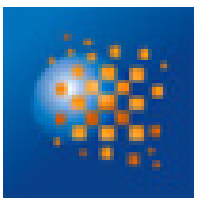
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'EUROPE ET DES
AFFAIRES ÉTRANGÈRES

Politique de Certification des AC UTILISATEURS RENFORCEE Carte MEAE

Gestion de certificats sur cartes à puce



Authentification forte Agent 1.2.250.1.214.69.3.1.6.1.1.2

Signature forte Agent 1.2.250.1.214.69.3.1.6.1.3.2

Confidentialité forte Agent 1.2.250.1.214.69.3.1.6.1.5.2

Authentification forte Externe 1.2.250.1.214.69.3.1.6.1.7.2

Signature forte Externe 1.2.250.1.214.69.3.1.6.1.9.2

Confidentialité forte Externe 1.2.250.1.214.69.3.1.6.1.11.2

Cotation Archive : E.3.1.6.1

Version 2.0.4 du 06/09/2019

État : validé

Suivi des mises à jour			
Version	**Date**	**Auteur**	**Commentaire(s)**
1.0	08/12/2011	Solucom	Version livrée au MAE
1.1	14/12/2011	Solucom	Mise à jour suite aux retours de CAZENAVE Michel
2.0.1	17/07/2015	Solucom	Mise en conformité avec le RGS V2
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 personne » version 3.0
[2]	☑	☐	Politique de Certification de l'AC RACINE DIPLOMATIE

1 INTRODUCTION

1.1 PRESENTATION GENERALE

1.1.1 OBJET DU DOCUMENT

Le Ministère des Affaires Étrangères dispose d'une infrastructure de gestion de clés (IGC DIPLOMATIE), qui assure la fourniture de certificats électroniques destinés à l'ensemble des agents du MAE, à certains prestataires du MAE, ainsi qu'à certaines personnes d'autres Ministères, l'Élysée et Matignon et d'autres entités externes.

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

- l'AC RACINE DIPLOMATIE,
- trois AC Déléguées: AC UTILISATEURS, AC INFRASTRUCTURE, et AC UTILISATEURS RENFORCÉE.

L'AC UTILISATEURS RENFORCÉE émet notamment des certificats sur carte à puce correspondant aux profils :

- Gabarit « Authentification forte d'utilisateurs Agent »
- Gabarit « Signature forte Agent »
- Gabarit « Confidentialité forte Agent»
- Gabarit « Authentification Forte Externe »
- Gabarit « Signature forte Externe »
- Gabarit « Confidentialité forte Externe »

La carte à puce stockant ces certificats est désignée sous le terme de « carte MAE » au sein du MAE.

Ces certificats sont destinés aux agents du MAE, à des prestataires du MAE ou encore à certaines personnes d'autres ministères ou de l'Élysée rattachées au MAE. Ces certificats sont de type matériel.

Le présent document constitue la Politique de Certification (PC) de l'Autorité de Certification – AC UTILISATEURS RENFORCÉE - pour les usages décrits ci-dessus.

Ce document respecte le plan de la Politique de Certification Type « certificats électroniques de personne » du RGS v3.0 [1].

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

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

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

1.1.1 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 UTILISATEURS RENFORCÉE
Carte MAE

Cette Politique de Certification est identifiée par plusieurs OID du fait de l'utilisation de certificats pour plusieurs usages et gammes de certificats. Les OID sont les suivants :

Gamme de certificats	OID
Authentification forte Agent	1.2.250.1.214.69.3.1.6.1.1.2
Signature forte Agent	1.2.250.1.214.69.3.1.6.1.3.2
Confidentialité forte Agent	1.2.250.1.214.69.3.1.6.1.5.2
Authentification forte Externe	1.2.250.1.214.69.3.1.6.1.7.2
Signature forte Externe	1.2.250.1.214.69.3.1.6.1.9.2
Confidentialité forte Externe	1.2.250.1.214.69.3.1.6.1.11.2

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

1.3 DEFINITIONS ET ACRONYMES

Les acronymes suivants sont utilisés dans le cadre de ce document :

IGC : Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de gestionnaire de Certificats, d'une entité d'archivage, d'une entité de publication, etc.

PC : Politique de Certification, document décrivant le niveau d'exigence que s'engage à respecter et maintenir l'AC, lors de l'émission, de la gestion du cycle de vie et de la publication de ses certificats.

DPC : Déclarations des Pratiques de Certification, documents décrivant de façon détaillée comment est mise en œuvre une ou plusieurs politiques de certification.

AA : Autorité Administrative responsable de l'ensemble de l'IGC, définit les PC de l'IGC et valide les DPC.

Composants de l'IGC du MAE :

AC : Autorité de Certification mettant en œuvre une ou plusieurs politiques de certification au sein de l'IGC, l'AC signe les demandes de certificats.

ACR : Autorité de Certification RACINE, AC qui certifie les autres AC, AC de plus haut niveau, dans ce document l'ACR est l'AC RACINE DIPLOMATIE

AC Déléguée (ACD) : Autorité de Certification émettant des certificats à destination de Porteurs.

Opérateurs de Bureau des Badges : Personnes chargées par le directeur d'une des directions du MAE de l'enregistrement et la validation des demandes de carte MAE.

Opérateur de Révocation : personnes chargées par l'AA de la révocation des certificats des Porteurs.

Porteur : Le demandeur de certificat devient le Porteur à partir du moment où il a reçu son certificat.

Production de l'IGC :

LCR : Liste des Certificats Révoqués émise périodiquement par une AC, liste les certificats invalidés.

Autres acronymes et notions :

HFDS : Haut Fonctionnaire Défense et Sécurité, Fonctionnaire chargé des questions de défense auprès du ministre.

AQSSI : Autorité Qualifiée en Sécurité des Systèmes d'Information nommée par arrêté ministériel responsable de la politique de sécurité pour une entité d'un Ministère.

SG : Secrétariat Général du MAE.

PS : Politique de sécurité

SDSI : Sous-Direction des Systèmes d'Information sous l'autorité du Service de la Modernisation.

MSSI : Mission Sécurité des Systèmes d'Information, rattachée au responsable de la SDSI.

CERI : Centre d'Études et de Réalisations Informatiques, centre de production informatique du MAE rattaché au responsable de la SDSI.

X.509 : Format des certificats d'identité recommandé par l'Union Internationale des Télécommunications (UIT).

ISO 9594-8 : norme décrivant, entre autres, le format X509 v3 qui constitue le format normalisé des certificats.

OID (Object Unique Identifier) : identifiant universel organisé sous forme hiérarchique et défini dans une recommandation de l'*International Telecommunication Union*.

ANSSI : Agence Nationale pour la Sécurité des Systèmes d'Information.

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 MAE 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 à des personnes physiques : agents du MAE et externes (prestataires du MAE et agents d'autres Ministère, de l'Élysée ou d'autres entités externes).
        - Les usages des certificats délivrés sont divers : signature personnelle et confidentialité (chiffrement pour l'usage de messagerie sécurisée), et authentification pour l'authentification des administrateurs de l'IGC aux interfaces de l'IGC. 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 à des éléments de l'infrastructure du MAE et éventuellement d'autres entités (composants de l'IGC, supports matériels, serveurs, routeurs, etc.).
        - Les usages des certificats délivrés sont divers : certificats d'authentification client/serveur, certificats SSL, etc.
        - Les supports sont logiciels.
    - AC UTILISATEURS RENFORCÉE
        - Elle délivre des certificats destinés à des personnes physiques : agents du MAE et externes (prestataires du MAE et agents d'autres Ministère ou de l'Élysée).
        - Les usages des certificats délivrés sont divers : signature personnelle forte (signature de documents…), confidentialité forte (chiffrement de la base locale sur le poste du porteur) et authentification forte (à des applications sensibles). Les certificats sont nominatifs.
        - Les supports sont matériels, sur carte à puce appelée « carte MAE ».

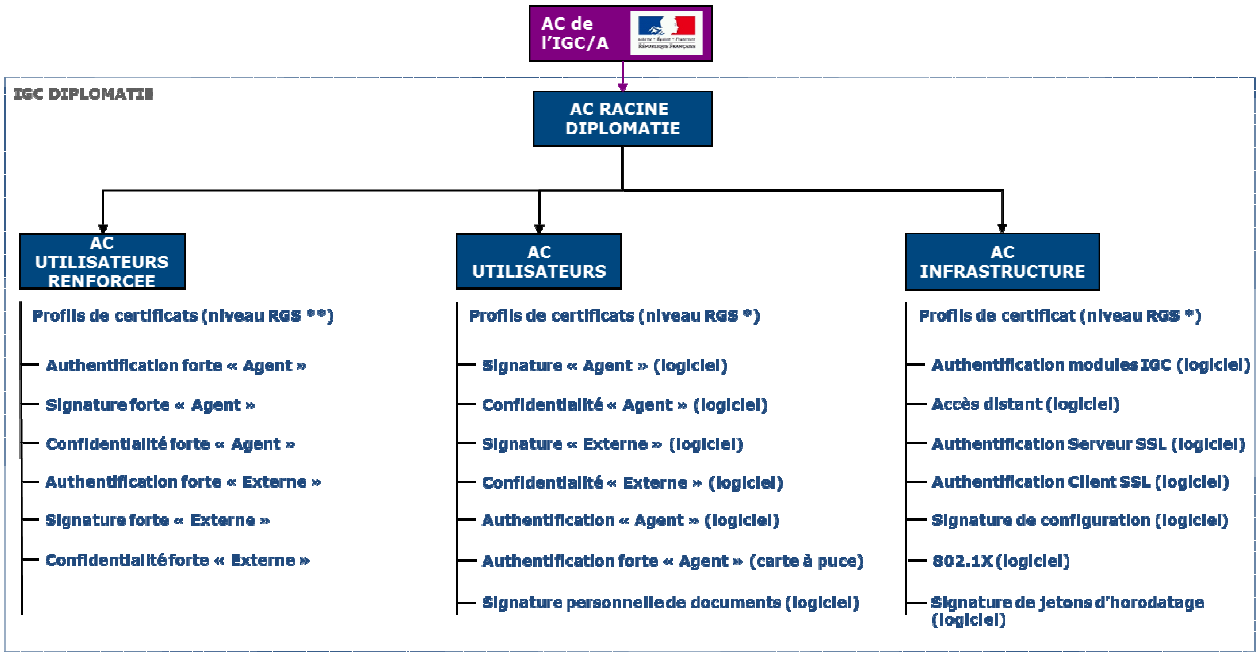


Figure 1 : Hiérarchie de Certification

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

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

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI dans le domaine (cf. ETSI TS 102 042 V1.3.4 (décembre 2007) applicable Policy Requirements for Certification Authorities issuing public key certificates) la décomposition fonctionnelle d'une IGC qui est retenue dans la présente PC est la suivante :

- **Autorité d'enregistrement (AE)** - Cette fonction vérifie et valide les informations d'identification du futur porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. L'AE a également en charge, lorsque cela est nécessaire, la revérification des informations du porteur lors du renouvellement du certificat de celui-ci ;

- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du porteur provenant soit du porteur, soit de la fonction de génération des éléments secrets du porteur, si c'est cette dernière qui génère la bi-clé du porteur ;

Authentification forte Agent 1.2.250.1.214.69.3.1.6.1.1.2
Signature forte Agent 1.2.250.1.214.69.3.1.6.1.3.2
Confidentialité forte Agent 1.2.250.1.214.69.3.1.6.1.5.2
Authentification forte Externe 1.2.250.1.214.69.3.1.6.1.7.2
Signature forte Externe 1.2.250.1.214.69.3.1.6.1.9.2
Confidentialité forte Externe 1.2.250.1.214.69.3.1.6.1.11.2
Cotation Archive : E.3.1.6.1

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

- **Fonction de remise au porteur** - Cette fonction remet au porteur au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif du porteur, clé privée du porteur, 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 porteurs et/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 de ses porteurs ;

- **Fonction de gestion des révocations** - Cette fonction traite les demandes de révocation après identification et authentification des demandeurs puis détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats ;

- **Fonction d'information sur l'état des certificats** - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus...). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR et LAR).

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

- **Porteur** - La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat ;

- **Utilisateur de certificat** - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique ou une valeur d'authentification provenant du porteur du certificat ou chiffrer des données à destination du porteur du certificat ;

- **Personne autorisée-** Il s'agit d'une personne autre que le porteur et le mandataire de certification 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 porteur (demande de révocation, de renouvellement, …). Il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.

1.4.2 AUTORITE D'ENREGISTREMENT

L'Autorité d'Enregistrement assure les tâches suivantes :

- Authentification des demandeurs de certificats sur carte MAE ;
- Prise en compte et vérification des informations figurant dans les demandes de délivrance de certificats qui lui parviennent ;
- Établissement et transmission technique des demandes de certificat ou des demandes de révocation vers l'Autorité de Certification ;
- Remise de la carte MAE aux Porteurs ;
- Recouvrement des clés de chiffrement sur support matériel ;
- Archivage des demandes.

L'AE réalise ses tâches à l'aide d'un système de gestion de carte mis à sa disposition.

Le rôle d'AE est assuré par les personnes suivantes :

- Opérateurs du bureau des badges central (Administration centrale sur les sites Paris et Nantes) ;
- Opérateurs du bureau des badges décentralisé (Correspondants régionaux CRASIC, Correspondants CSI).

1.4.3 PORTEURS DE CERTIFICATS

Les Porteurs sont des personnes physiques, agents du MAE, prestataires du MAE ou agents d'autres Ministère ou de l'Élysée rattachés au MAE. Les Porteurs doivent respecter les conditions définies dans cette Politique de Certification.

Dans la suite, Les Porteur sont divisés en deux catégories, n'utilisant pas les mêmes gabarits de certificats : les Agents, désignant les personnes du MAE, et les Externes, désignant les prestataires du MAE et les employés des autres ministères ou de l'Élysée rattachés au MAE.

Un Porteur pourra notamment effectuer les actions suivantes :

- Retirer sa carte MAE auprès de l'Opérateur du bureau des badges auquel il est rattaché, via le système de gestion de carte ;
- Renouveler sa carte MAE auprès de l'Opérateur du bureau des badges auquel il est rattaché, via le système de gestion de carte ;
- Demander la révocation de sa carte MAE auprès de l'Opérateur du bureau des badges auquel il est rattaché ;

- Changer le code PIN de la carte MAE protégeant son bi-clé et son certificat à réception de sa carte.

1.4.4 UTILISATEURS DE CERTIFICATS

Sont appelés tiers utilisateurs, les personnes physiques qui utilisent les certificats émis par le MAE.

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

1.4.5 AUTRES PARTICIPANTS

1.4.5.1 COMPOSANTE DE L'IGC

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

1.4.5.2 MANDATAIRE DE CERTIFICATION

Les Mandataires de Certification sont les personnes habilitées à demander à l'Autorité d'Enregistrement des certificats, leur renouvellement et leur éventuelle révocation pour le bénéfice de Porteurs appartenant à leur périmètre de responsabilité. Ce sont les Opérateurs de bureau des badges, les responsables hiérarchiques des porteurs ou bien un représentant de l'AC.

Bien qu'ils jouent un rôle particulier dans le processus de gestion des certificats, les Mandataires de Certification n'ont pas accès aux clés privées des Porteurs. Ainsi, les Mandataires de Certification ne sont pas en mesure de les utiliser.

Les Mandataires de Certification s'engagent à :

- effectuer correctement et de manière approfondie les contrôles d'identité des futurs Porteurs sous leur responsabilité ;
- respecter les parties de la PC qui leur incombent.

1.5 USAGE DES CERTIFICATS

1.5.1 DOMAINES D'UTILISATION APPLICABLES

1.5.1.1 BI-CLES ET CERTIFICATS DES PORTEURS

Les certificats de la carte MAE permettent à leurs Porteurs de signer électroniquement, de s'authentifier et de garantir la confidentialité de leurs données.

Les Porteurs ne peuvent utiliser leurs certificats et les données cryptographiques associées que dans les cadres suivants :

- pour apposer une signature électronique sur des documents, dans le cadre de leur activité professionnelle en relation avec leurs collaborateurs et des personnes d'autres Ministères, l'Élysée, Matignon ;
- pour s'authentifier fortement à des applications sensibles du SI du MAE ou externes ;
- pour chiffrer des données, notamment les bases locales de leur poste de travail MAE.

1.5.1.2 Bi-cles et certificats d'AC et de ses composantes

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

- signature des certificats des Porteurs émis par l'Autorité de Certification – AC UTILISATEURS RENFORCÉE N ;
- signature de la Liste des Certificats Révoqués (LCR) émise par l'Autorité de Certification – AC UTILISATEURS RENFORCÉE N.

1.5.2 Domaines d'utilisation interdits

Le RSI du MAE décline toute responsabilité dans l'usage fait d'un certificat dans le cadre d'un domaine non mentionnée dans les paragraphes précédents.

1.6 Gestion de la PC

1.6.1 Entite gerant la PC

La PC de l'Autorité de Certification AC UTILISATEURS RENFORCÉE N – Carte MAE est élaborée et mise à jour par le Responsable de la Sécurité de l'Information du MAE.

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 de l'Europe et des Affaires Étrangères
Direction des Systèmes d'Information
AC UTILISATEURS RENFORCÉE
37 quai d'Orsay
75700 PARIS 07 SP

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

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 SSI	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 MAE 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 MAE 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 UTILISATEURS RENFORCÉE N met en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats.

2.2 INFORMATIONS DEVANT ETRE PUBLIEES

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

- la Politique de Certification de l'AC UTILISATEURS RENFORCÉE N 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 des ACD, et des LCR émises par l'AC UTILISATEURS RENFORCÉE N ;
- les certificats auto-signés de l'ACR, en cours de validité et les informations permettant aux tiers utilisateurs de certificats de s'assurer de l'origine de ces certificats (empreintes) ;
- la LCR en cours de validité, conforme au profil indiqué en partie 7 et accessible par le protocole http ;
- l'adresse (URL) permettant d'obtenir des informations concernant l'AC RACINE DIPLOMATIE à laquelle sont rattachées les ACD ;
- le certificat de l'AC RACINE DIPLOMATIE ;
- le certificat de l'AC UTILISATEURS RENFORCÉE N.

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

Tableau 2 : Liste des informations publiées

2.3 DELAIS ET FREQUENCES DE PUBLICATION

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

La fréquence de mise à jour des LCR est au minimum de 24 heures.

Les systèmes publiant ces informations sont disponibles les jours ouvrés.

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 a une disponibilité de 24h/24 et 7j/7.

Certificats des ACD	
Délais de publication :	Ceux-ci sont diffusés préalablement à toute diffusion de certificats de Porteurs et/ou de LCR correspondants sous un délai de 24 heures.
Disponibilité de l'information :	L'infrastructure assurant cette fonction a une disponibilité de 24h/24 et 7j/7.

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 : 24 heures
Disponibilité de l'information :	L'infrastructure assurant cette fonction a une disponibilité de 24h/24 et 7j/7. La durée maximale d'indisponibilité par interruption de service (panne ou maintenance) est de 4 heures (jours ouvrés) et la durée totale maximale d'indisponibilité par mois est de 16 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 Porteurs 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, à l'adresse suivante : **http://crl.diplomatie.gouv.fr**.

L'accès en modification au système de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) interne à l'IGC 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 autres systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) internes ou externes est strictement limité aux personnes habilitées avec une authentification de type login/mot de passe sur ces systèmes.

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

Cette partie traite des données du certificat identifiant son Porteur.

3.1.1 TYPES DE NOMS

Les données d'identification des Porteurs figurent dans le champ « Objet » (« *Subject* » en anglais) du certificat (respectant la norme X.509 de l'ITU), sous la rubrique DN (« *Distinguished Name* ») au format *printableString* défini par la norme X.501 de l'ITU.

3.1.2 NECESSITE D'UTILISATION DE NOMS EXPLICITES

Les noms choisis doivent être explicites.

L'identification des Porteurs se fait en utilisant le DN dont la composition est décrite dans les tableaux ci-dessous :

Pour la population de Porteurs constituée des Agents :

Attribut	Valeur
Nom du Porteur (Attribut « CN »)	<Prenom NOM>
Adresse de courriel (Attribut « E »)	<prenom.nom@diplomatie.gouv.fr>
Identifiant unique (Attribut « 0.9.2342.19200300.100.1.1 »)	<logon Windows>
Code Agent (Attribut « SERIALNUMBER »)	<Identifiant AROBAS>
Nom de l'Unité Organisationnelle (Attribut « OU »)	0002 12000601000025

Attribut	Valeur
Nom de l'Organisation (Attribut « O »)	MINISTERE DES AFFAIRES ETRANGERES
Pays (Attribut « C »)	FR

Tableau 3 : Composition des champs du DN pour les agents

Pour la population de Porteurs constituée des Externes :

Attribut	Valeur
Nom du Porteur (Attribut « CN »)	<Prenom NOM>
Code Agent (Attribut « SERIALNUMBER »)	<identifiant AROBAS>
Nom de l'Unité Organisationnelle (Attribut « OU »)	0002 12000601000025
Nom de l'Organisation (Attribut « O »)	MINISTERE DES AFFAIRES ETRANGERES
Pays (Attribut « C »)	FR

Tableau 4 : Composition des champs du DN pour les externes

3.1.3 ANONYMISATION OU PSEUDONYMISATION DES PORTEURS

Sans objet.

3.1.4 REGLES D'INTERPRETATION DES DIFFERENTES FORMES DE NOM

Le contenu du DN du certificat s'appuie sur le référentiel AROBAS, source de données fiables.

3.1.5 UNICITE DES NOMS

Le champ DN est unique au sein des profils contenus dans la carte MAE. La méthode mise en place pour assurer cette unicité est décrite dans la DPC.

3.1.6 IDENTIFICATION, AUTHENTIFICATION ET ROLE DE MARQUES DEPOSEES

Sans objet.

3.2 VALIDATION INITIALE DE L'IDENTITE

3.2.1 METHODES POUR PROUVER LA POSSESSION DE LA CLE PRIVEE

Sans objet

3.2.2 VALIDATION DE L'IDENTITE D'UN ORGANISME

Sans objet.

3.2.3 VALIDATION DE L'IDENTITE D'UN INDIVIDU

Sont considérés comme individus les Porteurs ou futurs Porteurs ou Mandataires de Certification.

La validation initiale de l'identité d'un individu et de son entité de rattachement fonde la confiance portée aux certificats émis par le MAE. La validation de l'identité d'un individu est réalisée par l'AE, en particulier par un Opérateur du bureau des badges lors du face-à-face avec l'individu. Elle repose sur un document officiel d'identité en cours de validité du futur porteur comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) et est corroborée à l'aide des informations personnelles fournies par la source de données fiable (référentiel AROBAS).

3.2.4INFORMATIONS NON VERIFIEES DU PORTEUR

Aucune exigence particulière n'est formulée dans la présente PC.

3.2.5 VALIDATION DE L'AUTORITE DU DEMANDEUR

La demande est réalisée par le Mandataire de Certification, il doit avoir signé au préalable un engagement lors d'un face-à-face avec un opérateur de bureau des badges :

- le désignant comme Mandataire de Certification,

- indiquant qu'il s'engage à effectuer correctement et de façon indépendante les contrôles des dossiers des Porteurs,
- indiquant qu'il s'engage à signaler à l'Autorité d'Enregistrement son départ de l'entité.

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

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

3.3.1 IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT COURANT

Le processus d'identification pour un renouvellement courant est le même que le processus d'identification pour une délivrance initiale.

3.3.2 IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT APRES REVOCATION

Le processus d'identification pour un renouvellement après révocation est le même que le processus d'identification pour une délivrance initiale. Pour valider un tel renouvellement, l'Opérateur du bureau des badges doit s'assurer au préalable, de la révocation effective des certificats précédents du Porteur.

3.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

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

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

Moyen	Demandeur autorisé	Authentification du demandeur	Opérateur de révocation
En face à face avec l'Opérateur du bureau des badges	Porteur Mandataire de Certification l'Autorité d'Enregistrement Représentant légal de l'AA	Pièce d'identité et vérification du droit à demander la révocation (ex : MC du Porteur concerné)	Opérateur du bureau des badges
Courriel signé adressé à l'Opérateur du bureau des badges	Porteur Mandataire de Certification l'Autorité d'Enregistrement Représentant légal de l'AA	Vérification du droit à demander la révocation (ex : MC du Porteur concerné)	Opérateur du bureau des badges

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES

4.1 DEMANDE DE CERTIFICAT

4.1.1 ORIGINE D'UNE DEMANDE DE CERTIFICAT

Une demande de certificat ne peut être adressée à l'Autorité d'Enregistrement que via l'Opérateur du bureau des badges.
Une demande de certificat ne peut être adressée à un Opérateur du bureau des badges que par un Mandataire de Certification du futur Porteur.

Le Mandataire qui est à l'origine de la demande de certificat pour un Porteur devra avoir réalisé au préalable un face-à-face avec un opérateur de bureau des badges, par exemple notamment à l'occasion de sa remise préalable d'une carte MAE.

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

Le Mandataire de Certification établit une demande de carte-MAE pour un Porteur auprès de l'Opérateur du bureau des badges. La demande de carte-MAE implique systématiquement la demande de certificats.

Le Mandataire de Certification doit s'assurer au préalable de l'éligibilité du porteur, le cas échéant, il communique les informations nécessaires à l'enregistrement de la demande :

- le nom et prénom du Porteur ;
- l'identifiant unique (identifiant AROBAS) ;
- l'adresse électronique du Porteur (si nécessaire).

La demande peut être formalisée par un mail du Mandataire de Certification envoyé à l'AE.

Le Mandataire de Certification a la responsabilité du droit à disposer d'une carte MAE pour un Porteur. Par conséquence, le Mandataire de Certification doit conduire les actions nécessaires (ex : demande de révocation) si le besoin de carte MAE pour le Porteur n'est plus avéré (changement de poste par exemple).

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

Ce processus est conduit par l'Opérateur du bureau des badges, il procède aux vérifications suivantes :

- Identité du Mandataire de Certification et habilitation à effectuer une demande pour le Porteur ;

- Complétude des informations fournies par le Mandataire de Certification (cf. section 3.2.5) ;
- Identification du Porteur et comparaison avec les données fournies dans AROBAS.

Une fois ces éléments validés, l'Opérateur bu bureau des badges invite le Porteur à se présenter au bureau des badges pour finaliser la validation de la demande et lui remettre sa carte en main propre.

Le Porteur doit présenter à l'AE lors du face-à-face :

- Une pièce désignant l'individu comme futur Porteur auquel le certificat doit être délivré ;
- Une preuve du rattachement du Porteur à son entité d'appartenance ;
- L'adresse mail professionnelle du Porteur.

L'Opérateur du bureau des badges procède alors aux vérifications suivantes :

- Complétude des informations fournies par le Porteur requises pour la demande (cf. liste ci-dessus) ;
- Signature par le Porteur des Conditions Générales d'Utilisation.

4.2.2 ACCEPTATION OU REJET DE LA DEMANDE

Pour qu'une demande soit acceptée, il faut que les processus d'identification et de validation de la demande décrit ci-dessus soient satisfaits.

Si les informations personnelles du Porteur sont erronées ou incomplètes (ex : confusion avec un homonyme), le Mandataire de Certification doit reformuler sa demande avec des informations correctes.

Si le Mandataire de Certification n'est pas habilité à demander une carte à puce MAE pour le Porteur mentionné, l'Opérateur du bureau des badges notifie le demandeur de la fermeture de la demande.

Si la demande est acceptée, l'Opérateur du bureau des badges émet les certificats et remet la carte MAE au Porteur présent lors de cette opération.

4.2.3 DUREE D'ETABLISSEMENT D'UN CERTIFICAT

La durée de la demande est conditionnée par la durée de deux opérations :

- Le traitement du courriel du Mandataire de Certification par l'Opérateur du bureau des badges ;
- Le délai entre l'acceptation de la demande et le rendez-vous effectif en face à face entre l'Opérateur du bureau des badges et le Porteur.

Lors du rendez-vous en face à face, l'émission des certificats et de la carte MAE ne dure que quelques minutes.

La durée totale entre l'envoi de la demande et la remise des certificats ne devrait pas excéder quelques jours.

4.3 DELIVRANCE DU CERTIFICAT

Les certificats sont intégrés dans la carte MAE remise au Porteur.

4.3.1 ACTIONS DE L'AC CONCERNANT LA DELIVRANCE DU CERTIFICAT

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

- authentification de l'Opérateur du bureau des badges (à l'interface de l'Autorité d'Enregistrement) ;
- vérification de l'intégrité de la demande ;
- vérification technique de la demande ;
- création de la bi-clé du futur Porteur sur la carte MAE ;
- création de la requête de certificat (format CSR) ;
- signature de la CSR à l'aide de la clé privée de l'AC et émission du certificat ;
- envoi du certificat à la carte MAE.

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

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

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

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

4.4 ACCEPTATION DU CERTIFICAT

4.4.1 DEMARCHE D'ACCEPTATION DU CERTIFICAT

À l'issu de la délivrance de la carte MAE au Porteur, celui-ci doit s'engager à respecter les conditions générales d'utilisation de ses clés privées et des certificats correspondants.

L'acceptation est tacite à compter de la date d'émission du certificat. Le Porteur dispose de 5 jours ouvrés pour déclarer toute anomalie.

L'acceptation d'un certificat vaut acceptation de la PC de l'Autorité de Certification AC UTILISATEURS RENFORCÉE N – carte MAE.

4.4.2 PUBLICATION DU CERTIFICAT

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

Les certificats d'authentification et de signature du Porteur ne sont pas publiés.

Le certificat de chiffrement du Porteur pourra être publié à l'avenir dans annuaire afin de répondre à de nouveaux usages.

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

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

4.5 USAGE DE LA BI-CLE ET DU CERTIFICAT

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

Les tiers utilisateurs de certificats ne doivent les utiliser que dans les domaines d'utilisation spécifiés à la partie 1.4.1 de la présente PC. Les tiers utilisateurs s'engagent à respecter strictement ces domaines d'utilisation. Dans le cas contraire, leur responsabilité pourrait être engagée.

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

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

Les utilisateurs de certificats ne doivent utiliser le certificat et la clé publique associée que dans les domaines d'utilisation spécifiés à la partie 1.4.1. Les utilisateurs s'engagent à respecter strictement ces domaines d'utilisation. Dans le cas contraire, leur responsabilité pourrait être engagée.

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

4.6 RENOUVELLEMENT D'UN CERTIFICAT

Les certificats et les bi-clés correspondants ont la même durée de vie. Il ne peut donc pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé cryptographique. Le renouvellement du certificat correspond donc à la délivrance d'un nouveau certificat.

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

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 résulter d'une nouvelle demande suite à une révocation ou suite à un oubli de renouvellement.

4.7.2 ORIGINE D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

Cas d'un renouvellement :

La demande de renouvellement est tacite si le certificat à renouveler existe et est toujours valide. Dans ce cas, elle ne nécessite pas de validation de la part du Mandataire de Certification.

Cas d'une nouvelle demande :

La demande de certificat s'effectue à l'identique d'une demande initiale de certificat.

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

Cas d'un renouvellement :

Le Porteur est notifié trois fois par courriel de l'expiration prochaine de son certificat (90, 30 et 15 jours avant expiration) pour lui demander de prendre rendez-vous avec l'Opérateur du bureau des badges. Le renouvellement s'effectue à l'identique de la demande initiale de certificat.

Cas d'une nouvelle demande :

Le traitement d'une nouvelle demande s'effectue à l'identique d'une demande initiale de certificat.

4.7.4 NOTIFICATION AU PORTEUR DE L'ETABLISSEMENT D'UN NOUVEAU CERTIFICAT

La notification au Porteur de l'établissement du nouveau certificat est identique à la notification reçue lors de la délivrance initiale.

4.7.5 DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT

La démarche d'acceptation du nouveau certificat est identique à la démarche à la délivrance initiale.

4.7.6 PUBLICATION DU NOUVEAU CERTIFICAT

La publication du nouveau certificat se fera de la même façon qu'à la délivrance initiale.

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

La notification se fera de la même façon qu'à la délivrance initiale.

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

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

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

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

- les informations du Porteur figurant dans son certificat ne sont pas ou plus exactes, ceci avant l'expiration normale du certificat ;
- le Porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le Porteur n'a pas respecté les obligations découlant de la PC de l'AC, dont le certificat dépend ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du Porteur ;
- la clé privée associée au certificat du Porteur est suspectée de compromission, est compromise, est perdue ou volée ;
- le Porteur ou une entité autorisée (Mandataire de Certification par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du Porteur et/ou de son support) ;
- éventuellement la mutation du Porteur (selon le lieu de mutation) ;
- le départ, le changement de fonction du Porteur ;
- le décès du Porteur ;
- la cessation d'activité de l'entité du Porteur.

4.9.2 ORIGINE D'UNE DEMANDE DE REVOCATION

Les personnes / entités habilitées à demander une révocation de certificat sont :

- le Porteur du certificat ;
- le Mandataire de Certification ;
- un opérateur de l'Autorité d'Enregistrement (Opérateur du bureau des badges)
- tout représentant de l'AC.

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

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

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

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

4.9.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE REVOCATION

Le Porteur, le Mandataire de Certification, l'Autorité d'Enregistrement ou un représentant légal de l'AA peuvent demander la révocation de la carte MAE (et donc des certificats inscrits dedans) :

- Par courriel signé auprès d'un Opérateur du bureau des badges.
- Lors d'un face-à-face avec un Opérateur du bureau des badges.

La révocation de la carte MAE implique systématiquement la révocation de tous les certificats qui y sont stockés.

4.9.4 DELAI ACCORDE AU PORTEUR POUR FORMULER LA DEMANDE DE REVOCATION

Dès qu'une personne ou entité autorisée a connaissance d'une des causes possibles de révocation, de son ressort, elle doit formuler sa demande de révocation sans délais.

4.9.5 DELAI DE TRAITEMENT PAR L'AC D'UN DEMANDE DE REVOCATION

L'AE traite les demandes qui lui parviennent au plus tard 24 heures après réception.
Une fois la demande de révocation envoyées par l'AE à l'AC, la Liste des Certificats Révoquées est mise à jour et générée.

4.9.5.1 REVOCATION D'UN CERTIFICAT DE PORTEUR

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. Cette fonction a une durée maximale totale d'indisponibilité par mois de 8h.

L'AE traite les demandes qui lui parviennent au plus tard 24 heures après réception.
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 LES UTILISATEURS DE CERTIFICATS

Le MAE met à disposition des utilisateurs de certificats des Listes de Certificats Révoqués (LCR).
Il est de la responsabilité de l'utilisateur de certificat de vérifier, avant utilisation, le statut des certificats de l'ensemble de la chaîne de certification correspondante.

4.9.7 FREQUENCE D'ETABLISSEMENT DES LCR

Les Listes des Certificats Révoqués sont générées au minimum toutes les 24 heures.

4.9.8 DELAI MAXIMUM DE PUBLICATION D'UNE LCR

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

4.9.9DISPONIBILITE D'UN SYSTEME DE VERIFICATION EN LIGNE DE LA REVOCATION ET DE L'ETAT DES CERTIFICATS

Sans objet.

4.9.10 EXIGENCES DE VERIFICATION EN LIGNE DE LA REVOCATION DES CERTIFICATS PAR LES UTILISATEURS DE CERTIFICATS

Cf. partie 4.9.9.

4.9.11 AUTRES MOYENS DISPONIBLES D'INFORMATION SUR LES REVOCATIONS

Sans objet.

4.9.12 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.

4.9.13 CAUSES POSSIBLES D'UNE SUSPENSION

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

4.9.14 ORIGINE D'UNE DEMANDE DE SUSPENSION

Sans objet.

4.9.15 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE SUSPENSION

Sans objet.

4.9.16 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 utilisateurs 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 utilisateurs 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	16h

Tableau 5 : 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 PORTEUR ET L'AC

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

4.12 SEQUESTRE DE CLE ET RECOUVREMENT

Ce paragraphe concerne uniquement les clés de chiffrement.

Les clés privées d'AC ne sont en aucun cas séquestrées. Tout comme les autres clés associées aux certificats de signature ou d'authentification.

Concernant les clés privées des certificats de chiffrement des Porteurs, un mécanisme permettant de déchiffrer des informations, préalablement chiffrées, en l'absence de la clé privée d'origine du Porteur concerné (absence du Porteur, perte de sa clé privée par le Porteur, panne de son dispositif de protection de clés privées, …) est mis en place.

Afin de pouvoir déchiffrer un document chiffré par une clé alors absente, il est nécessaire de séquestrer les clés privées des Porteurs, et de les recouvrer, au cas par cas, lorsque nécessaire. Dans le cas présent, le séquestre est réalisé dans une base dédiée de la PKI.

La présente PC ne traite que du recouvrement de données chiffrées suite au séquestre des clés privées de chiffrement des Porteurs.

4.12.1 POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR SEQUESTRE DES CLES

Les différentes étapes de séquestre et de recouvrement de clés privées de Porteurs respectent les exigences des parties suivantes.

4.12.1.1 DEMANDE DE SEQUESTRE

La demande de séquestre de clé privée est inhérente à la demande du certificat correspondant (cf. partie 4.1). Le processus d'identification et de validation d'une telle demande correspond à celui d'une demande de certificat (cf. partie 4.2.1).

La durée de séquestre des clés de chiffrement vaut au minimum la durée de vie de l'AC.

4.12.1.2 TRAITEMENT D'UNE DEMANDE DE SEQUESTRE

L'AE transmet la demande de séquestre à la fonction adéquate de l'IGC.

Les demandes de séquestre sont archivées par l'AE au même titre que les dossiers d'enregistrement correspondants.

La fonction de génération des éléments secrets du Porteur, suite à la génération de la clé privée à séquestrer, transmet le bi-clé du Porteur à la fonction de séquestre et recouvrement suivant un processus qui en assure, de bout en bout, la confidentialité, l'intégrité et l'authentification d'origine.

La conservation de ces clés se fait sous forme chiffrée au sein d'une autorité de séquestre.

Les informations permettant d'identifier de manière unique et non ambiguë chaque clé privée séquestrée sont par exemple :

- L'identification du Porteur (DN).
- Le n° de série du certificat correspondant (SN).
- Un n° de série propre à la clé privée.

Un Porteur pouvant disposer de plusieurs clés privées de chiffrement, à un instant donné ainsi que suite aux renouvellements successifs de ses bi-clés, une identification reposant uniquement sur l'identification du Porteur (DN) n'est pas suffisante.

Au moment du séquestre effectif de la clé privée concernée (au plus tard), l'AC transmet à toute personne autorisée à demander ultérieurement le recouvrement de cette clé (cf. partie suivante), les informations d'identification de la clé privée séquestrée et qui devront être mentionnées dans toute demande de recouvrement.

4.12.1.3 ORIGINE D'UNE DEMANDE DE RECOUVREMENT

Outre les entités autorisées par la loi à accéder aux clés privées séquestrées par une AC, seules les personnes suivantes peuvent demander le recouvrement d'une clé privée d'un Porteur donné :

- Un représentant légal de l'entité ou toute personne explicitement désignée par un représentant légal de l'entité, cette personne pouvant être désignée nominativement ou par sa fonction.

4.12.1.4 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RECOUVREMENT

La demande de recouvrement est effectuée auprès d'un Opérateur du bureau des badges, rôle de confiance de l'IGC.

L'identité du demandeur d'un recouvrement d'une clé séquestrée doit être validée par l'Opérateur du bureau des badges suivant les mêmes exigences que la validation initiale de l'identité d'un demandeur d'un certificat définies à la partie 3.2.

La demande de recouvrement doit comporter au minimum les informations suivantes :

- le motif du recouvrement de la clé privée ;
- les informations permettant d'identifier la clé privée à recouvrer (cf. partie 4.12.1.2).

Une fois l'identité du demandeur validée et la clé à recouvrer identifiée, l'Opérateur du bureau des badges s'assure que le demandeur est bien l'une des personnes autorisées à demander le recouvrement de la clé concernée (cf. partie 4.12.1.3).

4.12.1.5 TRAITEMENT D'UNE DEMANDE DE RECOUVREMENT

L'opération de recouvrement doit nécessiter l'authentification d'au moins deux personnes dans des rôles de confiance (par exemple : l'Opérateur du bureau des badges et un responsable sécurité).

Suite à identification et validation de la demande de recouvrement (cf. partie précédente), l'Opérateur du bureau des badges accompagné d'une tierce personne de confiance, émet la demande pour effectuer le recouvrement de la clé privée concernée auprès de la fonction de gestion des recouvrements vers la fonction de séquestre et recouvrement de l'IGC, en protégeant cette demande en intégrité et en confidentialité.

La fonction de séquestre et recouvrement authentifie la demande de recouvrement faite par la fonction de gestion des recouvrements.

L'opération de recouvrement garantie qu'aucune autre information, que la clé privée sur laquelle porte le recouvrement, n'est divulguée.

La fonction de séquestre et recouvrement remet ensuite de manière sécurisée la clé privée recouvrée au demandeur du recouvrement. Cette remise s'effectue avec une sécurité équivalente à la remise de la clé privée lors de la génération du certificat du porteur (cf. chapitres VI.1.2 et VI.4). Aussi, la clé est remise sur un support physique.

La fonction de gestion des recouvrements a la responsabilité de l'archivage des pièces du dossier de demande de recouvrement, l'archivage des informations liées à l'opération de recouvrement étant du ressort de la fonction de séquestre et recouvrement au titre de l'archivage des journaux d'évènements correspondants (cf. parties 5.4 et 5.5).

4.12.1.6 DESTRUCTION DES CLES SEQUESTREES

Dès la fin de la période de conservation d'une clé séquestrée, tout exemplaire de cette clé détenue par l'AC est détruite de manière fiable afin de ne pouvoir ni recouvrer ni reconstituer la clé.

La DPC décrit les moyens de destruction des clés mis en œuvre par l'AC.

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

Sans objet.

5 MESURES DE SECURITE NON TECHNIQUES

5.1 MESURES DE SECURITE PHYSIQUE

5.1.1 SITUATION GEOGRAPHIQUE ET CONSTRUCTION DES SITES

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

5.1.2ACCES PHYSIQUE

Les zones hébergeant les systèmes informatiques de l'ACD sont physiquement protégées. L'accès doit être strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.
Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant un tel accès.

5.1.3ALIMENTATION ELECTRIQUE ET CLIMATISATION

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

5.1.4 VULNERABILITE AUX DEGATS DES EAUX

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

5.1.5 PREVENTION ET PROTECTION INCENDIE

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

5.1.6 CONSERVATION DES SUPPORTS

Les sauvegardes des données et de l'application opérant l'ACD sont conservées dans une enceinte sécurisée, accessible aux seules personnes habilitées, autorisées et désignées à ces fins.
Les supports papier de l'ACD sont également être conservés avec des mesures de sécurité compatibles avec leur niveau de sensibilité.
La DPC identifie les différentes informations et données intervenant dans les activités de l'ACD, ainsi que les mesures de sécurité qui leur sont appliquées, afin d'en garantir la confidentialité, l'intégrité et la disponibilité.

5.1.7 MISE HORS SERVICE DES SUPPORTS

Les supports papier et électroniques de l'ACD en fin de vie sont systématiquement détruits par des moyens appropriés, permettant d'éviter toute perte de confidentialité.
Les matériels et supports informatiques de l'ACD ne sont pas utilisés à d'autres fins avant destruction complète des informations liées à l'ACD qu'ils sont susceptibles de contenir.

5.1.8 SAUVEGARDE HORS SITE

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

5.2 MESURES DE SECURITE PROCEDURALES

5.2.1 ROLES DE CONFIANCE

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

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

5.2.1.1 ROLES DE CONFIANCE MUTUALISES

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

- **Administrateur sécurité** - Personne chargée d'assurer la gestion de la sécurité au niveau des systèmes, ainsi que de l'habilitation des administrateurs centraux et locaux.
- **Responsable de salle** - Personne chargée de la gestion des accès physiques aux salles informatiques hébergeant l'infrastructure et aux équipements.
- **Exploitant -** Personne chargée d'assurer l'exploitation, la surveillance et la maintenance des systèmes et des réseaux. Cette personne est également chargée d'assurer l'administration des systèmes, la mise

en route et la configuration des équipements composant l'infrastructure. Elle réalise notamment le contrôle des fichiers d'audit du système, ainsi que de l'analyse courante des journaux d'évènements système afin de détecter tout incident, anomalie, tentative de compromission, etc.
- **Fonctionnaire de Sécurité des Systèmes d'Informations (FSSI) -** Personne chargée de la Politique de Sécurité du SI du Ministère.
- **Responsable de production -** Personne chargée du maintien en conditions opérationnelles du système d'information du Ministère.

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

5.2.2 NOMBRE DE PERSONNES REQUISES PAR TACHES

Les rôles liés à la gestion des systèmes sont distincts des rôles de gestion de l'application IGC, ainsi que des rôles intervenants sur les données enregistrées au niveau de l'application. Ces différents rôles doivent être assurés par des personnes distinctes.
Par ailleurs, toute opération impliquant les secrets principaux de l'ACD nécessite l'intervention de trois personnes. La DPC précise les opérations nécessitant l'intervention de plusieurs personnes ainsi que les contraintes que ces personnes doivent respecter.

5.2.3 IDENTIFICATION ET AUTHENTIFICATION POUR CHAQUE ROLE

Tout accès à l'application IGC est soumis à authentification (éventuellement forte), les droits d'accès étant définis en fonction des rôles. Notamment, toute personne susceptible d'intervenir auprès de l'application IGC, et ainsi de modifier des données ou des informations de configuration, doit être préalablement enregistrée dans l'application IGC et disposer d'un certificat d'authentification.
Pour les autres rôles en relation avec l'IGC, l'AC fait vérifier l'identité et les autorisations du personnel concerné avant :
- que son nom soit ajouté aux listes de contrôle d'accès aux locaux hébergeant la plate-forme de l'IGC ;
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans ces systèmes.

Ces contrôles sont décrits dans la DPC associée à cette PC.
Chaque attribution de rôle dans l'IGC est notifiée par écrit.

5.2.4 ROLES EXIGEANT UNE SEPARATION DES ATTRIBUTIONS

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre, et dans le respect des règles de non-cumul définis dans la partie 5.2.2.
Les attributions associées à chaque rôle doivent être décrites dans la DPC de l'AC.
Les règles de non-cumul des rôles de confiance sont décrites au sein de la DPC.

5.3 MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

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

5.3.1 QUALIFICATIONS, COMPETENCES ET HABILITATIONS REQUISES

Tous les personnels intervenant sur l'IGC sont soumis à un devoir de réserve.
Le responsable de l'application IGC s'assure que les attributions des personnels détenteurs de rôles de confiance correspondent à leurs compétences professionnelles et tient à jour la liste des personnels intervenants sur l'IGC.
Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier des procédures de sécurité en vigueur au sein de l'ACD.
L'AC informe toute personne intervenant dans des rôles de confiance de l'AC :

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

par une lettre de mission signée par l'AC.

5.3.2PROCEDURES DE VERIFICATION DES ANTECEDENTS

Le personnel amené à assurer un rôle de confiance vis-à-vis de l'ACD fait l'objet lors de son entrée en fonction, d'une vérification de ses antécédents par les services du Ministère.
Ces personnels ne doivent notamment pas avoir de condamnation incompatible avec leurs attributions.
Les personnes ayant un rôle de confiance ne souffrent pas de conflits d'intérêts préjudiciables à l'impartialité de leurs tâches. En particulier, les Porteurs de secrets permettant la reconstitution de la clé privée de l'AC ne subissent pas de pression hiérarchique les incitants à se dessaisir de leur secret.

5.3.3 EXIGENCES EN MATIERE DE FORMATION INITIALE

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

5.3.4 EXIGENCES ET FREQUENCE EN MATIERE DE FORMATION CONTINUE

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

5.3.5 FREQUENCE ET SEQUENCE DE ROTATION ENTRE DIFFERENTES ATTRIBUTIONS

Aucune rotation programmée des attributions n'est prévue.

5.3.6 SANCTIONS EN CAS D'ACTIONS NON AUTORISEES

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

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

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

5.3.8 DOCUMENTATION FOURNIE AU PERSONNEL

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

5.4 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

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

5.4.1 TYPES D'EVENEMENTS A ENREGISTRER

5.4.1.1 ENREGISTREMENTS SUR PAPIER OU BUREAUTIQUE

Sont enregistrés sur papier :

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

Doivent être enregistrés sur outil bureautique :

- les actions de maintenance et de changements de configuration des systèmes de l'infrastructure suivant les procédures d'exploitation ;
- les changements apportés au personnel détenteur de rôle de confiance ;
- les mises à jour de la présente PC, au sein du présent document.

5.4.1.2 ENREGISTREMENTS ELECTRONIQUES PAR L'APPLICATION IGC

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

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

5.4.1.3 AUTRES ENREGISTREMENTS ELECTRONIQUES

Les accès physiques aux locaux hébergeant l'infrastructure matérielle font l'objet d'un enregistrement électronique automatique.
Les événements suivants font l'objet d'un enregistrement électronique au niveau des systèmes d'exploitation de la plate-forme hébergeant l'ACD, dès le démarrage de ceux-ci :

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation ;
- modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des détenteurs des rôles de confiance, et les tentatives non réussies correspondantes.

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

- publication de la LCR.

5.4.1.4 CARACTERISTIQUES COMMUNES

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

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

La personne, le service ou le système ayant exécuté l'événement doit être responsable de sa journalisation.
Les opérations de journalisation électronique doivent être effectuées au cours du processus ou à la fin de celui-ci.
En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement.

5.4.2 FREQUENCE DE TRAITEMENT DES JOURNAUX D'EVENEMENTS

Cf. chapitre 5.4.8 « Évaluation des vulnérabilités » ci-dessous.

5.4.3 PERIODE DE CONSERVATION DES JOURNAUX D'EVENEMENTS

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

5.4.3.1 ENREGISTREMENTS SUR PAPIER OU BUREAUTIQUE

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

5.4.3.2 ENREGISTREMENTS ELECTRONIQUES PAR L'APPLICATION IGC

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

5.4.3.3 AUTRES ENREGISTREMENTS ELECTRONIQUES

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

5.4.4 PROTECTION DES JOURNAUX D'EVENEMENTS

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.
Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).
Le système de datation des évènements respecte les exigences du chapitre 6.8.

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

5.4.4.1 ENREGISTREMENTS SUR PAPIER OU BUREAUTIQUE

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

5.4.4.2 ENREGISTREMENTS ELECTRONIQUES PAR L'APPLICATION IGC

Les journaux d'événements conservés par l'application IGC sont protégés en intégrité.
Ils ne sont accessibles qu'en lecture et exclusivement pour les administrateurs centraux.

5.4.4.3 AUTRES ENREGISTREMENTS ELECTRONIQUES

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

5.4.5 PROCEDURE DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS

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

5.4.5.1 ENREGISTREMENTS SUR PAPIER OU BUREAUTIQUE

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

5.4.5.2 ENREGISTREMENTS ELECTRONIQUES PAR L'APPLICATION IGC

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

5.4.5.3 AUTRES ENREGISTREMENTS ELECTRONIQUES

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

5.4.6 SYSTEME DE COLLECTE DES JOURNAUX D'EVENEMENTS

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

5.4.7 NOTIFICATION DE L'ENREGISTREMENT D'UN EVENEMENT AU RESPONSABLE DE L'EVENEMENT

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

5.4.8 ÉVALUATION DES VULNERABILITES

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

5.5 ARCHIVAGE DES DONNEES

5.5.1 TYPES DE DONNEES A ARCHIVER

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

Les données archivées sont au minimum les suivantes :

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

5.5.1.1 DONNEES SOUS FORME PAPIER OU BUREAUTIQUE :

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

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

Les données conservées sous forme de document bureautique et archivées sont :

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

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

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

5.5.1.3 AUTRES DONNEES SOUS FORME ELECTRONIQUE :

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

5.5.2 PERIODE DE CONSERVATION DES ARCHIVES

5.5.2.1 DOSSIERS D'ENREGISTREMENT

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

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

Recouvrement des certificats de confidentialité :
Tout dossier de demande de recouvrement accepté est archivé pendant au moins cinq ans, comptés à partir de la fin du séquestre par l'AC de la clé privée correspondante.
Au cours de cette durée d'opposabilité des documents, le dossier de demande de recouvrement doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées.
Ce dossier doit permettre de retrouver l'identité réelle de la personne physique ayant demandé et obtenu le recouvrement.

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

5.5.2.2 LCR EMISES PAR L'AC

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

5.5.2.3 JOURNAUX D'EVENEMENTS

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

5.5.2.4 DONNEES SOUS FORME PAPIER ET BUREAUTIQUE

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

5.5.3 PROTECTION DES ARCHIVES

Pendant tout le temps de leur conservation, les archives :

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

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

5.5.4 PROCEDURES DE SAUVEGARDE DES ARCHIVES

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

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

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

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

5.5.5 EXIGENCES D'HORODATAGE DES DONNEES

5.5.5.1 DONNEES SOUS FORME PAPIER OU BUREAUTIQUE

La datation des données enregistrées est réalisée à partir d'une source de temps d'utilisation courante supposée correcte avec une précision inférieure à 30 minutes.

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

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

5.5.6 SYSTEME DE COLLECTE DES ARCHIVES

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

5.5.6.1 DONNEES SOUS FORME PAPIER OU BUREAUTIQUE

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

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

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

5.5.7 PROCEDURES DE RECUPERATION ET DE VERIFICATION DES ARCHIVES

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

5.5.7.1 DONNEES SOUS FORME PAPIER OU BUREAUTIQUE

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

5.5.7.2 DONNEES DE L'APPLICATION IGC (SOUS FORME ELECTRONIQUE)

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

5.6 CHANGEMENT DE CLE D'AC

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

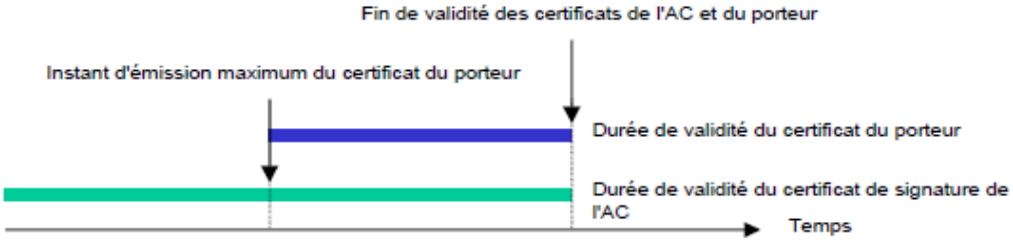


Figure 2 : Changement de clé d'AC

Au regard de la date de fin de validité d'un certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.
Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.
Le nommage utilisé pour distinguer les clés successives de l'autorité de certification répond aux règles suivantes.

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

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

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

5.7 REPRISE SUITE A COMPROMISSION ET SINISTRE

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

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

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

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

L'ACD dispose d'un Plan de Reprise d'Activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'AC découlant de la présente PC et identifiées comme critiques.
Ce plan doit être testé au minimum une fois tous les deux ans.

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

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

5.7.4 CAPACITES DE CONTINUITE D'ACTIVITE SUITE A UN SINISTRE

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

5.8 FIN DE VIE DE L'IGC

Dans l'hypothèse d'une cessation d'activité totale, l'ACD s'engage à assurer la continuité des fonctions de révocation des certificats et la publication de la LCR, dans la limite de ses propres possibilités.
En particulier, lors de l'arrêt du service, l'ACD :

1) doit s'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
2) doit prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
3) doit demander la révocation de son certificat auprès de l'AC RACINE DIPLOMATIE si cette dernière a certifié sa clé ;
4) doit révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
5) doit publier cette information sur les sites web *http://crl.diplomatie.gouv.fr* (dédié aux LCR des AC et aux autres informations).

6 MESURES DE SECURITE TECHNIQUES

6.1 GENERATION ET INSTALLATION DE BI-CLES

6.1.1 GENERATION DE BI-CLES

6.1.1.1 CLES D'AC

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

Les clés sont générées et mises en œuvre dans un module cryptographique de type HSM (Hardware Security Module).

La génération de la clé des ACD est effectuée dans des circonstances contrôlées, par des personnels dans des rôles de confiance, dans le cadre de « Cérémonies de Clés ». Ces Cérémonies se déroulent suivant des scripts préalablement définis. Ces documents ne sont pas publics.

La génération des clés des AC s'accompagnent de la génération de parts de secrets. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées des AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés des ACD.

Suite à leur génération, les parts de secrets sont remises à des Porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance. Un même Porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets est mise en œuvre par son Porteur.

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

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

6.1.1.1 CLES DE PORTEURS GENEREES PAR L'AC

Les Bi-clés de chiffrement sont générées en central par l'AC puis importées sur la carte. Elles sont séquestrées par l'AC.

6.1.1.2 CLES DE PORTEURS GENEREES PAR LE PORTEUR

Les Bi-clés d'authentification et de signature sont générées dans la carte MAE par l'AC. Elles ne sont pas séquestrées par l'AC. Cette génération est effectuée dans un dispositif répondant aux exigences de sécurité pour le niveau de sécurité considéré. L'AC s'assure que la clé publique exportée réside effectivement dans le dispositif de protection des éléments secrets du porteur.

6.1.2TRANSMISSION DE LA CLE PRIVEE AU PORTEUR

Le transfert de la clé privée au Porteur s'effectue via l'Opérateur du bureau des badges lors de la remise de la carte MAE, pendant l'entretien en face à face. L'AC déclenche la génération des clés privées de signature et d'authentification des Porteurs directement sur leur support (la carte MAE) en utilisant le module cryptographique contenu dans la carte.

Pour les clés de chiffrement, les clés privées sont générées en central par l'AC puis importées sur la carte MAE pendant l'entretien en face à face, et l'AC procède au séquestre de la clé.

Dans les deux cas, les transferts de données entre la carte MAE et l'AC sont effectuées via le système de gestion de certificats sur carte à puce.

La DPC détaille les mesures mises en œuvre.

6.1.3 TRANSMISSION DE LA CLE PUBLIQUE A L'AC

La transmission de la clé publique du Porteur à l'AC UTILISATEURS RENFORCÉE N, pour permettre la signature du certificat du Porteur, est effectuée en ligne après authentification réciproque.

La communication est protégée de bout en bout en confidentialité et en intégrité.

La DPC détaille les mesures mises en œuvre.

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

La clé publique des AC Déléguées sont publiées et accessibles aux tiers utilisateurs de certificats.

Pour les tiers utilisateurs internes au Ministère, les clés publiques des ACD seront installées automatiquement dans le magasin de certificat des postes de travail.

6.1.5 TAILLE DE CLES

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

La longueur des clés des Porteurs émises par l'AC UTILISATEURS RENFORCÉE N est 2048 bits.

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

La vérification est faite par l'application qui utilise les certificats.

6.1.7 OBJECTIFS D'USAGE DE LA CLE

La clé de signature de l'AC UTILISATEURS RENFORCÉE N est utilisée uniquement pour signer les certificats des Porteurs, les LCR et les communications électroniques avec les autres composantes de l'IGC.

Les clés privées d'**authentification** des Porteurs ne sont utilisées qu'à des fins d'authentification forte de leur titulaire.

Les clés privées de **signature** des Porteurs ne sont utilisées qu'à des fins de signature électronique de fichiers ou documents.

Les clés privées de **chiffrement** ne sont utilisées que pour déchiffrer des données préalablement chiffrées avec les clés publiques associées (intégrées au certificat concerné).

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

6.2.1 STANDARDS ET MESURES DE SECURITE POUR LES MODULES CRYPTOGRAPHIQUES

6.2.1.1 MODULES CRYPTOGRAPHIQUES DE L'AC

Les modules cryptographiques, utilisés par les ACD, pour la génération et la mise en œuvre de leurs clés, sont des modules cryptographiques de type HSM (*Hardware Security Module*) répondant au minimum aux exigences du chapitre 11 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 DES PORTEURS

Les dispositifs de protection des éléments secrets des porteurs, pour la mise en œuvre de leurs clés privées de personne, doivent respecter les exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré.

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 » via un outil mettant en œuvre le partage des secrets.

6.2.3 SEQUESTRE DE LA CLE PRIVEE

Les clés privées d'AC ne sont pas séquestrées.

Les clés privées d'authentification et de signature des Porteurs ne sont pas séquestrées.

Les clés privées de chiffrement des Porteurs sont chiffrées et séquestrées sur une base de données prévue à cet effet.

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 Porteurs 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 se fait sous forme chiffrée depuis le module cryptographique et est soumis à un dispositif mettant en œuvre le partage de secrets.

6.2.7 STOCKAGE DE LA CLE PRIVEE DANS UN MODULE CRYPTOGRAPHIQUE

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

6.2.8 METHODE D'ACTIVATION DE LA CLE PRIVEE

6.2.8.1 CLE PRIVEE D'AC

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

6.2.8.2 CLE PRIVEE DES PORTEURS

Les clés privées des Porteurs sont utilisables avec des données d'activation, appelée « code PIN ». C'est le même code utilisé pour les certificats contenus sur la carte MAE appelée « code PIN global ».

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 de Porteurs

Sans objet.

6.2.10 Methode de destruction des cles privees

6.2.10.1 Cle privee d'AC

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

6.2.10.2 Cle privee de Porteurs

La destruction des clés privées correspondant aux certificats des Porteurs sont gérés par la ressource matérielle qui les héberge, c'est-à-dire par la carte MAE et son middleware du lecteur de carte.

Lors du premier renouvellement des certificats, la même carte MAE peut être réutilisée, en conséquence, le contenu de la carte est effacé complètement, et les nouveaux certificats sont installés.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs de protection de cles prives

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

Les cartes à puce utilisées respectent la norme IAS-ECC et sont certifiées 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 Porteurs sont archivées dans le cadre de l'archivage des certificats correspondants.

6.3.2 Durees de vie des bi-cles et des certificats

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

- 9 ans pour AC UTILISATEURS RENFORCEE
- 2082 jours pour AC UTILISATEURS RENFORCEE 2
- 9 ans pour AC UTILISATEURS RENFORCEE 3

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

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

6.4 DONNEES D'ACTIVATION

6.4.1 GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION

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

La génération et l'installation des données d'activation des modules cryptographiques de l'IGC, au sein desquels sont mises en œuvre les clés des AC, se font lors de la phase d'initialisation et de personnalisation de ce module, pendant la Cérémonie des Clés. Les données d'activation sont choisies et saisies par les Porteurs de secret responsables de ces données.

6.4.1.2 GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION CORRESPONDANT A LA CLE PRIVEE DU PORTEUR

Les données d'activation sont choisies par le Porteur.

Plus d'informations sont fournies dans la DPC.

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 PORTEURS

Les données d'activation sont des données secrètes. Les données d'activation de la clé privée d'un Porteur sont sous son contrôle exclusif et il lui appartient de les protéger.

Le Porteur doit mettre en œuvre tous les moyens nécessaires pour protéger sa donnée d'activation, en particulier, ne pas noter cette donnée et ne pas le communiquer.

Lors de l'entretien en face à face avec l'Opérateur du bureau des badges, l'Opérateur invite l'utilisateur à renseigner sa donnée d'activation de façon confidentielle, directement dans le système de gestion des cartes.

6.4.3 AUTRES ASPECTS LIES AUX DONNEES D'ACTIVATION

Sans objet.

6.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

Les mesures de sécurité relatives aux systèmes informatiques satisfont aux objectifs de sécurité qui découlent de l'analyse de risque que l'AC peut mener (cf. chapitre I.4.1).

Une analyse des objectifs de sécurité peut être effectuée en amont de tout projet d'IGC par l'AC, de façon à garantir la prise en compte de la sécurité dans les systèmes informatiques.

Le ministère est en mesure de justifier, par tout moyen, qu'il a pris les mesures nécessaires pour assurer la protection des échanges d'information entre les différentes composantes de l'IGC. Il vérifie périodiquement les mesures de sécurité prises dans ce cadre. Le moyen privilégié consiste en un audit technique réalisé par un prestataire d'audit de la sécurité des systèmes d'information qualifié.

6.5.1 EXIGENCES DE SECURITE TECHNIQUE SPECIFIQUES AUX SYSTEMES INFORMATIQUES

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

- identification et authentification forte des détenteurs de rôles de confiance pour l'accès aux serveurs hébergeant les AC Déléguées,
- identification et authentification forte des administrateurs centraux pour l'accès à l'IGC,
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels,
- gestion des comptes des administrateurs centraux au niveau de l'application IGC,
- gestion des comptes des détenteurs de rôles de confiance au niveau des systèmes des serveurs des AC Déléguées,
- protection du réseau contre toute intrusion d'une personne non autorisée,
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui transitent entre les composantes des ACD,
- fonctions d'audits (imputabilité des actions effectuées),
- gestion des incidents,
- protection en confidentialité, en intégrité et en disponibilité des clés nécessaires au fonctionnement des ACD.

6.5.2 NIVEAU DE QUALIFICATION DES SYSTEMES INFORMATIQUES

Sans objet.

6.6 MESURES DE SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES

6.6.1 MESURES LIEES A LA GESTION DE LA SECURITE

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

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

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

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

6.6.3NIVEAU D'EVALUATION DU CYCLE DE VIE DES SYSTEMES

Sans objet.

6.7 MESURES DE SECURITE RESEAU

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

6.8 HORODATAGE / SYSTEME DE DATATION

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

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 PROFILS DES CERTIFICATS

7.1.1 PROFILS DE CERTIFICAT DE L'AC UTILISATEURS RENFORCÉE N

Généralités

Attribut	Valeur
Nom de l'Autorité de Certification (Attribut « CN »)	AC UTILISATEURS RENFORCEE N
Nom de l'Unité Organisationnelle (Attribut « OU »)	0002 12000601000025
Nom de l'Organisation (Attribut « O »)	MINISTERE DES AFFAIRES ETRANGERES
Pays (Attribut « C »)	FR
Longueur des clefs de l'AC	4096 bits
Espace de création des clefs	Matériel sur HSM
Durée de validité du certificat	9 ans pour la première AC 2082 jours pour la seconde AC 9 ans pour la troisième AC

Champs de base

Champ	Valeur
Version	V3

Champ	Valeur
Numéro de série	*Défini lors de la cérémonie des clés*
DN Émetteur	CN= AC RACINE DIPLOMATIE OU= 0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C = FR
DN Objet	CN= AC UTILISATEURS RENFORCEE N OU= 0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C = FR
Valide à partir du	YYMMDDHHMMSS
Valide jusqu'au	YYMMDDHHMMSS + 9 ans pour la première AC YYMMDDHHMMSS + 2082 jours pour la seconde AC YYMMDDHHMMSS + 9 ans pour la troisième AC
Algorithme de clé publique	sha2WithRSAEncryption (sha256RSA ou 1.2.840.113549.1.1.13)

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

Extensions standards

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé du sujet	O	N	<Valeur de Hachage>
Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Utilisation de la clé	O	O	Signature du certificat, Signature de la liste de révocation de certificats hors connexion, Signature de la liste de révocation de certificats (06)
Stratégies de certificat	O	N	Identificateur de politique = OID de la PC de l'AC régissant l'émission du certificat 1.2.250.1.214.69.3.1.1.1.1.1 (=OID de la PC de l'AC RACINE DIPLOMATIE)
Points de distribution des LCR	O	N	http://crl.diplomatie.gouv.fr/AC_Racine_Diplomatie/crl/crl-1.crl
Contraintes de base	O	O	Type d'objet=Autorité de certification Contrainte de longueur de chemin d'accès=Aucun(e)

Tableau 6 : Gabarits des certificats de l'AC UTILISATEURS RENFORCÉE

7.1.2 PROFILS DE CERTIFICAT DES AGENTS

Les champs généralités et champs de base sont communs aux trois gabarits de certificats Agent (authentification forte, signature forte, confidentialité forte)

Généralités

Attribut	Valeur
Nom du Porteur (Attribut « CN »)	<Prenom NOM>
Adresse de courriel (Attribut « E »)	<prenom.nom@diplomatie.gouv.fr>
Identifiant unique	<logon Windows>

Authentification forte Agent 1.2.250.1.214.69.3.1.6.1.1.2
Signature forte Agent 1.2.250.1.214.69.3.1.6.1.3.2
Confidentialité forte Agent 1.2.250.1.214.69.3.1.6.1.5.2
Authentification forte Externe 1.2.250.1.214.69.3.1.6.1.7.2
Signature forte Externe 1.2.250.1.214.69.3.1.6.1.9.2
Confidentialité forte Externe 1.2.250.1.214.69.3.1.6.1.11.2
Cotation Archive : E.3.1.6.1

(Attribut « 0.9.2342.19200300.100.1.1 »)	
Code Agent (Attribut « SERIALNUMBER »)	<identifiant AROBAS>
Nom de l'Unité Organisationnelle (Attribut « OU »)	0002 12000601000025
Nom de l'Organisation (Attribut « O »)	MINISTERE DES AFFAIRES ETRANGERES
Pays (Attribut « C »)	FR
Longueur des clefs émises par l'AC	2048 bits
Espace de création des clefs	Matériel sur support physique (de type carte à puce)
Durée de validité du certificat	3 ans

Champs de base

Champ	Valeur
Version	V3
Numéro de série	Défini par Opentrust PKI
DN Émetteur	CN= AC UTILISATEURS RENFORCEE N OU= 0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C = FR
DN Objet	CN= <Prenom NOM> E= <prenom.nom@diplomatie.gouv.fr> UID=<logon Windows> SERIALNUMBER = <identifiant AROBAS> OU= 0002 12000601000025

	O= MINISTERE DES AFFAIRES ETRANGERES C = FR
Valide à partir du	YYMMDDHHMMSS
Valide jusqu'au	YYMMDDHHMMSS + 3 ans
Algorithme de clé publique	sha2WithRSAEncryption (1.2.840.113549.1.1.13)

Tableau 7 : Gabarits des certificats Agent (Généralités et champs de base) issus de AC UTILISATEURS RENFORCEE

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

Les tableaux suivants décrivent les champs extensions propre à chaque gabarit :

7.1.2.1 GABARIT AUTHENTIFICATION FORTE AGENT

Extensions standards

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé du sujet	O	N	<Valeur de Hachage>
Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>
Utilisation de la clé	O	O	Signature numérique (80)
Stratégies de certificat	O	N	Identificateur de politique = OID de la PC de l'AC régissant l'émission du certificat 1.2.250.1.214.69.3.1.6.1.1.2

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Autre nom de l'objet	O	N	Microsoft UPN=<prenom.nom@comptes.diplomatie.gouv.fr>
Points de distribution des LCR	O	N	http://crl.diplomatie.gouv.fr/AC_Utilisateurs_Renforcee_N/Crl/AC_UTILISATEURS_RENFORCEE_N.crl
Contraintes de base	O	O	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)

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

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Utilisation avancée de la clé	N	N	Authentification SSL/TLS client (clientAuth) (1.3.6.1.5.5.7.3.2) Login par carte à puce Microsoft (msSmartcardLogin)
Type de certificat Netscape	N	N	Authentification SSL/TLS client (NSclient)

Tableau 8 : Gabarits des certificats Authentification forte Agent (Extensions) issus de AC UTILISATEURS RENFORCEE

7.1.2.2 GABARIT SIGNATURE FORTE AGENT

Extensions standards

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé du sujet	O	N	<Valeur de Hachage>

Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>
Utilisation de la clé	O	O	Non-Répudiation (40)
Stratégies de certificat	O	N	Identificateur de politique = OID de la PC de l'AC régissant l'émission du certificat 1.2.250.1.214.69.3.1.6.1.3.2
Autre nom de l'objet	N	N	Nom RFC822=<prenom.nom@diplomatie.gouv.fr>
Points de distribution des LCR	O	N	http://crl.diplomatie.gouv.fr/AC_Utilisateurs_Renforcee_N/Crl/AC_UTILISATEURS_RENFORCEE_N.crl
Contraintes de base	O	O	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)

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

Autres extensions

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Utilisation avancée de la clé	N	N	Messagerie électronique sécurisée (1.3.6.1.5.5.7.3.4)

Tableau 9 : Gabarits des certificats Signature forte Agent (Extensions) issus de AC UTILISATEURS RENFORCEE

7.1.2.3 GABARIT CONFIDENTIALITÉ FORTE AGENT

Extensions standards

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé du sujet	O	N	<Valeur de Hachage>
Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>
Utilisation de la clé	O	O	Cryptage de la clé (20)
Stratégies de certificat	O	N	Identificateur de politique = OID de la PC de l'AC régissant l'émission du certificat 1.2.250.1.214.69.3.1.6.1.5.2
Autre nom de l'objet	N	N	Nom RFC822=<prenom.nom@diplomatie.gouv.fr>
Points de distribution des LCR	O	N	http://crl.diplomatie.gouv.fr/AC_Utilisateurs_Renforcee_N/Crl/AC_UTILISATEURS_RENFORCEE_N.crl
Contraintes de base	O	O	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)

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

Autres extensions

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur

Utilisation avancée de la clé	N	N	Messagerie électronique sécurisée (1.3.6.1.5.5.7.3.4)
Type de certificat Netscape	N	N	Messagerie électronique sécurisée SMIME (20)

Tableau 10 : Gabarits des certificats Confidentialité forte Agent (Extensions) issus de AC UTILISATEURS RENFORCEE

7.1.3 PROFILS DE CERTIFICAT DES EXTERNES

Les champs généralités et champs de base sont communs aux trois gabarits de certificats Externe (authentification forte, signature forte, confidentialité forte)

Généralités

Attribut	Valeur
Nom du Porteur (Attribut « CN »)	<Prenom NOM>
Code Agent (Attribut « SERIALNUMBER »)	<identifiant AROBAS>
Nom de l'Unité Organisationnelle (Attribut « OU »)	0002 12000601000025
Nom de l'Organisation (Attribut « O »)	MINISTERE DES AFFAIRES ETRANGERES
Pays (Attribut « C »)	FR
Longueur des clefs émises par l'AC	2048 bits

Authentification forte Agent 1.2.250.1.214.69.3.1.6.1.1.2
Signature forte Agent 1.2.250.1.214.69.3.1.6.1.3.2
Confidentialité forte Agent 1.2.250.1.214.69.3.1.6.1.5.2
Authentification forte Externe 1.2.250.1.214.69.3.1.6.1.7.2
Signature forte Externe 1.2.250.1.214.69.3.1.6.1.9.2
Confidentialité forte Externe 1.2.250.1.214.69.3.1.6.1.11.2
Cotation Archive : E.3.1.6.1

Attribut	Valeur
Espace de création des clefs	Matériel sur support physique (de type carte à puce)
Durée de validité du certificat	3 ans

Champs de base

Champ	Valeur
Version	V3
Numéro de série	Défini par Opentrust PKI
DN Émetteur	CN= AC UTILISATEURS RENFORCEE N OU= 0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C = FR
DN Objet	CN= <Prenom NOM> SERIALNUMBER = <identifiant AROBAS> OU= 0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C = FR
Valide à partir du	YYMMDDHHMMSS
Valide jusqu'au	YYMMDDHHMMSS + 3 ans
Algorithme de clé publique	sha2WithRSAEncryption (1.2.840.113549.1.1.13)

Tableau 11 : Gabarits des certificats Externe (Généralités et champs de base) issus de AC UTILISATEURS RENFORCEE

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

Les tableaux suivants décrivent les champs extensions propres à chaque gabarit :

7.1.3.1 GABARIT AUTHENTIFICATION FORTE EXTERNE

Extensions standards

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé du sujet	O	N	<Valeur de Hachage>
Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>
Utilisation de la clé	O	O	Signature numérique (80)
Stratégies de certificat	O	N	Identificateur de politique = OID de la PC de l'AC régissant l'émission du certificat 1.2.250.1.214.69.3.1.6.1.7.2
Points de distribution des LCR	O	N	http://crl.diplomatie.gouv.fr/AC_Utilisateurs_Renforcee_N/Crl/AC_UTILISATEURS_RENFORCEE_N.crl
Contraintes de base	O	O	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)

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

Autres extensions

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Utilisation avancée de la clé	N	N	Authentification SSL/TLS client (clientAuth) (1.3.6.1.5.5.7.3.2)

Type de certificat Netscape	N	N	Authentification SSL/TLS client (NSclient)

Tableau 12 : Gabarits des certificats Authentification forte Externe (Extensions) issus de AC UTILISATEURS RENFORCEE

7.1.3.2 GABARIT SIGNATURE FORTE EXTERNE

Extensions standards

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé du sujet	O	N	<Valeur de Hachage>
Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>
Utilisation de la clé	O	O	Non-Répudiation (40)
Stratégies de certificat	O	N	Identificateur de politique = OID de la PC de l'AC régissant l'émission du certificat 1.2.250.1.214.69.3.1.6.1.9.2
Points de distribution des LCR	O	N	http://crl.diplomatie.gouv.fr/AC_Utilisateurs_Renforcee_N/Crl/AC_UTILISATEURS_RENFORCEE_N.crl
Contraintes de base	O	O	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)

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

Autres extensions

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Utilisation avancée de la clé	N	N	Messagerie électronique sécurisée (1.3.6.1.5.5.7.3.4)

Tableau 13 : Gabarits des certificats Signature forte Externe (Extensions) issus de AC UTILISATEURS RENFORCEE

7.1.3.3 GABARIT CONFIDENTIALITÉ FORTE EXTERNE

Extensions standards

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé du sujet	O	N	<Valeur de Hachage>
Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>
Utilisation de la clé	O	O	Cryptage de la clé (20)
Stratégies de certificat	O	N	Identificateur de politique = OID de la PC de l'AC régissant l'émission du certificat 1.2.250.1.214.69.3.1.6.1.11.2
Points de distribution des LCR	O	N	http://crl.diplomatie.gouv.fr/AC_Utilisateurs_Renforcee<_N>/Crl/AC_UTILISATEURS_RENFORCEE<_N>.crl

Contraintes de base	O	O	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)

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

Autres extensions

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Utilisation avancée de la clé	N	N	Messagerie électronique sécurisée (1.3.6.1.5.5.7.3.4)
Type de certificat Netscape	N	N	Messagerie électronique sécurisée SMIME (20)

Tableau 14 : Gabarits des certificats Confidentialité forte Externe (Extensions) issus de AC UTILISATEURS RENFORCEE

7.2 PROFILS DES CRL

La CRL de l'AC UTILISATEURS RENFORCEE sera publié sur le serveur http et disponible à l'adresse suivante :

http://crl.diplomatie.gouv.fr/AC_Utilisateurs_Renforcee_N/Crl/AC_UTILISATEURS_RENFORCEE_N.crl

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

Le gabarit est décrit dans le tableau suivant :

Champs de base

Champs	Valeur
Version	V2
Numéro de série	Défini par Opentrust PKI

DN Émetteur	CN= AC UTILISATEURS RENFORCEE N OU= 0002 12000601000025 O= MINISTERE DES AFFAIRES ETRANGERES C = FR
Certificats révoqués	Pour chaque certificat révoqué : n° de série du certificat date de révocation du certificat
Date d'effet	YYMMDDHHMMSS
Durée de validité	YYMMDDHHMMSS + 7 jours
Prochaine mise à jour	YYMMDDHHMMSS + 24 heures
Algorithme de clé publique	sha2WithRSAEncryption (1.2.840.113549.1.1.13)

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

Extensions standards

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>
Numéro de CRL	O	N	Numéro unique et incrémental défini par Opentrust PKI

Tableau 15 : Gabarits des listes de certificats révoqués finaux issus de l'AC UTILISATEURS RENFORCÉE

7.3 PROFILS 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 des ACD autre que le présent rôle et doit être dûment autorisé à pratiquer les contrôles visés.

8.4 SUJETS COUVERTS PAR LES EVALUATIONS

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

8.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

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

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.

- En cas de résultat "à confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

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

8.6 COMMUNICATION DES RESULTATS

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

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 TARIFS

9.1.1 TARIFS POUR LA FOURNITURE OU LE RENOUVELLEMENT DE CERTIFICATS

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

9.1.2 TARIFS POUR ACCEDER AUX CERTIFICATS

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

9.1.3 TARIFS POUR ACCEDER AUX INFORMATIONS D'ETAT ET DE REVOCATION DES CERTIFICATS

L'accès aux LCR est libre en lecture.

9.1.4 TARIFS POUR D'AUTRES SERVICES

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

9.1.5 POLITIQUE DE REMBOURSEMENT

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

9.2 RESPONSABILITE FINANCIERE

Conformément à ses obligations, l'AC doit prendre les dispositions nécessaires pour couvrir, éventuellement financièrement, ses responsabilités liées à ses opérations et/ou activités.

9.2.1 COUVERTURE PAR LES ASSURANCES

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

9.2.2 AUTRES RESSOURCES

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

9.2.3 COUVERTURE ET GARANTIE CONCERNANT LES ENTITES UTILISATRICES

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

9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

9.3.1 PERIMETRE DES INFORMATIONS CONFIDENTIELLES

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

9.3.2 INFORMATIONS HORS DU PERIMETRE DES INFORMATIONS CONFIDENTIELLES

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

9.3.3 RESPONSABILITES EN TERMES DE PROTECTION DES INFORMATIONS CONFIDENTIELLES

La présente PC ne formule pas d'exigence supplémentaire au respect de la législation et de la réglementation en vigueur sur le territoire français relatives à la protection des informations confidentielles.

9.4 PROTECTION DES DONNEES PERSONNELLES

9.4.1 POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES

Toute collecte et tout usage de données à caractère personnel par l'AC et les rôles de confiance de l'AC sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
En particulier, l'IGC en tant qu'infrastructure de stockage et de gestion de données nominatives contenues dans les certificats électroniques, est déclarée et soumise à l'avis de la CNIL selon les termes de la Loi n° 78-17 du 6 janvier 1978 « Informatique et Libertés ».
Le récépissé de cette déclaration porte le numéro : 1245693.

9.4.2 INFORMATIONS A CARACTERE PERSONNEL

Les informations considérées comme personnelles sont les suivantes :

- les codes d'activation des cartes d'authentification administrateur des administrateurs de l'ACD ;
- les causes de révocation des certificats des Porteurs ;
- le dossier d'enregistrement des Porteurs.

9.4.3 INFORMATIONS 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 Porteurs ;
- 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 Porteur donné et que ce Porteur 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 Porteurs 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 Porteur 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 Porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

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

9.6.3PORTEURS DE CERTIFICATS

Le Porteur 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 Porteur et l'AC ou ses composantes est formalisée par un engagement du Porteur 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 ;
- pour chaque certificat de la chaîne de certification, du certificat du Porteur 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

Les Mandataires de Certification doivent :

- vérifier les éléments d'identification des Porteurs pour lesquels ils sont Mandataires ;
- respecter les obligations des Mandataires exprimées dans la présente PC.

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 UTILISATEURS est d'émettre des certificats à destination des Porteurs agents 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 UTILISATEURS RENFORCEE.
En cas de changement important, l'AC s'engage à faire appel à un auditeur pour en contrôler l'impact.

9.12.2 MECANISME ET PERIODE D'INFORMATION SUR LES AMENDEMENTS

Les tiers utilisateurs de certificat peuvent prendre connaissance des amendements au moyen du site web *http://crl.diplomatie.gouv.fr*. Les ACD seront également informées de ces amendements.

9.12.3 CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE

L'OID de la présente PC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) ou du document décrivant les profils associés se traduira par une évolution de l'OID. En particulier, des modifications de forme n'entraîneront pas une modification de l'OID.
Le nouvel OID, si nouvel OID il y a, apparaîtra dans tout nouveau certificat émis par l'ACD. Ainsi, les tiers utilisateurs de certificat pourront clairement distinguer quels certificats correspondent à quelles exigences.

9.13 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

L'AC mets en place des politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles elle fournit des services électroniques de confiance ou d'autres points qui y sont liés.

9.14 JURIDICTIONS COMPETENTES

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

9.15 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

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

Les textes législatifs et réglementaires applicables à la présente PC sont les suivants :

[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004
[ORDONNANCE]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre

	les autorités administratives
[DécretRGS]	Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005
[LSQ]	Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.
[DIRSIG]	Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.
[LCEN]	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
[SIG]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique

L'AC est notamment soumise aux dispositions prévues par l'article 31 de la [LSQ] concernant la remise des clés privées des porteurs, si celles-ci sont séquestrées par l'AC

9.16 DISPOSITIONS DIVERSES

9.16.1 ACCORD GLOBAL

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

9.16.2 TRANSFERT D'ACTIVITES

Cf. partie 5.8.

9.16.3 CONSEQUENCES D'UNE CLAUSE NON VALIDE

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

9.16.4 APPLICATION ET RENONCIATION

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

9.16.5 FORCE MAJEURE

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.

9.17 AUTRES DISPOSITIONS

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

10 ANNEXE 1 : EXIGENCES DE SECURITE DU DISPOSITIF DE PROTECTION DE CLES PRIVEES

Le dispositif de protection de clés privées, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- si la bi-clé de confidentialité du porteur est générée par le dispositif, 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 des clés privées qui ne sont plus utilisées ;
- garantir la confidentialité et l'intégrité des clés privées ;
- assurer la correspondance entre la clé privée et la clé publique ;
- assurer la fonction de déchiffrement, de clés symétriques de fichier ou de message, 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 symétrique de fichier ou de message, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif ;
- le cas échéant, permettre de garantir la confidentialité, l'authenticité et l'intégrité de la clé privée lors de son export hors du dispositif, à destination d'une fonction de séquestre ou d'archivage des clés privées.

Fin du document