |
| **OS** | *Operating System* |
| **OU** | *Organizational Unit* |
| **PC** | Politique de Certification |
| **PKCS** | *Public Key Cryptography Standards* |
| **PKI (voir IGC)** | *Public Key Infrastructure* |
| **PP** | Profil de Protection |
| **PRA** | Plan de Reprise d'Activité |
| **PRIS** | Politique de Référencement Intersectorielle de Sécurité |
| **RCAS** | Responsable du Certificat d'Authentification Serveur |
| **RGS** | Référentiel Général de Sécurité |
| **RSA** | *Rivest Shamir Adelman* |
| **SC** | Service de Certification technique |
| **SHA** | *Secure Hash Algorithm* |
| **SI** | Système d'Information |
| **SP** | Service de Publication |
| **URL** | *Uniform Resource Locator* |

Tableau 32 : Acronymes utilisés

## 12.2 DEFINITION DES TERMES UTILISES

Les termes utilisés pendant le déroulement du projet et leur définition sont présentés dans le tableau suivant :

| Acronyme | Signification |
|---|---|
| Administrateur | Personne autorisée par l'AC à gérer les droits d'accès logiciels à l'Autorité, avec la granularité suivante : gestion de la liste d'administrateurs, gestion des droits d'accès aux différentes composantes de l'Autorité pour chacun des administrateurs. De ce fait, détenteur lui-même de droits d'accès précis aux différentes composantes de l'Autorité, l'administrateur est autorisé à utiliser et configurer les fonctionnalités correspondantes des composantes de l'Autorité. |
| Agent | Personne physique agissant pour le compte d'une autorité administrative. |
| Algorithme RSA | Inventé en 1978 par Ronald L. Rivest, Adi Shamir et Leonard M. Adleman. Il peut être utilisé pour chiffrer des informations et/ou pour les signer (signature numérique). |
| Application utilisatrice | Service applicatif exploitant les certificats émis par l'Autorité de Certification. |

| Acronyme | Signification |
|---|---|
| | Dans le cadre de ce projet, la messagerie électronique est une application utilisatrice de certificats de chiffrement er de signature. |
| Autorité de Certification (AC) | Entité, composante de base de l'IGC, qui délivre des certificats à une population de porteurs ou à d'autres composants d'infrastructure. |
| Autorité de certification Déléguée | Autorité de certification dont le certificat est signé par l'Autorité de Certification racine.<br>Une Autorité de Certification déléguée signe les certificats finaux qu'elle émet. |
| Autorité de Certification racine | Autorité de Certification dont le certificat est auto signé.<br>L'Autorité de Certification racine signe les certificats des Autorités de Certification filles. |
| Autorité d'Enregistrement (AE) | Entité responsable du traitement des demandes et du cycle de vie des certificats. |
| Bi-clé | Ensemble constitué d'une clé publique et d'une clé privée, formant une paire indissociable utilisée par un algorithme cryptographique asymétrique. |
| Cérémonie des clés (ou *Key Ceremony*) | Opération pendant laquelle se font la création et l'activation des bi-clés des composantes de la PKI, en présence de témoins et éventuellement d'un huissier. |
| Certificat électronique | Fichier électronique (structuré au format x509 v3) attestant qu'un bi-clé appartient à la personne physique. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique et le bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. |
| Chaîne de certification | Ensemble ordonné de certificats nécessaires pour valider la filiation d'un certificat porteur. La chaîne de confiance du certificat final comprend le certificat de l'AC racine Diplomatie, le certificat de l'AC fille AC Messagerie Sécurisée et le certificat final du porteur, émis par l'AC Messagerie Sécurisée. |
| Clé privée | Composant confidentiel d'un bi-clé, connu uniquement de son propriétaire et utilisé par lui seul pour déchiffrer une donnée dont il est destinataire ou pour signer des données dont il est l'auteur. |
| Clé publique | Composant non confidentiel d'un bi-clé, pouvant être communiqué à tous les membres d'une population. Une clé publique permet de chiffrer des données à destination du porteur du bi-clé. Elle permet également de vérifier une signature apposée par le porteur. |
| *Common Name (CN)* | Champ du gabarit d'un certificat contenant une information identifiant le porteur. |
| Compromission | Une clé privée est dite compromise lorsqu'elle est connue par d'autres personnes que celles habilitées à l'utiliser. |
| Déclaration des Pratiques de Certification (DPC) | Ensemble des pratiques à mettre en œuvre pour satisfaire aux exigences de la PC.<br>Ce document est confidentiel. |
| Dispositif de création de signature | Il s'agit du dispositif matériel et/ou logiciel utilisé par le porteur pour stocker et mettre en œuvre sa clé privée de signature. |
| *Distinguished* | Nom distinctif X.500 du porteur de certificat. |

| Acronyme | Signification |
|---|---|
| *Name (DN)* | |
| Données d'activation (ou code PIN) | Données qui permettent l'activation d'une clé privée cryptographique d'AC ou de porteur. |
| Enregistrement | Opération qui consiste pour un Opérateur d'Enregistrement à prendre en compte une demande de certificat pour un porteur. |
| Entité | Désigne une autorité administrative ou une entreprise au sens le plus large. |
| Habilitation | Droit attribué à un administrateur de l'IGC pour réaliser des opérations techniques ou fonctionnels (audit, suivi logs, etc.). |
| Infrastructure de Gestion de Clés (IGC) | Ensemble de composants, fonctions et procédures dédiés à la gestion de bi-clés et de certificats. |
| Infrastructure de Gestion de Clés Diplomatie (IGC Diplomatie) | Ensemble de services de certification électronique mis en place au sein du Ministère des Affaires Étrangères, hébergeant l'Autorité de Certification racine et assurant la certification d'Autorités de Certification déléguées gérées par le MAE. |
| Infrastructure de Gestion de la Confiance de l'Administration (IGC/A) | Ensemble de services de certification électronique, participant à la validation par l'État français des certificats électroniques utilisés dans les échanges entre les usagers et les autorités administratives et entre les autorités administratives. |
| Liste des Certificats Révoqués | Certificate Revocation List (CRL) ou Liste de Certificats Révoqués (LCR)<br>Liste des numéros de certificats non expirés ayant fait l'objet d'une révocation. La LCR est signée par l'Autorité de Certification pour assurer son intégrité et son authenticité. |
| Ministère (MAE) | Ministère des Affaires Étrangères |
| Module cryptographique | Dispositif matériel, de type HSM, permettant de protéger les clés privées et de procéder à des calculs cryptographiques mettant en œuvre ces clés. |
| *Object IDentifier* (OID) | Identifiant alphanumérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.<br>Dans le cadre du projet, il permet de référencer la documentation relative à l'IGC (PC et DPC). |
| Opérateur d'Enregistrement | Personne nommée par un Responsable d'Enregistrement et chargée de réaliser toutes les opérations de gestion du cycle de vie des certificats (enregistrement, renouvellement, révocation, re-génération) |
| Opérateur d'Enregistrement Central (OEC) | Personne nommée par le Responsable d'Enregistrement et chargée de réaliser des opérations d'administration et de configuration de l'AE (configuration des profils, etc.). |
| Organisme | Entité de rattachement d'un porteur. |
| *Organizational Unit (OU) (ou Unité* | Champ du gabarit d'un certificat contenant l'identifiant officiel de l'établissement qui a émis le certificat.<br>En France, il s'agit du n° SIREN ou n° SIRET de l'établissement. |

| Acronyme | Signification |
|---|---|
| *Organisationnelle)* | |
| PKCS (*Public Key Cryptographic Standards*) | Ensemble de standards de chiffrement relatifs aux clefs publiques.<br>PKCS#12 : Conteneur cryptographique contenant la clé privée, le certificat et un mot de passe. Le mot de passe permet d'activer la clé privée.<br>PKCS#7 : Conteneur cryptographique embarquant un certificat et parfois l'ensemble de la chaîne de certification associée.<br>PKCS#10 : Fichier cryptographique contenant le requête de certificat, envoyée à l'Autorité de Certification pour signature. |
| Politique de Certification (PC) | Ensemble de règles qui indique les conditions d'applicabilité d'un certificat pour une communauté donnée ou pour des applications ayant des besoins de sécurité communs. |
| Porteur | Personne physique, support matériel ou Autorité de Certification, identifié dans le certificat et détentrice de la clé privée correspondant à la clé publique présente dans ce certificat.<br>▪ Dans le cas où l'Autorité de Certification génère un certificat final, le porteur peut être une personne physique ou un support matériel (ex : serveur). Le porteur détient alors la clé privée.<br>▪ Dans le cas où l'Autorité Racine certifie la clé publique de l'Autorité Déléguée, le porteur est une Autorité. Il fournit la preuve qu'il possède la clé privée de l'Autorité Déléguée via le certificat auto-signé de l'Autorité Déléguée ou via une demande de certification au format PKCS#10. |
| Processus centralisé | La clé est générée et détenue par l'Autorité de Certification (AC). Ce processus est compatible avec le séquestre des clés de chiffrement. |
| Profil (de certificat) | Gabarit de certificat associé à un usage et/ou une population de porteurs.<br>Dans le cadre de ce projet, il y a un seul profil « Accès distant »<br>Ce terme est aussi utilisé dans l'interface utilisateur et administrateur de l'IGC. |
| Publication (de LCR) | Opération consistant à mettre à disposition des porteurs et des applications utilisatrices (application de messagerie) une LCR, afin de leur permettre de vérifier le statut d'un certificat. |
| Publication (de certificat) | Opération qui consiste à mettre à disposition les certificats valides (non révoqués, non expirés) à l'ensemble des personnes en ayant besoin.<br>Cela concerne exclusivement les certificats de chiffrement utilisés dans le cadre de la messagerie sécurisée. |
| Re-génération (d'un certificat) | Demande de certificat faisant suite à la révocation d'un certificat porteur, qui donne lieu à l'émission d'un nouveau certificat. Tous les motifs de révocation ne permettent pas la re-génération : une nouvelle demande faisant suite à une révocation pour des motifs de non-respect des conditions d'utilisation ou de départ de l'utilisateur est traitée comme une demande initiale. |
| Renouvellement (d'un certificat) | Opération effectuée en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat pour un porteur. |
| Responsable de l'Autorité de | Personne physique représentant l'entité fonctionnelle Autorité de Certification. Il définit et contrôle l'application de la Politique de |

| Acronyme | Signification |
|---|---|
| Certification (RA) | Certification. Il nomme les Responsables d'Enregistrement. |
| Responsable du certificat d'authentification serveur (RCAS) | Personne physique responsable du certificat d'authentification du serveur, notamment de l'utilisation de ce certificat et de la bi-clé correspondante, pour le compte de l'entité dont dépend le serveur informatique identifié dans le certificat. |
| Révocation (d'un certificat) | Opération de mise en opposition demandée par le porteur du certificat ou un Mandataire de Certification, et dont le résultat est la suppression de la garantie d'engagement de l'Autorité de Certification sur un certificat donné, avant la fin de sa période de validité.<br>L'IGC DIPLOMATIE permet la révocation de certificats en masse (par batch). |
| Signature électronique | Une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies dans le second alinéa de l'article 1316-4 du Code Civil. Une signature électronique est un cryptogramme issu du chiffrement d'un condensat de fichier à l'aide d'une clé privée, lequel condensat étant obtenu par application d'une fonction de hachage (algorithme de codage irréversible) sur ledit fichier. Une signature accompagne généralement le fichier qui a été signé et en garantit l'intégrité et la non-répudiation par l'émetteur. |
| Tiers utilisateur | Utilisateur ou système faisant confiance à un certificat. |

*Tableau 33 : Définition des termes utilisés*

**Fin du document**