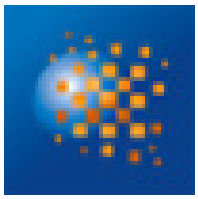
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'EUROPE ET DES
AFFAIRES ÉTRANGÈRES

Politique de Certification de l'AC RACINE DIPLOMATIE

Certificats de l'Autorité de Certification Racine Diplomatie



OID : 1.2.250.1.214.69.3.1.1.1.1.2

Cotation Archive : E.3.1.1.1

Version 2.0.4 du 06/09/2019

État : validé

Suivi des mises à jour			
Version	**Date**	**Auteur**	**Commentaire(s)**
2.0.1	17/07/2015	Solucom	Création au format RGSv2
2.0.2	26/05/2016	Solucom	Renouvellement des AC
2.0.3	20/07/2018	MEAE	Mise à jour du document
2.0.4	06/09/2019	MEAE	Mise à jour du document

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]	☑	☐	IGC/A – Politique de Certification concernant les Autorités de certification racines gouvernementales version 2.2 OID : 1.2.250.1.223.1.1.2.

1 INTRODUCTION

1.1 PRESENTATION GENERALE

1.1.1 OBJET DU DOCUMENT

Présentation de l'AC RACINE DIPLOMATIE

Pour assurer la confidentialité des échanges d'information entre ses représentations à l'étranger et les services de l'Administration centrale, le ministère des Affaires étrangères (MAE) dispose de moyens de communications chiffrés pour les échanges formels (inter-applicatifs ou inter-personnels).
Dans ce cadre, il a étendu les fonctionnalités de l'Infrastructure de Gestion de Clefs existante, dite IGC DIPLOMATIE, de façon à fédérer à long terme les différentes AC présentes au sein du ministère des Affaires étrangères, et à étendre les services de cette IGC DIPLOMATIE à de nouveaux usages, notamment aux échanges chiffrés inter-Administrations.

L'AC RACINE DIPLOMATIE est destinée à certifier plusieurs Autorités de Certification existantes ou à venir. En particulier les premières AC rattachées sont :

- AC UTILISATEURS de niveau RGS * délivrant des certificats d'authentification, de signature et de chiffrement pour des porteurs personnes physiques, principalement pour des applications de messagerie ;
- AC UTILISATEURS RENFORCEE de niveau RGS ** délivrant des certificats d'authentification, de signature et de chiffrement sur carte à puce pour des porteurs personnes physiques ;
- AC INFRASTRUCTURE de niveau RGS * délivrant des certificats d'authentification pour des ressources informatiques du ministère des Affaires étrangères ou d'autres entités.

D'autre part, l'AC RACINE DIPLOMATIE est rattachée au domaine de confiance interministériel défini par l'IGC/A. Les certificats émis par l'IGC/A permettent d'identifier officiellement les Autorités de Certification des administrations de l'État français. Ils attestent également de la qualité des pratiques de gestion des clefs publiques mises en œuvre par ces Autorités. Ils sont délivrés au terme d'un audit et peuvent être révoqués en cas de défaillance.
Cette démarche de rattachement de l'AC RACINE DIPLOMATIE du MAE au domaine de confiance de l'IGC/A s'inscrit dans le cadre de l'article 10 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les Autorités Administratives et entre les Autorités Administratives.

Présentation de la Politique de Certification AC RACINE DIPLOMATIE

Le présent document fait partie d'un ensemble de documents décrivant les politiques de certification définies dans le cadre du projet AC RACINE DIPLOMATIE.
Il spécifie les exigences applicables :

- à l'AC Racine, pour :
  - la génération et le renouvellement de ses clés,
  - la certification des clés publiques des AC Déléguées demandant leur rattachement, et la révocation des certificats des AC Déléguées émis par l'Autorité Racine,
  - la génération, le renouvellement et la révocation de ses propres certificats d'administrateurs,
  - la protection des communications entre les composantes de l'AC.
- aux AC Déléguées, pour :
  - la génération et le renouvellement de leurs clés ainsi que pour la gestion des demandes de certificats auprès de l'Autorité Racine,
- à l'application IGC, pour :

- la garantie de l'intégrité des codes mobiles utilisés par l'application IGC.

Le présent document constitue la Politique de Certification (PC) de l'Autorité de Certification RACINE DIPLOMATIE. L'Autorité de Certification Racine sera désignée dans la suite du document par « l'Autorité de Certification Racine » ou « ACR ». Les Autorités de Certification Déléguées seront désignées comme « AC déléguée » ou « ACD ».

La politique est définie indépendamment des détails de l'environnement utilisé pour la mise en œuvre de l'IGC. Ces exigences sont établies de façon à être conformes à celles de l'IGC/A pour la certification de l'AC RACINE DIPLOMATIE. Les procédures de certification sont détaillées dans un document appelé Déclaration des Pratiques de Certification (DPC), distinct de la PC, qui décrit comment ces exigences sont atteintes en pratique.

Cette PC est donc associée à la DPC relative à l'Autorité de Certification AC Racine. Contrairement à la PC, la consultation de la DPC n'a pas vocation à être publique et doit faire l'objet d'une autorisation préalable.

La gestion du cycle de vie des certificats couvre toutes les opérations relatives au cycle de vie d'un certificat, depuis son émission jusqu'à la fin de vie de ce certificat.

Le but de la présente PC est de fournir aux porteurs de certificats, auditeurs, maîtres d'œuvre etc. les informations relatives aux garanties offertes par les certificats, ainsi que les règles d'utilisation de ces certificats. Ce document a été établi sur la base de la « Politique de Certification Type, certificats électroniques de services applicatifs » en version 3.0, fournie par le Référentiel Général de Sécurité (RGS) en version 2.0.

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 RACINE DIPLOMATIE

La PC relative aux certificats délivrés par l'AC RACINE DIPLOMATIE est identifiée par l'OID suivant : 1.2.250.1.214.69.3.1.1.1.1.2
Le dernier chiffre permet de faire évoluer le numéro de version du document.

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, authentification pour l'authentification des administrateurs de l'IGC aux interfaces de l'IGC et des utilisateurs externes au MAE à l'application Diplomatie. 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 RENFORCEE
        - Elle délivre des certificats destinés à des porteurs 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 ».

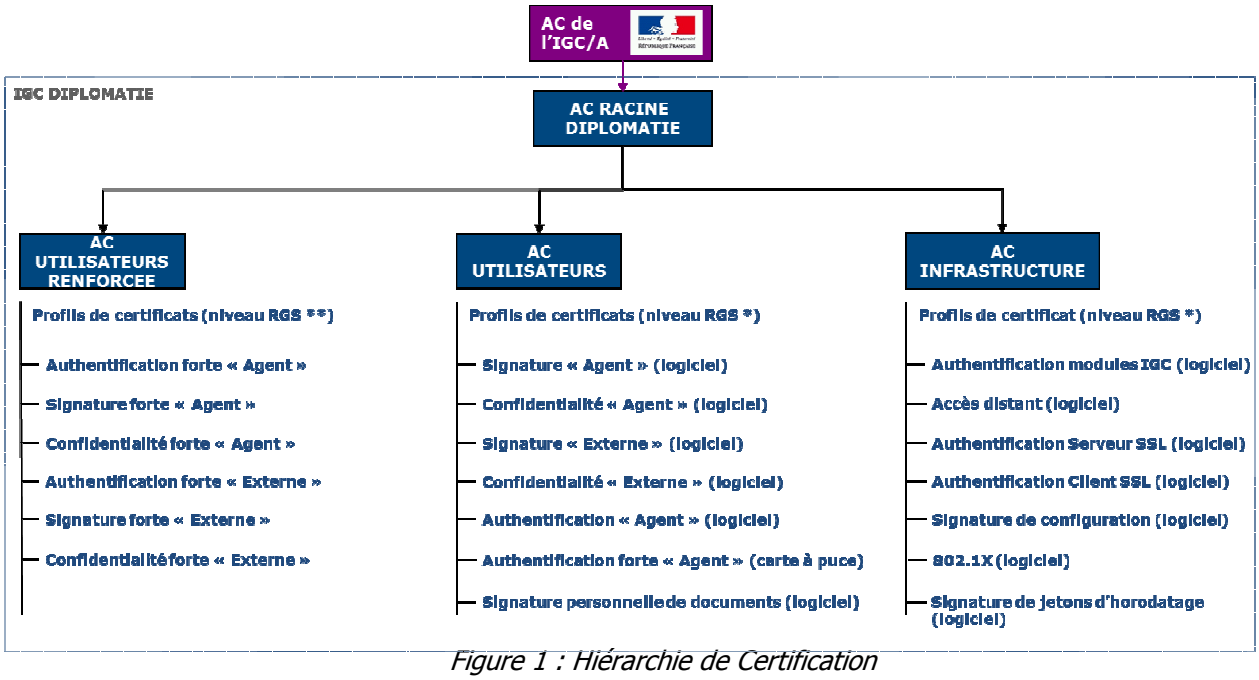


Figure 1 : Hiérarchie de Certification

Le rôle d'Autorité de Certification Racine est assuré par le Directeur des Systèmes d'Information, qui encadre l'ensemble des équipes de la DSI.
L'Autorité de Certification Racine (ACR) a en charge la fourniture des prestations de gestion des certificats des ACD et de ses administrateurs tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) et s'appuie pour cela sur une infrastructure technique : une Infrastructure de Gestion de Clés (IGC).
Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats :

Fonction de génération des certificats :

Cette fonction génère les certificats à partir des informations transmises par l'Autorité d'Enregistrement.

Fonction de remise au Responsable du Certificat (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'AC traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

Fonction d'information sur l'état des certificats :

Cette fonction fournit aux tiers utilisateurs de certificats des informations sur l'état des certificats (révoqués, non révoqués). Cette fonction est mise en œuvre par la publication d'informations de révocation sous forme de LCR.

L'AC 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...).

1.4.1.1 AUTORITÉ DE CERTIFICATION DÉLÉGUÉE

Chaque Autorité de Certification Déléguées (ACD) doit procéder à la génération de sa bi-clé et la faire certifier par l'ACR. Elle doit aussi demander la révocation de son certificat en cas de compromission réelle ou suspectée de sa clé privée, de changement de nom de l'AC ou de cessation d'activité.
Les responsabilités incombant à chaque ACD et relatives à la délivrance et à la gestion des certificats qu'elle émet sont décrites dans les Politiques de Certification de cette AC.
Ce document complète ces Politiques en décrivant les fonctions nécessaires à la création, au renouvellement et à la révocation des certificats de chaque ACD.
Les fonctions assurées par les Autorités Déléguées sont :
Fonction de création d'une demande de certificat d'une ACD :
Cette fonction assure la génération initiale d'une bi-clé et la création d'un fichier de demande de certificat pour une nouvelle Autorité Déléguée, soit au format PKCS#10, soit au format X509 dans le cas d'un certificat auto-signé.
Fonction de demande de renouvellement du certificat d'une ACD :
Cette fonction assure la génération d'une nouvelle bi-clé et la création d'un fichier de demande de certificat pour une Autorité Déléguée existante, soit au format PKCS#10, soit au format X509 dans le cas d'un certificat auto-signé.

Fonction de demande de révocation du certificat d'une ACD :
Cette fonction assure la demande de révocation d'un certificat d'ACD.

1.4.2 AUTORITE D'ENREGISTREMENT LOCALE AUPRES DE L'AC RACINE

Le rôle d'AEL est assuré par les administrateurs centraux de l'AC Racine.
L'AEL de l'ACR permet l'enregistrement des ACD et de ses administrateurs centraux, la remise des certificats et la prise en compte des demandes de révocation pour les certificats émis. Pour cela, elle assure les fonctions suivantes :
Fonction d'enregistrement des demandes de certificats :
Cette fonction assure la vérification des informations d'identification des demandeurs d'un certificat, la vérification des données à inclure dans le certificat, la constitution du dossier d'enregistrement y correspondant, et la transmission de cette demande de certificat à l'Autorité de Certification.
Fonction de remise du certificat aux demandeurs :
Cette fonction remet le certificat à son ou à ses demandeurs une fois qu'il a été généré par l'Autorité de Certification.
Fonction de gestion des révocations :
Dans le cadre de cette fonction, l'AEL prend en compte les demandes de révocation pour transmission et traitement par l'AC Racine.

1.4.3RESPONSABLE 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.

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

- demander la révocation d'un certificat.

1.4.3.1 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.

1.4.4UTILISATEURS DE CERTIFICATS

Les utilisateurs concernent les utilisateurs des certificats émis selon la présente Politique de Certification :

- certificat auto-signé de l'AC RACINE DIPLOMATIE ;
- certificats des Autorités Déléguées émis par l'AC RACINE DIPLOMATIE ;

- certificats de composantes de chaque AC ;
- certificats d'authentification des administrateurs centraux de l'AC RACINE DIPLOMATIE.

Les utilisateurs sont les systèmes et les applications informatiques :

- soit utilisant des certificats porteurs ou serveurs émis par l'une des Autorités Déléguées rattachées à l'AC RACINE DIPLOMATIE, et à ce titre nécessitant les certificats du chemin de certification,
- soit composantes de l'application IGC et à ce titre acceptant les certificats d'autres composantes et/ou des administrateurs de l'AC RACINE DIPLOMATIE.

1.4.4.1 COMPOSANTE DE L'IGC

La décomposition en fonctions de l'IGC est présentée au chapitre 1.3.1« Autorités de certification ». Les composantes de l'IGC mettant en œuvre ces fonctions sont présentées dans la DPC de l'AC.

1.4.4.2 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

L'AC Racine émet une seule gamme de certificats à destination des ACD. Ces certificats sont conformes aux exigences décrites dans cette présente Politique de Certification.

Ils peuvent faire l'objet des usages suivants :

- Signature de certificats destinés aux AC déléguées
- Signature des Listes de Certificats Révoqués (CRL)

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

Le certificat de l'ACR est limité aux usages suivants :

- Auto-signature de l'ACR.
- Signature des certificats des ACF demandeuses et conformes aux exigences de raccordement à l'Autorité de Certification Racine.
- Signature des Listes d'Autorités Révoquées (ARL). Le terme « CRL » sera préféré dans la suite du document.

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 RACINE DIPLOMATIE 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 RACINE DIPLOMATIE
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 75700 PARIS 07 SP
Personne physique responsable	Fabien FIESCHI - DSI	37 quai d'Orsay 75700 PARIS 07 SP
Entité gérant la conformité de la DPC avec la PC	COSSI	37 quai d'Orsay 75700 PARIS 07 SP
Entité représentant le Comité d'Approbation des Politiques de Certification	Nadir SOUABEG – RSSI	37 quai d'Orsay 75700 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 RACINE DIPLOMATIE 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 RACINE DIPLOMATIE publie les informations suivantes à destination des tiers utilisateurs de certificats :

- la Politique de Certification de l'ACR en cours de validité (le présent document),
- les versions antérieures de la présente Politique de Certification, tant que des certificats émis selon ces versions sont en cours de validité,
- les profils des certificats de l'ACR, des ACD, et des LCR émises par l'ACR,
- 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 paragraphe §6 et accessible par le protocole http,
- l'adresse (URL) permettant d'obtenir des informations concernant l'AC RACINE DIPLOMATIE,
- en cas de rattachement à l'IGC/A, les certificats de l'ACR émis par l'IGC/A,
- en cas de rattachement à l'IGC/A, l'adresse (URL) permettant d'obtenir des informations concernant l'IGC/A, et notamment les certificats auto-signés de l'IGC/A.

Information publiée	Emplacement de publication
PC	http://crl.diplomatie.gouv.fr
LCR	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 RACINE DIPLOMATIE	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 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 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 X509v3, 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 X501.

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 AUTO-SIGNE DE L'ACR

Le nom distinctif de l'AC RACINE DIPLOMATIE est construit à partir des composants suivants :

- C = FR
- O = MINISTERE DES AFFAIRES ETRANGERES
- OU = 0002 12000601000025
- CN = AC RACINE DIPLOMATIE

3.1.2.2 CERTIFICAT POUR UNE AC DELEGUEE

L'AC Déléguée en cours de certification choisit le contenu du champ « DN» qui sera présent dans son certificat établi par l'AC RACINE DIPLOMATIE.

Durant toute la durée de vie de l'AC RACINE DIPLOMATIE, un DN attribué à une ACD ne peut être attribué à une autre ACD. L'AC Racine vérifie l'unicité du DN demandé avant de valider la demande de certificat de l'AC Déléguée.

3.1.2.3 CERTIFICAT D'AUTHENTIFICATION ADMINISTRATEUR DE L'AC RACINE

Les types de noms employés, la nécessité d'employer des noms explicites et l'exigence d'unicité des noms sont respectés.
En particulier, le nom commun du porteur (CN) est vérifié à partir des prénom et nom de l'état civil tel que porté sur la carte d'identité officielle et en cours de validité présentée par le porteur lors de son enregistrement auprès de l'administrateur central réalisant l'enregistrement. Dans le cas où l'état-civil du porteur comporte plusieurs prénoms, seuls le ou les prénoms usuels du porteur sont inclus dans le CN en sus du nom.
L'UID du porteur, égal à l'ID arobas du SI du MAE, est obtenu à l'aide d'une interrogation en ligne du système arobas du SI du MAE.
Durant toute la durée de vie de l'AC RACINE DIPLOMATIE, un DN attribué à un administrateur ne peut être attribué à un autre administrateur. L'entité AC vérifie l'unicité de l'UID demandé avant de valider la demande de certificat d'authentification administrateur.

Les éléments d'identification des administrateurs font partie du dossier d'enregistrement qui sera conservé par le FSSI. Le FSSI conservera en particulier une photocopie de la carte d'identité présentée par le porteur.

3.1.3 PSEUDONYMISATION OU ANONYMISATION DES SERVICES APPLICATIFS

Sans objet.

3.1.4 REGLES D'INTERPRETATION DES DIFFERENTES FORMES DE NOM

Sans objet.

3.1.5 UNICITE DES NOMS

Cf. 3.1.2.

L'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'Autorité de Certification Racine.

Les DN des AC Déléguées (champ « Subject ») permettent d'identifier de manière unique le porteur du certificat au sein l'Espace de Confiance du ministère.

Les autres attributs du DN ne sont pas soumis à un format en particulier ;

L'AE se charge de fournir aux AC déléguées un numéro d'identifiant, puis veille à la cohérence du DN proposé dans la requête de certification.

3.1.6 IDENTIFICATION, AUTHENTIFICATION ET ROLE DE MARQUES DEPOSEES

Sans objet pour les marques déposées.

L'AC est responsable de l'unicité des noms de ses services applicatifs et de la résolution des litiges éventuels relatifs aux noms de services.

3.2 VALIDATION INITIALE DE L'IDENTITE

La validation initiale de l'identité du ministère, en tant qu'entité à l'origine des demandes de certificat pour l'AC Racine et ses AC déléguées, est effectuée en face à face, lors d'une procédure formelle appelée « cérémonie des clés ».

3.2.1 METHODES POUR PROUVER LA POSSESSION DE LA CLE PRIVEE

La génération des bi-clés des AC déléguées étant effectuée sous contrôle de l'ACR, la preuve de possession de la clé privée est automatiquement acquise.

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

L'identification des AC déléguées est réalisée par un face-à-face entre les responsables des AC déléguées et le responsable de l'ACR. Ce face-à-face est réalisé au cours de la cérémonie des clés, en produisant un titre d'identité délivré ou reconnu par l'Administration française.

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

3.3.1 IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT COURANT

L'identification et la validation pour un renouvellement courant d'un certificat sont effectuées de la même manière que lors d'une demande initiale (cf. chapitre 3.2. «Validation initiale de l'identité»).

3.3.2 IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT APRES REVOCATION

L'identification et la validation pour un renouvellement après révocation d'un certificat sont effectuées de la même manière que lors d'une demande initiale (chapitre 3.2. « Validation initiale de l'identité »).

3.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

Les demandes de révocation des certificats émis par l'ACR sont réalisées en face-à-face avec l'AE sur présentation d'un formulaire signé par l'entité responsable de l'AC déléguée. La validation de l'identité et de l'autorité de la personne physique à l'origine de la demande sont vérifiées par l'AE.
La révocation d'un certificat d'AC déléguée émis par l'ACR peut être aussi déclenchée par l'entité responsable de l'ACR dans le cas de non-respect des exigences de l'IGC par cette AC déléguée. L'entité responsable de l'AC déléguée est ensuite prévenue dans les plus brefs délais de cette décision.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 DEMANDE DE CERTIFICAT

4.1.1 ORIGINE D'UNE DEMANDE DE CERTIFICAT

- Certificat d'AC Délégué : Tout agent du Ministère identifié comme responsable d'une AC dont la PC et la DPC sont conformes à cette PC, peut soumettre une demande de certification à l'AE de l'ACR.
- Certificat d'administrateur de l'AC Racine : Cf. chapitre 4.2.

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

Cf. chapitre 4.2.

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 GENERATION D'UNE BI-CLE ET D'UN CERTIFICAT AUTO-SIGNE DE L'ACR

La génération des bi-clés de l'ACR est réalisée dans le cadre d'une cérémonie des clés.
Le but de cette cérémonie est de générer la clé de signature de l'ACR ainsi qu'un certificat racine auto-signé, de récupérer la valeur du certificat auto-signé à des fins de publication et de déclarer l'ACR opérationnelle.
La génération de la clé de signature de l'AC Racine doit être réalisée au sein d'un module cryptographique, conforme aux exigences du paragraphe 6.2.1 du document [2].

La cérémonie implique la présence d'au moins les personnes tenant les rôles de confiance suivants, outre le maître de cérémonie :

- Témoins de l'Autorité Administrative, garants du déroulement conforme au scénario de la cérémonie établi ;
- Opérateurs de l'IGC et des modules cryptographiques, garants du fait que les systèmes (matériels, logiciels et modules cryptographiques) sont correctement configurés et opérationnels ;
- Responsable sécurité pour la cérémonie, garant du bon déroulement de la cérémonie sur le plan de la sécurité ;
- Détenteurs de secrets et de supports sensibles.

L'AC Racine s'engage à établir le scénario complet de la cérémonie. Ce document n'est pas public.
L'AC Racine s'engage à émettre des procès-verbaux pour chaque étape importante de la Cérémonie, marquant notamment la conformité de la cérémonie déroulée, et l'engagement des détenteurs de secrets à respecter les règles de conservation des secrets remis. Ces documents ne sont pas publics.
La publication du certificat auto-signé de l'Autorité Racine par l'AC marque l'acceptation de ce certificat par celle-ci.

4.2.1.2 GENERATION D'UN CERTIFICAT POUR UNE AC DELEGUEE

L'AC Déléguée doit s'assurer auprès de l'AA de l'ACR que le nom qu'elle propose d'utiliser pour s'identifier n'est pas déjà réservé pour une autre AC Déléguée : l'AC Déléguée propose donc ce nom puis l'AA, grâce aux informations dont elle dispose, signale à l'AC Déléguée que ce nom est déjà utilisé si c'est le cas. Dans ce cas, la demande de certification n'est pas transmise à l'Autorité de Certification.

La demande de certification de la clé publique d'une AC Déléguée doit se faire lors d'un face-à-face, en la présence du responsable sécurité de l'AC Déléguée et d'au moins un témoin de l'Autorité Administrative de l'ACD et signataire du procès-verbal de la cérémonie de génération de la clé de l'AC Déléguée et qui atteste par sa présence l'accord de l'AA de l'ACD.

Cas 1 : génération d'un certificat à partir d'un fichier PKCS#10 émis par l'AC Déléguée
Les opérations suivantes :

- génération des bi-clés d'une ACD et émission de la demande de certificat correspondante,
- installation du certificat suite à sa génération par l'AC RACINE DIPLOMATIE

s'inscrivent dans le cadre d'une cérémonie des clés d'ACD. Le but de cette cérémonie est de générer une bi-clé ainsi qu'un fichier de demande de certificat, et de créer un procès-verbal de demande de certificat.

Le résultat de la première opération sert à constituer le dossier d'enregistrement présenté à l'administrateur central de l'AC Racine. Il est constitué :

- d'un procès-verbal signé de la cérémonie de génération de la clé de l'AC Déléguée et incluant l'empreinte de la CSR dont la certification est demandée à l'AC RACINE DIPLOMATIE,
- d'un fichier PKCS#10 signé, afin de prouver la possession de la clé privée.

Le résultat de la seconde opération donne lieu à l'établissement d'un procès-verbal signé.

Cas 2 : génération d'un certificat à partir d'un certificat auto-signé émis par l'AC Déléguée
Les opérations suivantes :

- génération des bi-clés d'une ACD et émission du certificat auto-signé d'ACD,
- installation du certificat suite à sa génération par l'AC RACINE DIPLOMATIE

s'inscrivent dans le cadre d'une cérémonie des clés d'ACD. Le but de cette cérémonie est de générer une bi-clé ainsi qu'un certificat auto-signé, et de créer un procès-verbal de demande de certificat.

Le résultat de la première opération sert à constituer le dossier d'enregistrement présenté à l'administrateur central de l'AC Racine. Il est constitué :

- d'un procès-verbal signé de la cérémonie de génération de la clé de l'AC Déléguée et incluant l'empreinte du certificat dont la certification est demandée à l'AC RACINE DIPLOMATIE,
- du certificat auto-signé de l'AC Déléguée, afin de prouver la possession de la clé privée

Le résultat de la seconde opération donne lieu à l'établissement d'un procès-verbal signé.

Dans tous les cas :
La cérémonie implique la présence d'au moins les personnes tenant les rôles suivants :

- Témoins de l'Autorité Administrative, garants du déroulement conforme de la cérémonie ;
- Opérateurs de l'AC Déléguée et des modules cryptographiques, garants du fait que les systèmes (matériels, logiciels et modules cryptographiques) sont correctement configurés et opérationnels ;
- Responsable sécurité pour la cérémonie, garant du bon déroulement de la cérémonie sur le plan de la sécurité.
- Détenteurs de secrets et de supports sensibles.

L'ACD s'engage à établir un descriptif complet de chaque cérémonie. Ce document n'est pas public.
L'ACD s'engage à émettre des procès-verbaux pour chaque étape importante du processus. Ces documents ne sont pas publics.
L'opérateur de l'ACR doit remettre au responsable sécurité de la Cérémonie de l'ACD le certificat une fois qu'il a été généré.
L'utilisation du certificat généré pour l'Autorité Déléguée par le responsable Sécurité de l'ACD marque l'acceptation de celui-ci.

L'Autorité d'Enregistrement conservera les dossiers d'enregistrement papier.

4.2.1.3 GENERATION D'UN CERTIFICAT D'AUTHENTIFICATION ADMINISTRATEUR DE L'AC RACINE

L'authentification du nouvel administrateur par l'administrateur assurant l'enregistrement est réalisée lors d'un face-à-face physique, à partir de la carte d'identité officielle et en cours de validité présentée par le nouvel administrateur.
La bi-clé est générée par la carte d'authentification administrateur du porteur lors du face-à-face avec l'administrateur central assurant l'enregistrement.
Le certificat est ensuite émis et remis au porteur sous contrôle de l'administrateur central.
L'utilisation du certificat généré par le nouvel administrateur marque l'acceptation de celui-ci.

4.2.2 ACCEPTATION OU REJET DE LA DEMANDE

L'utilisation du certificat généré marque l'acceptation de celui-ci.

4.2.3 DUREE D'ETABLISSEMENT D'UN CERTIFICAT

La durée de traitement d'une demande de certificat nécessitant des opérations humaines, celle-ci ne peut être totalement automatisée. Ce traitement est néanmoins effectué au plus vite.

4.3 DELIVRANCE DU CERTIFICAT

4.3.1 ACTIONS DE L'AC CONCERNANT LA DELIVRANCE DU CERTIFICAT

Une cérémonie des clés est nécessaire à la délivrance de certificats aux AC déléguées.

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande, l'ACR, en qualité de service technique, déclenche les processus de génération et de préparation des différents éléments destinés au porteur. Les clés privées des AC déléguées sont générées au cours de la cérémonie des clés, sous contrôle de l'ACR.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres 4.12.1 et 6 ci-dessous, notamment la séparation des rôles de confiance (se reporter au chapitre 5.2).

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

Le certificat est remis en face-à-face au responsable de l'AC déléguée lors de la cérémonie des clés. Une copie du procès-verbal de la cérémonie des clés est remise au responsable de l'AC déléguée une fois le certificat émis.

4.4 ACCEPTATION DU CERTIFICAT

4.4.1 DEMARCHE D'ACCEPTATION DU CERTIFICAT

L'acceptation des certificats est matérialisée par la signature du procès-verbal de la cérémonie des clés au cours de laquelle les certificats des AC déléguées sont générés. Les responsables des AC déléguées sont chargés de vérifier l'exactitude des informations contenues dans les certificats avant acceptation.

4.4.2 PUBLICATION DU CERTIFICAT

La publication des certificats des AC déléguées n'incombe pas à l'ACR.

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

La notification des autres entités lors de l'émission d'un certificat est effectuée par l'AC déléguée, et n'incombe pas à l'ACR.

4.5 USAGE DE LA BI-CLE ET DU CERTIFICAT

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

L'utilisation de la clé privée et du certificat associé est strictement limitée aux usages définis dans le chapitre 1.5. Les services applicatifs doivent respecter strictement les usages autorisés des bi-clés et des certificats.

L'usage autorisé de la bi-clé du service applicatif et du certificat associé doit par ailleurs être indiqué dans le certificat lui-même, via les extensions concernant les usages des clés (se référer au chapitre 7).

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

Cf. chapitre précédent et chapitre 1.5.

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

4.6 RENOUVELLEMENT D'UN CERTIFICAT

Pour l'ACR 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 à la 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

Le déclenchement de la fourniture d'un nouveau certificat d'AC est à l'initiative de l'AC déléguée.

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

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre 3.3. « Identification et validation d'une demande de renouvellement des clés » ci-dessus.

Pour les actions de l'AC, cf. chapitre 4.3.1. « Actions de l'AC concernant la délivrance du certificat ».

- Certificat d'AC déléguée :

La demande de renouvellement du certificat de la clé publique d'une AC Déléguée est soumise aux mêmes exigences que la demande de certification initiale d'une AC Déléguée. La valeur du champ qui identifie l'ACD, le champ DN, au sein du certificat issu du renouvellement doit être identique à la valeur du champ DN utilisée dans le certificat précédent. Le numéro de série du certificat issu du renouvellement est incrémenté, comparativement au numéro de série du certificat précédent.

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

Cf. chapitre 4.4.1. « Démarche d'acceptation du certificat ».

4.7.6 PUBLICATION DU NOUVEAU CERTIFICAT

Cf. chapitre 4.4.2. « Publication du certificat ».

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

Cf. chapitre 4.4.3. « Notification par l'AC aux autres entités de la délivrance du certificat ».

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 CERTIFICAT D'ADMINISTRATEUR DE L'AC RACINE

La demande de révocation se fait auprès d'un administrateur central de l'AC RACINE DIPLOMATIE.
La révocation peut être demandée :

- par le porteur : en cas de compromission réelle ou suspectée de sa clé privée associée au certificat émis par l'AC Racine,
- par l'AA ou l'AC : dans le cas où le porteur ne nécessite plus pour des raisons de service l'usage d'un tel certificat, ou en cas de manquements de la part du porteur aux exigences de la présente PC.

4.9.1.2 CERTIFICATS DE SERVICE APPLICATIF (AC DELEGUEE)

Les circonstances suivantes doivent être à l'origine de la révocation du certificat électronique d'une AC déléguée :

- Les informations du service figurant dans le certificat ne sont plus en conformité avec l'identité du service ou l'utilisation prévue dans le certificat (par exemple, modification du FQDN), ceci avant l'expiration normale du certificat ;
- Le RC n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le RC ou l'entité n'ont pas respecté leurs obligations découlant de la présente PC ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- La clé privée de l'ACF est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- La clé privée de l'ACF (ou son support) est détruite ou altérée ;

- L'arrêt définitif du service applicatif ou la cessation d'activité de l'entité du RC de rattachement du service applicatif.

- Fin de la relation contractuelle, hiérarchique ou réglementaire entre l'ACR et l'ACF avant la fin de validité du certificat, pour une raison ou pour une autre.

- Il n'y a plus de RC explicitement identifié responsable du certificat.

Lorsqu'une des circonstances ci-dessus se réalise et que l'ACR 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.

4.9.1.3 CERTIFICATS D'UN COMPOSANT D'IGC

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

- 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

La révocation d'un certificat peut émaner :

- Du porteur lui-même (RC de l'AC déléguée). Le formulaire de révocation à présenter à l'ACR est disponible sur le service de publication ;

- De l'ACR.

4.9.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE REVOCATION

4.9.3.1 REVOCATION D'UN CERTIFICAT D'ADMINISTRATEUR D'AC RACINE

Cf. Chapitre 4.9.1.

4.9.3.2 REVOCATION D'UN CERTIFICAT D'AC DELEGUEE

En cas de compromission réelle ou suspectée d'une clé d'AC Déléguée ou tout autre évènement motivant la révocation d'un certificat d'AC Déléguée, l'événement doit être déclaré par l'AC Déléguée auprès d'un administrateur de l'ACR sous 24 heures. Alors, dans un délai de 3 jours ouvrés, un administrateur de l'ACR doit procéder à la révocation du certificat de l'ACD (et l'information doit être publiée).
La révocation d'un certificat d'AC Déléguée peut également être demandée par l'AA de l'ACR, dans le cas où cette ACD ne respecterait pas les exigences prévues par la présente PC.

4.9.3.3 REVOCATION D'UN CERTIFICAT D'UNE COMPOSANTE DE L'IGC

La révocation du certificat d'ACR ne peut être décidée que par le responsable de cette présente Politique de Certification.

Lorsqu'une des circonstances ci-dessus se réalise et qu'un détenteur de rôle de confiance auprès de l'AC Racine en a connaissance, l'évènement doit être déclaré auprès d'un administrateur de l'ACR sous 24 heures. Alors l'AC :

- doit s'interdire de transmettre la clé privée lui ayant permis de signer le certificat en question ;
- doit prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- doit demander la révocation de son certificat auprès de l'IGC/A si cette dernière a certifié sa clé publique ;
- doit révoquer tous les certificats qu'elle a signés avec cette clé privée et qui seraient encore en cours de validité ;
- doit publier largement cette information (en ayant pour cible les Autorités Déléguées rattachées, les porteurs et tiers utilisateurs des certificats émis en utilisant la clé compromise), dans un délai de 3 jours. En particulier, l'information doit être publiée sur les sites web *http://crl.diplomatie.gouv.fr* (pour les CRL des AC et pour les autres informations).

Dans le cas d'une fin d'activité de l'ACR, la fin de vie effective de l'ACR prend effet 3 mois minimum après l'annonce de la fin de vie de l'activité.

Le détail des procédures à mettre en œuvre est défini dans le Plan de Reprise d'Activité. Ce document n'est pas public.

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) .

4.9.7 FREQUENCE D'ETABLISSEMENT DES LCR

La LAR (LCR qui ne contient que des certificats d'AC révoquées) est générée par anticipation tous les 6 mois et publiée toutes les 24 heures.
La durée de vie d'une LAR est de 7 jours, afin de disposer d'une période de recouvrement.
La LCR ou la LAR sont également publiées à chaque événement nécessitant une modification.

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.

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 3 : 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 relation contractuelle, hiérarchique ou réglementaire entre l'ACR et une AC Déléguée avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.
De plus, l'ACR doit révoquer un certificat électronique pour lequel il n'y a plus de RC explicitement identifié.

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

5.1.4 VULNERABILITE AUX DEGATS DES EAUX

Les locaux hébergeant l'ACR 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'ACR 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'ACR sont conservées dans une enceinte sécurisée, accessible aux seules personnes habilitées, autorisées et désignées à ces fins.
Les supports papier de l'ACR sont également conservés avec des mesures de sécurité compatibles avec leur niveau de sensibilité.
La DPC identifiee les différentes informations et données intervenant dans les activités de l'ACR, 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'ACR 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'ACR ne sont pas utilisés à d'autres fins avant destruction complète des informations liées à l'ACR 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'ACR, 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 de l'ACR sont :
Administrateur central :
Personne chargée de la configuration applicative et du maintien en conditions opérationnelles de l'application IGC, de l'habilitation des administrateurs centraux, ainsi que de l'analyse régulière des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission. Elle assure également le rôle d'AEL et réalise à ce titre les opérations de gestion des certificats émis par l'AC RACINE DIPLOMATIE.
Auditeur :
Personne désignée par l'Autorité Administrative dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par l'AC RACINE DIPLOMATIE par rapport à la Politique de Certification et à la Déclaration des Pratiques de Certification de l'AC RACINE DIPLOMATIE.
Autorité Qualifiée :
Personne chargée de la Sécurité de l'application IGC pour le compte de l'Autorité Administrative.
Responsable de l'application IGC :
Personne ayant reçu délégation par l'ACR de la mise en œuvre de la Politique de Certification et de la Déclaration des Pratiques de Certification de l'ACR, au niveau de l'application IGC. Sa responsabilité couvre l'ensemble des fonctions rendues par l'application IGC et des performances correspondantes.
Responsable Qualité :
Personne ayant reçu délégation par l'ACR de la vérification de la cohérence des actions des différents rôles décrits précédemment et de la qualité des processus de l'ACR.

5.2.1.1 ROLES DE CONFIANCE MUTUALISES

Ci-dessous sont décrites les fonctions assurées par ces rôles dans le cadre de l'IGC ou ayant une incidence sur les processus de l'IGC :
Administrateur sécurité :
Personne chargée d'assurer la gestion de la sécurité au niveau des systèmes.
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.
Responsable de salle :
Personne chargée de la gestion des accès physiques aux salles informatiques hébergeant l'infrastructure et aux équipements.

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

- de ses responsabilités relatives aux services de l'ACR ;
- 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'ACR 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'ACR, ainsi qu'aux logiciels, matériels et procédures d'exploitation applicables.
Les administrateurs centraux sont formés aux concepts et objectifs de l'ACR, 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'ACR 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'ACR 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 changement 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'ACR est enregistrée et un historique complet du dossier doit être conservé dans la base de données de l'ACR.
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'ACR, 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'événements 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 ACR, 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'ACR, 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'événements 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'ACR (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 certificats d'administrateurs de l'ACR, émis par l'ACR :
Les dossiers électroniques, les dossiers papier d'enregistrement et les certificats attachés doivent être conservés par l'application IGC pendant toute la vie de l'AC RACINE DIPLOMATIE sans être purgés.
Les dossiers d'enregistrement et les certificats attachés peuvent être présentés par l'ACR lors de toute sollicitation par les Autorités habilitées.
Ces dossiers doivent permettre de retrouver :

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

Certificats de composantes :
Les certificats de composantes doivent être 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.

Certificat auto-signé de l'ACR :
Le certificat auto-signé de l'ACR doivent être émis sitôt la génération de la clé de l'Autorité Racine. Il n'est donc pas constitué de dossiers d'enregistrement relatifs à ce certificat.

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'ACR 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 **Erreur ! Source du renvoi introuvable.**.

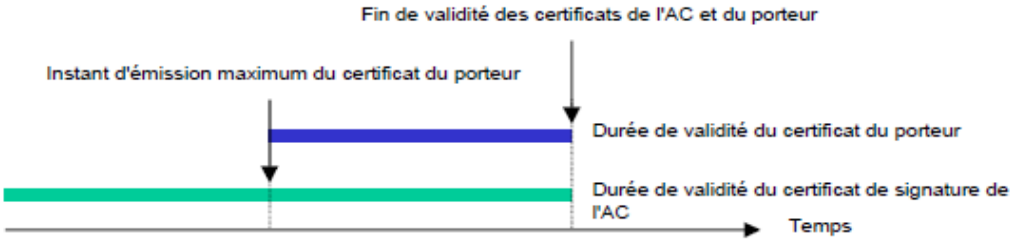


Figure 2 : Changement de clé d'AC

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.

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'ACR 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'ACR.
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'ACR 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'ACR 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'ACR 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 ACR.

5.7.4 CAPACITES DE CONTINUITE D'ACTIVITE SUITE A UN SINISTRE

En cas d'incident impactant l'infrastructure de l'ACR, les services de l'ACR 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'ACR 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'ACR :

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 de signature des Autorités est effectuée dans un environnement sécurisé.
Les clés de signature d'ACR sont générées et mises en œuvre dans un module cryptographique conforme aux exigences au paragraphe 6.2.1 du document [2].
La génération de la clé de signature de l'ACR 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.
L'initialisation de l'IGC et/ou la génération des clés de signature d'AC s'accompagnent de la génération de parts de secrets. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC.
Suite à leur génération, les parts de secrets sont remises à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AA. 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.
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

Sans objet.

6.1.2 TRANSMISSION DE LA CLE PRIVEE AU SERVICE APPLICATIF

Sans objet.

6.1.3 TRANSMISSION DE LA CLE PUBLIQUE A L'AC

La clé publique de l'ACD peut être transmise pour certification à l'ACR:

- soit via une CSR générée par l'ACD,
- soit via le certificat auto-signé de l'ACD,

Lors de la transmission de la clé publique d'une ACD vers l'ACR en vue de sa certification, son origine est authentifiée.

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

La clé publique de l'ACR est contenue dans un certificat signé par l'AC RACINE DIPLOMATIE (certificat auto-signé). La clé publique d'une ACD est diffusée dans un certificat signé par l'AC RACINE DIPLOMATIE.
La clé publique de l'AC RACINE DIPLOMATIE sera signée par l'IGC/A puis sera diffusée dans un certificat signé par l'IGC/A.

6.1.5 TAILLE DE CLES

Les clés des certificats suivants respectent les exigences de caractéristiques (tailles, algorithmes, etc.) du RGS et sont de type :

- pour le certificat auto-signé de l'AC RACINE DIPLOMATIE, RSA de 4096 bits
- pour les certificats des Autorités Déléguées, RSA de 2048 bits ou RSA de 4096 bits (suivant l'ACD)
- pour les certificats des composantes, RSA de 2048 bits
- pour les certificats des administrateurs de l'AC Racine, RSA de 2048 bits

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

Les équipements de génération des bi-clés utilisent des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

6.1.7 OBJECTIFS D'USAGE DE LA CLE

L'utilisation des clés privées des différentes Autorités et des certificats associés est strictement limitée à la signature de certificats et de LCRs.
L'utilisation des clés privées et des certificats des composantes associés est strictement limitée à la sécurisation des échanges entres composantes.
L'utilisation des clés privées et des certificats des administrateurs centraux de l'AC RACINE DIPLOMATIE associés est strictement limitée au service d'authentification auprès des services de l'AC RACINE DIPLOMATIE.

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 l'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 clés et certificats des administrateurs centraux de l'ACR (RC) sont stockés au sein de cartes d'authentification administrateur, fournies aux administrateurs centraux lors de leur enregistrement.

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 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.
Tout transfert de clés privée d'AC se fait sous forme chiffrée, conformément aux exigences du chapitre 6.2.4. « Copie de secours de la clé privée ».

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

La méthode d'activation des clés privées d'AC, décrite dans la DPC, permet de répondre aux exigences définies pour le niveau de sécurité considéré.
L'activation des clés privées d'AC est contrôlée via des données d'activation (cf. chapitre 6.4. « Données d'activation ») et fait intervenir les différents porteurs de secrets identifiés lors de la cérémonie des clés.

6.2.8.2 CLE PRIVEE DES PORTEURS

Cf. chapitre 6.4.

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 PORTEURS

Les conditions de désactivation de la clé privée d'un serveur répondent 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 PORTEURS

Les clés privées sont stockée sur la carte à puce des administrateurs d'AC, la destruction de la carte implique la destruction des clés privées.

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

Les certificats de l'ACR couverts par la présente PC ont une durée de validité de douze ans.
La durée de validité des certificats des ACD et de leurs composantes est de neuf ans ou six ans.
La durée de validité des certificats des administrateurs centraux de l'AC RACINE DIPLOMATIE est de trois ans.

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.
La génération et l'installation des données d'activation des modules cryptographiques de l'IGC, au sein desquels sont mises en œuvre les clés de signature de l'ACR, 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 PORTEURS ADMINISTRATEUR D'AC

Les administrateurs centraux (RC) sont invités à choisir un code d'activation (PIN) pour leur carte d'authentification administrateur, qu'ils puissent mémoriser, mais non trivial.
La clé privée d'un administrateur central est désactivée dès que la carte d'authentification administrateur est déconnectée.

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

Sans objet.

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 l'AC Racine,
- 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 ACR,
- fonctions d'audits (imputabilité des actions effectuées),
- gestion des incidents,
- protection en confidentialité, en intégrité et en disponibilité des clés nécessaires au fonctionnement des ACR.

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

La configuration des systèmes de la plate-forme d'AC RACINE DIPLOMATIE (systèmes d'exploitation, application IGC…), ainsi que toute modification et mise à niveau, sont documentées et contrôlées.
L'Autorité Qualifiée est tenue informée de toute évolution majeure sur les systèmes de la plate-forme d'AC RACINE DIPLOMATIE.
Celle-ci est documentée et apparaît dans les procédures d'exploitation de l'AC (document non public).

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.
La plate-forme hébergeant l'AC RACINE DIPLOMATIE est déconnectée de tout réseau.

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 DES CERTIFICATS AUTO-SIGNES DE L'AC RACINE DIPLOMATIE

7.1.1.1 NUMÉRO DE VERSION

CHAMP	VALEUR	REMARQUES
Version	V3	
CertificateSerialNumber	*Variable*	Nombre entier unique
SignatureAlgorithmId	Sha256WithRSAEncryption	
Issuer	CN=AC RACINE DIPLOMATIE OU= 0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C=FR	Identique au champ « Subject »
Validity	*Suivant date de signature*	Durée de validité : 12 ans
Subject	CN=AC RACINE DIPLOMATIE OU=0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C=FR	Identique au champ « Issuer »
Public Key Algorithm	rsaEncryption	
SubjectPublicKey	*Valeur de la clé*	Taille de clé : 4096 bits.
signatureValue	*Valeur de la signature*	

7.1.1.2 EXTENSIONS DE CERTIFICAT

CHAMP	VALEUR	CRITICITE	REMARQUES
basicConstraints : CA	Vrai	Critique	Type d'objet : Autorité de certification
certificatePolicies	1.2.250.1.214.69.3.1.1.1.1.1	Non critique	OID de la PC de l'AC RACINE DIPLOMATIE
keyUsage	keyCertSign, CRLSign	Critique	
SubjectKeyIdentifier	*Variable*	Non critique	Hash de la clé

7.1.2 GABARIT DES CERTIFICATS D'ACD EMIS PAR L'ACR ET DE LONGUEUR DE CLE 2048 BITS

7.1.2.1 NUMÉRO DE VERSION

Le profil des certificats des AC Déléguées émis par l'AC RACINE DIPLOMATIE et de longueur de clé 2048 bits est le suivant :

CHAMP	VALEUR	REMARQUES
Version	V3	

CertificateSerialNumber	*Variable*	Nombre entier unique
SignatureAlgorithmId	Sha256WithRSAEncryption	
Issuer	CN=AC RACINE DIPLOMATIE OU= 0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C=FR	
Validity	*Suivant date de signature*	Durée de validité : 9 ans
Subject	CN=<*AC déléguée*> OU= <*OU de l'AC Déléguée*> O= <*O de l'AC Déléguée*> C=<*C de l'AC Déléguée*>	
Public Key Algorithm	rsaEncryption	
SubjectPublicKey	*Valeur de la clé*	Taille de clé : 2048 bits.
signatureValue	*Valeur de la signature*	

7.1.2.2 EXTENSIONS DE CERTIFICAT

CHAMP	VALEUR	CRITICITE	REMARQUES
basicConstraints : CA	Vrai	Critique	Type d'objet : Autorité de certification
crlDistributionPoint	http://crl.diplomatie.gouv.fr/AC_Racine_Diplomatie/crl/crl-<indice de la clé d'AC>.crl	Non critique	Points de distribution de la LCR de l'AC RACINE DIPLOMATIE
certificatePolicies	1.2.250.1.214.69.3.1.1.1.1.1	Non critique	OID de la PC de l'AC RACINE DIPLOMATIE
keyUsage	keyCertSign, CRLSign		
AuthorityKeyIdentifier	Variable	Non critique	Id de la clé de l'Autorité
SubjectKeyIdentifier	Variable	Non critique	Identifiant de la clé

7.1.3 GABARIT DES CERTIFICATS D'ACD EMIS PAR L'ACR ET DE LONGUEUR DE CLE 4096 BITS

7.1.3.1 NUMÉRO DE VERSION

Le profil des certificats des AC Déléguées émis par l'AC RACINE DIPLOMATIE et de longueur de clé 4096 bits est le suivant :

CHAMP	VALEUR	REMARQUES
Version	V3	
CertificateSerialNumber	*Variable*	Nombre entier unique
SignatureAlgorithmId	Sha256WithRSAEncryption	
Issuer	CN=AC RACINE DIPLOMATIE OU= 0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C=FR	
Validity	*Suivant date de signature*	Durée de validité : 9 ans
Subject	CN=<*AC déléguée*> OU= <*OU de l'AC Déléguée*> O= <*O de l'AC Déléguée*> C=<*C de l'AC Déléguée*>	

Public Key Algorithm	rsaEncryption	
SubjectPublicKey	*Valeur de la clé*	Taille de clé : 4096 bits.
signatureValue	*Valeur de la signature*	

7.1.3.2 EXTENSIONS DE CERTIFICAT

CHAMP	VALEUR	CRITICITE	REMARQUES
basicConstraints : CA	Vrai	Critique	Type d'objet : Autorité de certification
crlDistributionPoint	http://crl.diplomatie.gouv.fr/AC_Racine_Diplomatie/crl/crl-<indice de la clé d'AC>.crl	Non critique	Points de distribution de la LCR de l'AC RACINE DIPLOMATIE
certificatePolicies	1.2.250.1.214.69.3.1.1.1.1.1	Non critique	OID de la PC de l'AC RACINE DIPLOMATIE
keyUsage	keyCertSign, CRLSign		
AuthorityKeyIdentifier	Variable	Non critique	Id de la clé de l'Autorité
SubjectKeyIdentifier	Variable	Non critique	Identifiant de la clé

7.1.4 GABARIT DES CERTIFICATS D'AUTHENTIFICATION DES ADMINISTRATEURS CENTRAUX DE L'AC RACINE DIPLOMATIE

7.1.4.1 NUMÉRO DE VERSION

Le profil des certificats d'authentification administrateur de l'AC RACINE DIPLOMATIE est le suivant :

- Attributs obligatoires :

CHAMP	VALEUR	REMARQUES
Version	V3	
CertificateSerialNumber	*Variable*	Nombre entier unique
SignatureAlgorithmId	Sha256WithRSAEncryption	
Issuer	CN=AC RACINE DIPLOMATIE OU= 0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C=FR	
Validity	*Suivant date de signature*	Durée de validité : 3 ans
Subject	UID=<UID> CN= *NOM Prénom* OU= 0002 12000601000025 O=MINISTERE DES AFFAIRES ETRANGERES C=FR	UID = ID arobas de l'utilisateur du SI MAE
Public Key Algorithm	rsaEncryption	
SubjectPublicKey	*Valeur de la clé*	Taille de clé : 2048 bits
signatureValue	*Valeur de la signature*	

7.1.4.2 EXTENSIONS DE CERTIFICAT

CHAMP	VALEUR	CRITICITE	REMARQUES
basicConstraints : CA	Faux	Non critique	Type d'objet : Entité finale
crlDistributionPoint	http://crl.diplomatie.gouv.fr/AC_Racine_Diplomatie/crl/crl-<indice de la clé d'AC>.crl	Non critique	Points de distribution de la LCR de l'AC RACINE DIPLOMATIE
certificatePolicies	1.2.250.1.214.69.3.1.1.1.1.1	Non critique	OID de la PC de l'AC RACINE DIPLOMATIE
keyUsage	digitalSignature	Critique	
extendedKeyUsage	clientAuth	Non critique	
AuthorityKeyIdentifier	*Variable*	Non critique	Id de la clé de l'Autorité
SubjectKeyIdentifier	*Variable*	Non critique	Identifiant de la clé

7.1.5 GABARIT DES CERTIFICATS DES COMPOSANTES DE L'AC RACINE DIPLOMATIE

7.1.5.1 NUMÉRO DE VERSION

CHAMP	VALEUR	REMARQUES
Version	V3	
CertificateSerialNumber	*Variable*	Nombre entier unique
SignatureAlgorithmId	Sha256WithRSAEncryption	
Issuer	CN=AC RACINE DIPLOMATIE OU= 0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C=FR	
Validity	*Suivant date de signature*	Durée de validité : 12 ans (égale à celle du certificat de l'AC)
Subject	CN = « *nom de la composante* » OU = composante, OU = internal OU = MetaPKI, O = BULL, C = FR	
Public Key Algorithm	rsaEncryption	
SubjectPublicKey	*Valeur de la clé*	Taille de clé : 2048 bits.
signatureValue	*Valeur de la signature*	

7.1.5.2 EXTENSIONS DE CERTIFICAT

CHAMP	VALEUR	CRITICITE	REMARQUES
basicConstraints : CA	Faux	Non critique	Type d'objet : Entité finale
keyUsage	digitalSignature, nonRepudiation,	Critique	

	KeyEncipherment, dataEncipherment		
SubjectKeyIdentifier	*Variable*	Non critique	Empreinte de la clé publique
AuthorityKeyIdentifier	*Variable*	Non critique	Identique au champ « *SubjectKeyIdentifier* » du certificat de l'AC

7.2 PROFIL DES LCR / LAR

7.2.1 NUMEROS DE VERSIONS

CHAMP	VALEUR	REMARQUES
version	V2	
signature	Sha256WithRSAEncryption	
issuer	CN=AC RACINE DIPLOMATIE OU= 0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C=FR	
thisUpdate	*Variable*	Date de publication de la présente LCR
nextUpdate	*Variable*	Date au plus tard de la prochaine publication de la LCR Durée de validité : 7 jours
revokedCertificates userCertificate : revocationDate :	 *Variable* *Variable*	Pour chaque certificat révoqué : n° de série du certificat date de révocation du certificat.
SignatureAlgorithmId	sha256WithRSAEncryption	
signatureValue	*Valeur de la signature numérique*	

7.2.2LCR ET EXTENSION DES LCR

CHAMP	VALEUR	CRITICITE	REMARQUES
Authority Key Identifier	*Variable*	Non critique	Identique au champ « Subject Key Identifier » du certificat de l'Autorité
CRLnumber	*Variable*	Non critique	

7.3 PROFIL DES OCSP

Sans objet.

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 de l'ACR 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 de l'ACR, 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 de l'ACR.

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'AC ;
- 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 RACINE DIPLOMATIE est d'émettre des certificats à destination des administrateurs et des autres AC déléguées 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'ACR. 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
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*)
LDAP	*Lightweight Directory Access Protocol*
MAE	Ministère des Affaires Étrangères

Acronyme	Signification
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 4 : 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. Dans le cadre de ce projet, la messagerie électronique est une application utilisatrice de certificats de chiffrement er de signature.
Autorité de	Entité, composante de base de l'IGC, qui délivre des certificats à

Acronyme	Signification
Certification (AC)	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. 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. L'Autorité de Certification racine signe les certificats des Autorités de Certification déléguées.
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 déléguée 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. 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 Name (DN)	Nom distinctif X.500 du porteur de certificat.
Données d'activation (ou code PIN)	Données qui permettent l'activation d'une clé privée cryptographique d'AC ou de porteur.

Acronyme	Signification
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) 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. 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 Organisationnelle)	Champ du gabarit d'un certificat contenant l'identifiant officiel de l'établissement qui a émis le certificat. En France, il s'agit du n° SIREN ou n° SIRET de l'établissement.
PKCS (*Public Key Cryptographic Standards*)	Ensemble de standards de chiffrement relatifs aux clefs publiques. 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.

Acronyme	Signification
	PKCS#7 : Conteneur cryptographique embarquant un certificat et parfois l'ensemble de la chaîne de certification associée. 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. ▪ 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. ▪ 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. Dans le cadre de ce projet, il y a un seul profil « Accès distant » 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. 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 Certification (RA)	Personne physique représentant l'entité fonctionnelle Autorité de Certification. Il définit et contrôle l'application de la Politique de 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	Opération de mise en opposition demandée par le porteur du

Acronyme	Signification
(d'un certificat)	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. 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 5 : Définition des termes utilisés

Fin du document