Damanesign

Politique et déclaration des pratiques de certification AC Racine

Version 1.0 | Diffusion : public

OID n° 1.3.6.1.4.1.58553.1.1.1

Historique du document

Version	Date de version	Rédacteur(s)	Approbateur	Modifications
1.0	**30/08/2022**	**Samuel LACAS**	**Noureddin SOUAD**	**Création de la PC et DPC**

Table des matières

1 Introduction

1.1 Présentation générale

Ce document constitue la politique de certification racine et la déclaration des pratiques de certification mise en œuvre par la société Damanesign pour ses besoins internes. Elle réunit l'ensemble des obligations et engagements des différents acteurs relatifs à la délivrance et l'usage des certificats numériques des autorités de certification (A.C.) filles de la chaîne confiance.

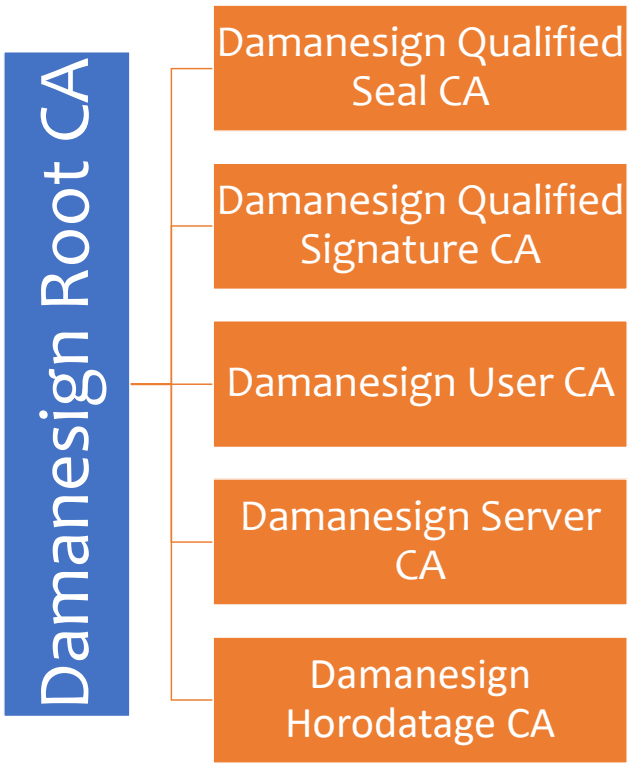
1.2 Identification du document

La présente P.C. est dénommé *Politique et déclaration des pratiques de certification Racine*. Elle est identifiée par son numéro d'identifiant d'objet, ainsi que par le nom, numéro de version, la date de mise à jour.

Le numéro d'OID de la présente P.C. est : **1.3.6.1.4.1.58553.1.1.1**

1.3 Entités intervenant dans l'I.G.C. et responsabilités

La hiérarchie d'A.C. du Groupe est la suivante :



1.3.1 Le Prestataire de services de certification électronique

Dans le cadre de cette P.C., le rôle de P.S.C.E. assuré par la société Damanesign.

À ce titre, il valide la création des A.C. filles.

Le P.S.C.E. est identifié dans tout certificat dont il a la responsabilité au travers des A.C. ayant émis ce certificat et qui sont elles-mêmes directement identifiées dans le champ « *issuer* » du certificat.

1.3.2 Autorité de certification

L'A.C. a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) et s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clés (I.G.C.).

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

Dans le cadre de le présente document, l'A.C. est la société Damanesign.

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI dans le domaine, la décomposition fonctionnelle d'une I.G.C. qui est retenue dans la présente P.C. est la suivante :

Fonction	Description	Entité responsable
Fonction d'enregistrement (A.E.)	Cette fonction vérifie les données propres à l'AC fille ainsi que des contraintes liées à l'usage du certificat qui lui est délivré, conformément à la P.C.	D*amanesign*
Fonction de génération des certificats	Cette fonction génère (création du format, signature électronique avec la clé privée associée) les certificats en s'appuyant son infrastructure.	*Damanesign*
Fonction de remise au porteur	Cette fonction remet aux AC filles leur certificat	*Damanesign*
Fonction de publication	Cette fonction met à disposition des différentes parties concernées : les politiques publiées, les certificats d'autorité et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats.	*Damanesign*
Fonction de gestion des révocations	Cette fonction traite les demandes de révocation des AC filles et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.	*Damanesign*
Fonction d'information sur l'état des certificats	Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats.	*Damanesign*

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, notamment à un prestataire de services de confiance (P.S.C.O.), les exigences qui incombent à l'A.C. en tant que responsable de l'ensemble de l'I.G.C. sont les suivantes :

- Être une entité juridique au sens de la loi marocaine.
- S'assurer que les exigences de la P.C. et les procédures de la D.P.C. sont appliquées par chacune des composantes de l'I.G.C. et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa P.C., correspondant au minimum aux fonctions obligatoires de la présente P.C., notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats.
- Élaborer, mettre en œuvre, contrôler et maintenir de façon itérative les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa P.C., et correspondant au minimum aux exigences de la présente P.C., notamment en termes de fiabilité, de qualité et de sécurité.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de L.C.R. et de réponses OCSP).
- Diffuser ses certificats d'A.C. aux porteurs et utilisateurs de certificats.

1.3.3 Autorité d'enregistrement

L'A.E. assure les tâches suivantes :

- La prise en compte et la vérification des informations des A.C. filles et la constitution du dossier d'enregistrement correspondant.

- L'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage)
- La conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du porteur y compris lors des échanges de ces données avec les autres fonctions de l'I.G.C. (notamment, elle respecte la législation relative à la protection des données personnelles). Le déclenchement de la génération programmée ou ponctuelle des LAR ;
- Le déclenchement des fonctions d'archivage des données d'enregistrement des demandes de certificats d'AC, des documents liés aux cérémonies des clés, tout autre document qui doit être conservé pour assurer la traçabilité des actions qui ont lieu autour de la chaîne d'A.C. la réception des dossiers de demande de révocation d'un certificat de la chaîne d'AC ;

En l'état actuel de la P.C., la fonction d'A.E. est exercée directement par l'A.C. dans le cadre des cérémonies de clés durant lesquelles les certificats des A.C. filles sont produits ou révoqués.

1.3.4 Porteurs de certificats

Sans objet.

1.3.5 Utilisateurs de certificat

Un utilisateur de certificat peut être une application ou une personne physique ou morale destinataire de données électroniquement signées ou authentifiées par (respectivement, chiffrées à destination de) une personne ou une machine porteuse d'un certificat émis par une A.C. dépendant de la présente A.C. racine. Cet utilisateur souhaite vérifier l'authenticité ou la validité de la signature électronique apposée sur ces données (resp., chiffrer ces données à destination du bon destinataire).

Les utilisateurs de certificats doivent prendre toutes autres précautions prescrites dans les éventuels accords ou tout autre document fournis par l'A.C.

1.3.6 Mandataire de certification

Sans objet.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Bi-clés et certificats des porteurs

La présente A.C. ne délivre que des certificats d'A.C.

1.4.1.2 Bi-clés et certificats d'A.C.

Une unique bi-clé est utilisée pour la signature des certificats des A.C. filles et de la L.A.R. sous la responsabilité de l'A.C.

1.4.2 Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.5 ci-dessous. L'A.C. respecte ces restrictions et impose leur respect par ses porteurs et ses utilisateurs de certificats.

1.5 Gestion de la P.C.

1.5.1 Entité gérant la P.C.

L'entité gérant la P.C. est Damanesign.

1.5.2 Point de contact

Adresse postale	4 RUE OUED ZIZ 3EME ETAGE APPT 7 AGDAL , Rabat
Adresse courriel	contact@damanesign.ma

1.5.3 Procédures d'approbation de la conformité de la PC et de la D.P.C.

La conformité de la D.P.C. est prononcée par l'A.C. au vu des résultats des audits internes effectués.

Cette PC sera revue périodiquement, a minima annuellement et à chaque changement majeur, par le comité de pilotage de l'A.C. pour assurer sa conformité aux normes de sécurité attendues par l'organisme de contrôle national

1.6 Définitions et sigles

1.6.1 Sigles

Les sigles utilisés dans la présente P.C. sont les suivants :

A.C.	Autorité de Certification
A.E.	Autorité d'Enregistrement
CEN	Comité Européen de Normalisation
DN	*Distinguished Name*
D.P.C.	Déclaration des Pratiques de Certification
ETSI	*European Telecommunications Standards Institute*
L.C.R.	Liste des Certificats Révoqués
O.C.	Opérateur de Certification
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
P.C.	Politique de Certification
P.S.C.E.	Prestataire de Services de Certification Électronique
P.S.C.O.	Prestataire de Services de Confiance
S.S.I.	Sécurité des Systèmes d'Information
URL	*Uniform Resource Locator*

1.6.2 Définitions

Les termes utilisés dans la présente P.C. sont les suivants :

Agent - Personne physique agissant pour le compte d'une autorité administrative.

Autorité d'Enregistrement (A.E.) : Fonction ou entité chargée de la vérification que les demandeurs ou les porteurs de certificat sont identifiés, que leur identité est authentique et que les contraintes liées à l'usage d'un certificat sont remplies conformément à la politique de certification. Ici, l'A.E. vérifie l'identité et l'habilitation de chacun des responsables des A.C. filles.

Autorité de Certification (A.C.) : L'A.C. assure les fonctions suivantes :

- Rédaction des documents de spécifications de l'I.G.C.
- Mise en application de la P.C.
- Gestion des certificats (de leur cycle de vie)
- Choix des dispositifs cryptographiques et gestion des données d'activation
- Publication des certificats valides et des listes de certificats révoqués
- Conseil, information ou formation des acteurs de l'I.G.C.
- Maintenance et évolution de la P.C. et de l'I.G.C.
- Journalisation et archivage des événements et informations relatives au fonctionnement de l'I.G.C., à son niveau ;

Autorité de Certification Racine (ou **A.C. Racine**) **:** désigne l'entité de plus haut niveau dans l'infrastructure à Clé publiques et qui certifie les autorités de certification filles.

Bi clé -Une bi clé est un couple composé d'une clé privée (devant être tenue secrète) et d'une clé publique, nécessaire à la mise en œuvre de techniques cryptologiques basées sur des algorithmes asymétriques.

Certificat électronique - Fichier électronique attestant qu'un bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'A.C. valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et le bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Composante - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'I.G.C. L'entité peut être le P.S.C.E. lui-même ou une entité externe liée au P.S.C.E. par voie contractuelle, réglementaire ou hiérarchique.

Déclaration des pratiques de certification (D.P.C.) - La D.P.C. identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'A.C. ou son opérateur appliquent dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Entité - Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

Identificateur d'objet (OID) - identificateur alphanumérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifique. Dans le cadre de l'I.G.C., les identificateurs OID servent notamment à identifier chacune des politiques, ainsi que les algorithmes de chiffrement acceptés.

Infrastructure à Clés Publiques (**I.G.C.**) **:** désigne un ensemble de moyens organisationnels, techniques (matériels et logiciels), humains, documentaires et contractuels pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques. L'I.G.C. génère, distribue, gère et archive les Certificats. Chacune des composantes de l'I.G.C. est décrite dans la politique de certification définissant le niveau de confiance confié à chacune d'entre elles.

Liste de Certificats Révoqués (LCR) -Liste contenant les identifiants des certificats révoqués ou invalides.

Online Certificate Status Protocol (OSCP) : protocole de l'I.G.C. par lequel un certificat est validé (non-révocation) en ligne. Le protocole fait l'objet de la norme RFC 2560.

Politique de certification (P.C.) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une A.C. se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une

classe d'applications avec des exigences de sécurité communes. Une P.C. peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Prestataire de services de certification électronique (P.S.C.E.) - Un P.S.C.E. se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un P.S.C.E. peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un P.S.C.E. comporte au moins une A.C. mais peut en comporter plusieurs en fonction de son organisation. Les différentes A.C. d'un P.S.C.E. peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (A.C. Racines / A.C. filles). Un P.S.C.E. est identifié dans un certificat dont il a la responsabilité au travers de son A.C. ayant émis ce certificat et qui est elle-même directement identifiée dans le champ issuer du certificat.

Produit de sécurité - Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Support : désigne un support physique contenant la Clé privée et le (ou les) certificat(s) électronique(s) (d'authentification et de signature), protégés à l'aide d'un code PIN, et permettant des opérations cryptographiques.

2 RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIÉES

2.1 Entités chargées de la mise à disposition des informations

L'A.C. met en œuvre une fonction de publication et une fonction d'information sur l'état des certificats sur les informations devant être publiées à destination des porteurs et des utilisateurs de certificats (cf. chapitre 1.3.2 ci-dessus).

Les méthodes de mise à disposition et les URL correspondantes (annuaire accessible par le protocole LDAP et/ou HTTP, serveur Web, serveur OCSP, etc.) sont précisées ci-après.

2.2 Informations devant être publiées

L'A.C. a pour obligation de publier au minimum les informations suivantes à destination des porteurs et utilisateurs de certificats :

- La politique de certification, établie par le P.S.C.E. et couvrant l'ensemble des rubriques du RFC3647
- La liste des certificats révoqués
- Les certificats de l'A.C., en cours de validité
- Le certificat de l'A.C. Racine et son empreinte cryptographique (SHA-256)
- La P.C. et D.P.C de l'A.C. Racine.

Ces documents sont publiés à l'adresse :

`https://pki.damanesign.ma/cps.html`

2.2.1 Publication du certificat d'AC

Le certificat de l'Autorité de Certification est publié aux adresses suivantes :

`http://pki.damanesign.ma/certs/ca_root_2022.crt`

2.2.2 Publication de la CRL

La liste de certificats révoqués (CRL) est publiée sur :

`http://pki.damanesign.ma/crl/ca_root_2022.crl`

Remarque : l'A.C. n'émettant que des certificats d'A.C., il s'agit d'une L.A.R.

2.3 Délais et fréquences de publication

Les informations liées à l'I.G.C. (nouvelle version de la P.C., formulaires, etc.) doivent être publiées 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'A.C. En particulier, toute nouvelle version doit être communiquée au porteur lors d'une demande de renouvellement de clé et doit faire l'objet d'un nouvel accord. Les systèmes publiant ces informations doivent avoir une disponibilité de 24 h sur 24, avec une durée maximale d'interruption d'une heure (et pas plus de quatre heures cumulées par mois).

Les certificats d'A.C. doivent être diffusés préalablement à toute diffusion de certificats de porteurs ou de L.C.R. correspondants et les systèmes les publiant doivent avoir la même disponibilité.

Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux chapitres 4.9 et 4.10.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats doit être libre d'accès en lecture.

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'I.G.C.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Les noms utilisés doivent être conformes aux spécifications de la norme X.500.

Dans chaque certificat conforme à la norme X.509, l'A.C. émettrice (*issuer*) et le porteur (*subject*) sont identifiés par un *Distinguished Name* (DN) de type X.501. Le contenu exact des certificats des A.C. filles est précisé au chapitre 7.

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les A.C. filles doivent être explicites.

Les noms des A.C. filles de l'A.C. Racine sont déterminés par celle-ci.

Les AC filles sont identifiables par leurs DN, comme suit.

3.1.2.1 A.C. Racine

C = MA	Pays
O=Damanesign	Nom déposé de l'organisation
OU=154609	Numéro du registre du commerce
OU=Damanesign trust services	Services de confiance Damanesign
CN=Damanesign Root CA	A.C. racine de l'I.G.C.

3.1.2.2 *A.C. Cachet qualifié*

C = MA	Pays
O=Damanesign	Nom déposé de l'organisation
OI=NTRMA-154609	Numéro du registre du commerce
OU=154609	Numéro du registre du commerce
OU=Damanesign trust services	Services de confiance Damanesign
CN= Damanesign Qualified Seal CA	Nom de l'A.C.

3.1.2.3 *AC qualifiée personnes (signature)*

C = MA	Pays
O=Damanesign	Nom déposé de l'organisation
OI=NTRMA-154609	Numéro du registre du commerce
OU=154609	Numéro du registre du commerce
OU=Damanesign trust services	Services de confiance Damanesign
CN= Damanesign Qualified Signature CA	Nom de l'A.C.

3.1.2.4 *AC personnes standard*

C = MA	Pays
O=Damanesign	Nom déposé de l'organisation
OU=154609	Numéro du registre du commerce
OU=Damanesign trust services	Services de confiance Damanesign
CN= Damanesign User CA	Nom de l'A.C.

3.1.2.5 *AC machines standard*

C = MA	Pays
O=Damanesign	Nom déposé de l'organisation
OU=154609	Numéro du registre du commerce
OU=Damanesign trust services	Services de confiance Damanesign
CN= Damanesign Server CA	Nom de l'A.C.

3.1.2.6 *AC horodatage*

C = MA	Pays
O=Damanesign	Nom déposé de l'organisation
OU=154609	Numéro du registre du commerce
OU=Damanesign trust services	Services de confiance Damanesign
CN= Damanesign Horodatage CA	Nom de l'A.C.

3.1.3 Pseudonymisation des porteurs

Sans objet

3.1.4 Règles d'interprétation des différentes formes de nom

Sans objet.

3.1.5 Unicité des noms

Le DN du champ « subject » de chaque certificat d'A.C. fille doit permettre d'identifier de façon unique celle-ci au sein du domaine de l'A.C.

L'A.C. est garante de l'unicité des noms des A.C. filles.

3.1.6 Identification, authentification et rôle des marques déposées

L'A.C. s'engage quant à l'unicité des noms de ses A.C. filles, conformément au paragraphe précédent, ainsi qu'à résoudre tout litige portant sur la revendication d'utilisation d'un nom.

3.2 Validation initiale de l'identité

Damanesign, agissant en tant qu'A.C., est responsable et en charge de la validation de l'identité de ses A.C. filles.

3.2.1 Méthode pour prouver la possession de la clé privée

La possession de la clé privée est constatée durant la cérémonie des clés.

3.2.2 Validation de l'identité d'un organisme

Sans objet : Les A.C. filles appartiennent à Damanesign.

3.2.3 Validation de l'identité d'un individu

Les représentants des différentes A.C. sont désignés par la direction de Damanesign.

3.2.4 Informations non vérifiées du porteur

Sans objet.

3.2.5 Validation de l'autorité du demandeur

Les demandeurs sont habilités par la direction de Damanesign.

3.2.6 Certification croisée d'A.C.

Pas d'exigences en l'état actuel de la P.C.

3.3 Identification et validation d'une demande de renouvellement des clés

Les bi-clés et les certificats d'AC fille sont renouvelés a minima trois ans avant l'expiration du certificat de l'AC Fille. Le renouvellement est réalisé dans le cadre d'une cérémonie des clés.

3.3.1 Identification et validation pour un renouvellement courant

Sans objet.

3.3.2 Identification et validation pour un renouvellement après révocation

Sans objet.

3.4 Identification et validation d'une demande de révocation

La révocation est effectuée par l'autorité d'enregistrement, qui valide ainsi la demande.

La demande de révocation de clé pour une A.C. fille, ne peut émaner que du responsable de celle-ci et est validée lors d'un face à face avec l'autorité d'enregistrement.

4 EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

Les demandes de certificat sont déposées et traitées dans le cadre d'une cérémonie de clés.

4.2 Traitement d'une demande de certificat

4.2.1 Exécution des processus d'identification et de validation de la demande

L'identification et la validation des demandes sont décrits dans le script de cérémonie des clés.

4.2.2 Acceptation ou rejet de la demande

Toutes les demandes sont acceptées lors de la cérémonie de clés, un refus ne pouvant se produire qu'en cas d'un incident durant celle-ci. L'incident sera alors consigné dans le procès-verbal de la cérémonie.

4.2.3 Durée d'établissement du certificat

Sauf incident, le certificat est établi à la fin de la cérémonie des clés.

4.3 Délivrance du certificat

4.3.1 Actions de l'A.C. concernant la délivrance du certificat

Se référer au script de la cérémonie des clés.

4.3.2 Notification de la délivrance du certificat au porteur (responsable d'une A.C. fille)

La remise du certificat doit se faire en mains propres (face-à-face).
Le certificat complet et exact doit être mis à la disposition de son porteur.

4.4 Acceptation du certificat

L'acceptation du certificat est formellement consignée dans le procès-verbal de la cérémonie des clés.

4.4.1 Publication du certificat

Les certificats d'A.C. filles sont publiés sur le site Internet indiqué en 2.2, à une adresse indiquée dans leurs politiques de certification respectives.

4.4.2 Notification aux autres entités de la délivrance du certificat

Sans objet.

4.5 Usages de la bi-clé et du certificat

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

Pour les A.C. filles, l'utilisation des clés privées est limitée :

- À la signature des certificats
- À la signature des CRL.
- À l'émission de certificat de répondeur OCSP, le cas échéant.

Cet usage est indiqué explicitement dans les extensions des certificats.

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

Les utilisateurs de ces certificats pourront vérifier la révocation ou l'expiration des certificats d'A.C. en analysant le contenu de ces certificats et la liste de révocation mise à disposition par la présente Autorité de Certification.

4.6 Renouvellement d'un certificat

Dans la cadre de la présente P.C., il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. Comme l'A.C. génère les bi-clés des porteurs, elle garantit qu'un certificat correspondant à une bi-clé existante ne peut pas être renouvelé au sens du RFC3647.

Tout renouvellement s'effectue dans les mêmes conditions et selon les mêmes modalités que la demande initiale.

4.7 Délivrance d'un nouveau certificat à la suite du changement de la bi-clé

Les bi-clés émises pour les certificats d'A.C. filles ont une durée de vie inférieure à 30 ans.

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

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont semblables aux opérations initiales.

4.8 Modification du certificat

La modification du certificat n'est pas admise.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificats de porteurs (A.C. fille)

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

- Compromission, suspicion de compromission, perte ou vol de clé privée
- Cessation de l'activité de l'A.C. fille concernée
- Décision à la suite d'un échec de contrôle de conformité
- Révocation de l'A.C. Racine
- Rupture technologique, nécessitant de procéder à la génération de nouveaux bi-clés (longueurs des clés trop faibles, algorithmes de hachage compromis).

4.9.1.2 Certificats d'une composante de l'I.G.C.

Les circonstances suivantes déclenchent la révocation du certificat d'une composante de l'I.G.C. :

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

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats de porteurs (A.C. fille)

Les personnes pouvant demander une révocation de certificat d'A.C. fille sont :

- Les responsables de ces A.C.
- Les représentants légaux de ces A.C.
- La direction de Damanesign, agissant en tant qu'A.C. Racine

4.9.2.2 *Certificats d'une composante de l'I.G.C.*

La révocation du certificat de l'A.C. est mise à décision du comité de pilotage de l'A.C. et est prononcée par le responsable de l'A.C.

La révocation des certificats des autres composantes est validée par le comité de pilotage de l'A.C. et opérée par l'entité responsable de la composante.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 *Révocation d'un certificat d'A.C. fille*

Une fois la demande authentifiée et contrôlée, l'A.C. révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la publication sur l'état des certificats. L'information de révocation doit être diffusée au minimum via une L.C.R. signée par l'A.C. D'autres moyens de diffusion complémentaires peuvent également être utilisés par l'A.C.

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

4.9.3.2 *Révocation d'un certificat d'une composante de l'I.G.C.*

La révocation du certificat de l'A.C. Racine nécessite la réunion des porteurs de secrets pour procéder aux étapes de :

- Révocation du certificat d'A.C. et de l'ensemble des certificats d'A.C. filles
- Signature d'une nouvelle L.A.R.

L'ensemble des populations concernées par la révocation du certificat de l'A.C. Racine sera alors informé, soit directement, soit par une information sur le site institutionnel de l'A.C.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

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

4.9.5 Délais de traitement par l'A.C. d'une demande de révocation

4.9.5.1 *Révocation d'un certificat de porteur (A.C. fille)*

Toute demande de révocation est traitée en urgence.

Il s'écoule au maximum 2 jours ouvrés entre la demande de révocation par le responsable de l'A.C. et la publication de la nouvelle L.A.R. prenant en compte cette demande.

4.9.5.2 *Révocation d'un certificat d'une composante de l'I.G.C.*

La révocation du certificat de l'A.C. Racine est effectuée immédiatement après la validation de cette procédure par le comité de pilotage et suite à la détection d'une des causes de révocation.

4.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat de porteur est tenu de vérifier (via l'OCSP), avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.

La L.A.R. est mise à jour annuellement et publiée via HTTP. Les L.A.R. sont pré-générées et publiées au fur et à mesure, sauf en cas de révocation.

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

Les systèmes de révocation et de vérification ont un taux de disponibilité de 99,5 pour cent, et respectent une durée maximum d'indisponibilité de 4 heures.

4.9.8 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

L'utilisateur d'un certificat de porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. Cf. chapitre 4.9.6 ci-dessus.

4.9.9 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.10 Exigences spécifiques en cas de compromission de la clé privée

La compromission de la clé privée d'un certificat d'A.C. fera l'objet d'une information claire sur le site de publication de l'A.C.

4.9.11 Suspension de certificats

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

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de L.A.R. Ces L.A.R. sont des L.C.R. au format V2.

La L.A.R. est accessible à l'adresse indiquée en 2.2.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24 heures sur 24 et 7 jours sur 7.

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 2 heures et une durée maximale totale d'indisponibilité par mois de 8 heures.

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'A.C. et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

4.10.3 Séquestre de clé et recouvrement

Il n'est procédé à aucun séquestre ni recouvrement des clés privées des porteurs.

Il n'est procédé à aucun séquestre ni recouvrement des clés d'A.C. (fille ou racine).

5 MESURES DE SÉCURITÉ NON TECHNIQUES

5.1 Mesures de sécurité physique

Les exigences définies dans la suite du présent chapitre sont les exigences déclinées en mesures de sécurité en fonction de l'environnement réel de l'I.G.C. C'est pourquoi elles sont précisées dans les points suivants :

- Accès physique
- Alimentation électrique et climatisation
- Vulnérabilité aux dégâts des eaux
- Conservation des supports
- Mise hors service des supports
- Sauvegardes hors site

5.1.1 Accès physique

L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilitédes accès doit être assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

L'accès aux machines (serveurs, boîtiers cryptographiques, poste d'administration de l'AC, élémentsactifs du réseau) est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines (contrôle d'accès par biométrie, droits associés).

5.1.2 Alimentation électrique et climatisation

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

Elles permettent également de respecter les exigences des PC et les engagements de l'AC en matièrede disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.3 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences et engagement de l'AC dans la présente PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.4 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences et engagement de l'AC dans la présente PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.5 Conservation des supports

Les supports (papier, disque dur, disquette, CD, etc.) correspondant aux informations relatives à l'activité de l'IGC (fonctions d'exploitation, de sauvegarde, etc.) sont traités et conservés dans une enceinte sécurisée accessibles aux seules personnes autorisées.

5.1.6 Mise hors service des supports

Les supports papiers et magnétiques en fin de vie sont systématiquement détruits par des moyens appropriés, permettant d'éviter toute perte de confidentialité. Les dossiers d'enregistrement devront êtreconservés au moins pendant la durée de validité du certificat d'entité (en cas de renouvellement, la durée sera prolongée)

5.1.7 Sauvegardes hors site

Les sauvegardes sont stockées sur les différents sites de production de l'hébergeur de l'IGC : en localsur le site primaire et à distance via des mécanismes de synchronisation automatique.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

L'A.C. distingue au moins les cinq rôles fonctionnels de confiance suivants :

Responsable de sécurité : Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé

de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est responsable des opérations de génération et de révocation des certificats.

Responsable d'application : Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'I.G.C. au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.

Ingénieur système : Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.

Opérateur : Un opérateur au sein d'une composante de l'I.G.C. réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.

Contrôleur : Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'I.G.C. et aux politiques de sécurité de la composante.

Un même rôle fonctionnel peut être tenu par différentes personnes.

De manière générale, des procédures doivent être établies et appliquées pour tous les rôles administratifs et les rôles de confiance ayant trait à la fourniture de services de certification. Ces rôles doivent être décrits et définis dans la description des postes propre à chaque entité opérant une des composantes de l'I.G.C. sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles doivent déterminer la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilisation des employés.

Lorsqu'appropriées, ces descriptions doivent différencier entre les fonctions générales et les fonctions spécifiques à l'A.C. L'A.C. doit implémenter techniquement ce principe de moindre privilège via les mécanismes de contrôle d'accès qu'elle met en œuvre.

5.2.2 Nombre de personnes requises par tâches

Le nombre de personnes requises par tâches selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents

5.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'I.G.C. doit faire vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment que :

- Son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- Son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- Le cas échéant et en fonction du rôle, un compte soit ouvert à son nom dans ces systèmes ;
- Éventuellement, des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'I.G.C.

5.2.4 Rôles exigeant une séparation des attributions

Les cumuls suivants sont interdits :

- Responsable de sécurité et ingénieur système / opérateur
- Contrôleur et tout autre rôle
- Ingénieur système et opérateur

5.3 Mesures de sécurité vis à vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Tout intervenant amené à occuper un rôle identifié comme sensible est soumis à une clause de confidentialité.

Les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles.

Le personnel d'encadrement possède l'expertise appropriée, et est familier des procédures de sécurité.

Toute personne intervenant dans des rôles de confiance est informée de ses responsabilités (description de poste), et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2 Procédures de vérification des antécédents

Des procédures de vérification des antécédents sont mises en place pour les personnes appelées à occuper un rôle sensible. L'AC demande en particulier la production d'une copie du casier judiciaire.

Ces vérifications sont effectuées préalablement à l'affectation à un rôle de confiance et revues au minimum tous les 3 ans.

5.3.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures de fonctionnement de l'Autorité de Certification, préalablement à la prise de fonction effective.

5.3.4 Exigences en matière de formation continue et fréquences des formations

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte le mode de travail de ces intervenants.

Les intervenants sont formés à la gestion des incidents et sont au fait de l'organisation de remontée d'incidents.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont énoncées dans la définition de poste ou la charte de sécurité du personnel (charte d'utilisation des ressources informatiques, numériques et technologiques) pour les rôles sensibles tenus par le personnel de l'AC.

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

Les exigences vis-à-vis des prestataires externes sont contractualisées.

5.3.8 Documentation fournie au personnel

Les règles de sécurité sont communiquées au personnel lors de leur prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel dans l'infrastructure de gestion de clés disposent des procédures correspondantes.

5.4 Procédures de constitution des données d'audit

5.4.1 Type d'événement à enregistrer

Les événements suivants sont enregistrés :

- Événements systèmes des différentes composantes de l'I.G.C. (démarrage des serveurs, accès réseau, …)
- Événements techniques des applications composant l'I.G.C.
- Événements fonctionnels des applications composant l'I.G.C. (demande de certificats, validation, révocation, rejet…)
- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.)
- Accès physiques aux locaux
- Publication et mise à jour des informations liées à l'A.C.
- Génération puis publication des L.C.R.
- Actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs...)
- Changements apportés au personnel.

Ces journaux permettent d'assurer la traçabilité et l'imputabilité des actions effectuées.

5.4.2 Fréquence de traitement des journaux d'événements

Les journaux d'événements sont exploités de manière quotidienne, et systématiquement en cas de remontée d'événement anormal.

5.4.3 Période de conservation des journaux d'événements

Le délai de conservation des journaux d'événements sur site est de 1 mois. L'archivage des journaux d'événements est effectué au plus tard 1 mois après leur génération.

5.4.4 Protection des journaux d'événements

Les journaux d'événements sont accessibles uniquement au personnel autorisé de l'AC. Ils ne sont pas modifiables. Des alarmes sont remontées en cas de modification des journaux, ou des paramètres définissant le contenu des journaux.

5.4.5 Procédure de sauvegarde des journaux d'événements

Les procédures de sauvegarde des journaux sont quotidiennes par delta avec la sauvegarde précédente, et globale de manière hebdomadaire. Ces journaux sont ensuite archivés par l'AC.

5.4.6 Système de collecte des journaux d'événements

Un système automatique de collecte des journaux d'événements est mis en place.

5.4.7 Notification de l'enregistrement d'un événement au responsable de l'événement

Sans objet.

5.4.8 Évaluation des vulnérabilités

Le contrôle des journaux d'événement système et technique est continu et quotidien afin de permettre une anticipation des vulnérabilités, et des remontées d'alerte en cas de vulnérabilités.

Le contrôle des journaux des événements fonctionnels est réalisé à la demande en cas de litige, ou pour analyse de comportement de l'Autorité de Certification.

5.5 Archivage des données

5.5.1 Types de données à archiver

Des dispositions en matière d'archivage sont prises par l'A.C. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'I.G.C.

Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- La P.C.
- La D.P.C.
- Les certificats et L.C.R. tels qu'émis ou publiés
- Les récépissés ou notifications (à titre informatif)
- Les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement, les journaux d'événements des différentes entités de l'I.G.C. : ces éléments se retrouvent dans les scripts et P.-V. de cérémonie de clés.

5.5.2 Période de conservation des archives

5.5.2.1 Dossiers de demande de certificat

Tout dossier de demande de certificat accepté doit être archivé aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi marocaine.

En ce qui concerne les certificats de l'AC, les dossiers d'enregistrement (demandes de certificats) sont archivés pendant cinq ans après l'expiration du certificat associé.

Les certificats de clés de porteurs et d'A.C., ainsi que les L.C.R. produites, doivent être archivés pendant au moins cinq ans après leur expiration.

5.5.2.2 Journaux d'événements et autres

La durée d'archivage des journaux d'événements et autres est de cinq ans après l'événement.

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, doivent :

- Être protégées en intégrité
- Être accessibles aux personnes autorisées
- Pouvoir être relues et exploitées

La Politique de sauvegarde expose les moyens mis en œuvre pour archiver les pièces en toute sécurité.

5.5.4 Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes, qui est équivalent au niveau de protection des archives, est précisé dans la Politique de sauvegarde.

5.5.5 Exigences d'horodatage des données

Le chapitre 6.8 précise les exigences en matière de datation et d'horodatage.

5.5.6 Système de collecte des archives

La Politique de sauvegarde décrit le système de collecte des archives, interne ou externe, qui doit respecter les exigences de protection des archives concernées.

5.6 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai inférieur à deux jours ouvrés sachant que seule l'A.C. peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'I.G.C. qui ne peut récupérer et consulter que les archives de la composante considérée).

L'A.C. ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'A.C. Pour cela la période de validité de ce certificat de l'A.C. doit être supérieure à celle des certificats qu'elle signe. Au regard de la date de fin de validité de ce 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'A.C. est générée, seule la nouvelle clé privée doit être utilisée pour signer des certificats. Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce au moins jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7 Reprise suite à compromission et sinistre

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

Chaque entité opérant une composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents. Les équipes d'exploitation mettent en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. L'AC

prévient également directement et sans délai l'organe de contrôle (DGSSI), et la CNDP, en cas d'événement concernant des données personnelles.

5.7.2 Procédures de reprise en cas de sinistre

Chaque composante dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions. La sauvegarde des composants l'IGC permet d'assurer une reprise d'activité en cas de sinistre sous 24 heures.

Ces plans sont testés au minimum une fois par an.

5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité de la composante (cf. § 5.7.2 > Procédures de reprise en cas de sinistre).

Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences du présent document (cf. § 5.7.2 > Procédures de reprise en cas de sinistre).

5.8 Fin de vie de l'I.G.C.

5.8.1 Transfert d'activité ou cessation d'activité

Une ou plusieurs Composantes de l'I.G.C. peuvent être amenées à cesser leur activité ou à les transférer à une autre entité.

Le transfert d'activité ne comporte pas d'incidence sur la validité des Certificats émis antérieurement au transfert considéré, et la reprise de cette activité est organisée par l'A.C. en collaboration avec la nouvelle entité.

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'A.C. prend les mesures suivantes :

- Elle assure la continuité du service d'archivage
- Elle assure la continuité du service de Révocation
- Elle prévient les Mandataires de Certification dans le cas où les changements envisagés peuvent avoir des répercussions sur les engagements pris.
- Communiquer au point de contact identifié au sein de la DGSSI les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité.
- Tenir informée la DGSSI de tout obstacle ou délai non prévu rencontrés dans le déroulement du processus.

La cessation d'activité affecte l'activité de l'A.C., telle que définie ci-dessous.

5.8.2 Cessation d'activité affectant l'activité de l'A.C.

La cessation d'activité comporte une incidence sur la validité des Certificats émis antérieurement à la cessation concernée, et une procédure spécifique est mise en œuvre dans ce cas.

En cas de cessation d'activité, l'A.C. s'engage à respecter les principes suivants :

- La clé privée d'émission des certificats ne sera transmise en aucun cas

- Toutes les mesures nécessaires seront prises pour la détruire ou la rendre inopérante
- Le certificat d'A.C. sera révoqué
- Tous les certificats émis encore en cours de validité seront révoqués
- Tous les mandataires de certification, responsables des certificats révoqués ou à révoquer seront tenus informés.
- Informer (par exemple par récépissé) tous ses clients et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant ;
- Informer l'organisme de contrôle (DGSSI) de cette décision

Les représentants du comité de pilotage de l'A.C. devront se réunir pour réaliser les opérations sensibles de désactivation des clés d'A.C., et de révocation des certificats préalablement émis.

5.8.3 Transfert des Archives

Dans le cas d'une fin de vie d'une AE, les modalités de transfert des archives. Celles-ci pourront :

- Soit être conservées pour la durée légale par l'organisme opérant l'AE.
- Soit être transférée à l'AC par une méthode sécurisée permettant de garantir l'intégrité et la confidentialité des archives transférées.

En cas d'arrêt d'activité du service, Damanesign se réserve au moment voulu le choix d'effectuer le transfert des archives

- Soit en interne au sein d'un autre service opérant un service d'archivage
- Soit via un tiers archiveur

5.8.4 Cas du transfert d'Activité

Dans le cas du transfert d'activité, la société reprenant l'activité de l'AC devra reprendre les archives, soit en gestion directe, soit par l'intermédiaire d'un prestataire.

5.8.5 Cas de la cessation d'activité

Si l'AC arrête son activité, elle devra transférer ses archives à un prestataire agréé dans ce domaine et informer l'AC ainsi que l'organe de contrôle national (DGSSI) des coordonnées de cette société.

6 MESURES DE SÉCURITÉ TECHNIQUES

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'A.C. doit respecter. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'I.G.C., notamment par des dispositions spécifiques de la D.P.C.

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés de l'A.C.

Les clés de l'A.C. Racine et des A.C. filles sont générées lors de la cérémonie des clés, en présence du comité de pilotage, et suivant la procédure du maître de cérémonie.

Cette séance de cérémonie des clés a lieu sous le contrôle d'un officier public ministériel, veillant à la bonne application des procédures et au respect des exigences de sécurité définies dans ce document.

6.1.1.2 *Clés porteurs générées par l'A.C.*

Sans objet.

6.1.1.3 *Clés porteurs générées par le porteur*

Sans objet.

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet.

6.1.3 Transmission de la clé publique à l'A.C.

Sans objet

6.1.4 Transmission de la clé publique de l'A.C. aux utilisateurs de certificats

Le certificat de l'A.C. racine et des A.C. filles sont téléchargeables sur le site Internet mentionné en 2.2.

6.1.5 Tailles des clés

La clé RSA de l'A.C. Racine a une taille de 4096 bits.
Les clés RSA des A.C. filles ont une taille de 4096 bits.

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

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé. Les paramètres et les algorithmes de signature sont documentés dans le présent document, chapitre 7.

6.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée d'A.C. et du certificat associé est strictement limitée à la signature de certificats et de L.C.R. / L.A.R. (voir chapitre 1.4.1).

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 *Modules cryptographiques de l'A.C.*

L'A.C. s'assure que :

- La préparation des modules cryptographiques est contrôlée de façon sécurisée par le prestataire de service
- Le module cryptographique de signature de certificat et des informations de révocation ne fait pas l'objet de manipulation non autorisée lors de son transport ou lors de son stockage

6.2.1.2 *Dispositifs de création de signature des porteurs*

Sans objet.

6.2.2 Contrôle de la clé privée de l'A.C. par plusieurs personnes

Ces questions sont traitées dans d'autres documents de spécifications de l'I.G.C.

6.2.3 Séquestre de la clé privée

Les clés privées des porteurs ne doivent en aucun cas être séquestrées.

6.2.4 Copie de secours de la clé privée

La clé privée de l'A.C. Racine et des clés privées des A.C. filles font l'objet de copie de secours. Ces copies de secours bénéficient du même niveau de sécurité que la clé privée originale.

6.2.5 Archivage de la clé privée

Les clés privées des A.C. ne doivent en aucun cas être archivées, ni par l'A.C., ni par aucune des composantes de l'I.G.C.

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

Pour les clés privées d'A.C., tout transfert doit se faire sous forme chiffrée, conformément aux exigences du chapitre 6.2.4.

6.2.7 Stockage de la clé privée dans un module cryptographique

Voir ci-après.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'A.C.

L'activation des clés privées d'A.C. dans un module cryptographique doit être contrôlée via des données d'activation (cf. chapitre 6.4) et doit faire intervenir au moins trois personnes dans des rôles de confiance.

6.2.8.2 Clés privées des A.C. filles

L'activation des clés privées d'A.C. dans un module cryptographique doit être contrôlée via des données d'activation (cf. chapitre 6.4) et doit faire intervenir au moins trois personnes dans des rôles de confiance.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'A.C.

La désactivation des clés privées d'A.C. dans un module cryptographique doit être automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc. Une clé privée d'A.C. peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation doivent permettre de répondre aux exigences définies dans le chapitre 10.

6.2.9.2 Clés privées des A.C. filles

La désactivation des clés privées d'A.C. dans un module cryptographique doit être automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc. Une clé privée d'A.C. peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation doivent permettre de répondre aux exigences définies dans le chapitre 10.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées d'A.C.

La méthode de destruction des clés privées d'A.C. doit permettre de répondre aux exigences définies dans le chapitre 10. En fin de vie d'une clé privée d'A.C., normale ou anticipée (révocation), cette clé doit être systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.10.2 Clés privées des A.C filles

La méthode de destruction des clés privées d'A.C. doit permettre de répondre aux exigences définies dans le chapitre 10. En fin de vie d'une clé privée d'A.C., normale ou anticipée (révocation), cette clé doit être systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.10.3 Niveau de qualification du module cryptographique et des dispositifs de création de signature

Ces exigences sont précisées au chapitre 10.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

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

6.3.2 Durées de vie des bi-clés et des certificats

La fin de validité d'un certificat d'A.C. doit être postérieure à la fin de vie des certificats des A.C. filles qu'elle émet.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

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

La génération et l'installation des données d'activation d'un module cryptographique de l'I.G.C. doivent se faire lors de la phase d'initialisation et de personnalisation de ce module. Si les données d'activation ne sont pas choisies et saisies par les responsables de ces données eux-mêmes, elles doivent leur être transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne doivent être connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués.

6.4.1.2 Génération et installation des données d'activation correspondant à la clé privée d'une A.C. fille

La génération et l'installation des données d'activation d'un module cryptographique de l'I.G.C. doivent se faire lors de la phase d'initialisation et de personnalisation de ce module. Si les données d'activation ne sont pas choisies et saisies par les responsables de ces données eux-mêmes, elles doivent leur être transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne doivent être connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués.

6.4.2 Protection des données d'activation

Les données d'activation sont sous la responsabilité des porteurs de secret.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Les objectifs de sécurité des systèmes informatiques utilisés par l'A.C. sont les suivants :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique ou logique)
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur)
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès
- 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 y transitent
- Fonctions d'audits (non-répudiation et nature des actions effectuées)
- Gestion des reprises sur erreur

La protection en confidentialité et en intégrité des clés privées et secrètes fait l'objet de mesures particulières découlant de l'analyse de risque de DAMANESIGN.

Les procédures de sécurité des systèmes informatiques est décrite dans la documentation interne de l'IGC

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Sans objet

6.6 Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes des services de confiance est documentée et respecte dans la mesure du possible des normes de modélisation et d'implémentation.

La configuration du système des composantes, ainsi que toute modification et mise à niveau, est documentée et contrôlée.

6.7 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics doit être protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'I.G.C.

L'A.C. s'assure que les composants du réseau local sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'A.C.

De plus, les échanges entre composantes au sein de l'I.G.C. peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

6.8 Horodatage / Système de datation

Plusieurs exigences de la présente P.C. nécessitent la datation par les différentes composantes de l'I.G.C. d'événements liés aux activités de l'I.G.C. (cf. chapitre 5.4).

Pour dater ces événements, les différentes composantes sont synchronisées quotidiennement, au minimum, à la minute près, et par rapport à une source fiable de temps UTC.

7 Profils des certificats et des L.C.R.

7.1 Certificat de l'A.C. Racine

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	`sha256WithRSAEncryption`
Issuer	Voir 3.1.2.1
Validity	30 ans
Subject	Voir 3.1.2.1 (certificat auto-signé)
Subject Public Key Info	RSA 4096 bits

Champ	Criticité	Général
Authority Key Identifier	N	Contient l'identifiant de clé de la clé publique de l'AC émettrice (champ *Subject Key Identifier* du certificat de l'AC émettrice). Méthode 1 définie dans la RFC 5280, § 4.2.1.2.
Subject Key Identifier	N	Identifiant de la clé du sujet (AC) Méthode 1 définie dans la RFC 5280, § 4.2.1.2.
Key Usage	O	`keyCertSign, CRLSign`
Basic Constraints	O	`CA:TRUE`
Certificate Policies	N	`anyPolicy` (2.5.29.32.0)
CRL Distribution Points	N	`http://pki.damanesign.ma/crl/ca_root_2022.crl`
Authority Information Access	N	`CA:` `http://pki.damanesign.ma/certs/ca_root_2022.crt`

7.2 Certificats filles

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	`sha256WithRSAEncryption`
Issuer	Voir 3.1.2.1
Validity	30 ans
Subject	Voir 3.1.2
Subject Public Key Info	RSA 4096 bits

Champ	Criticité	Général
Authority Key Identifier	N	Contient l'identifiant de clé de la clé publique de l'AC émettrice (champ *Subject Key Identifier* du certificat de l'AC émettrice). Méthode 1 définie dans la RFC 5280, § 4.2.1.2.
Subject Key Identifier	N	Identifiant de la clé du sujet (AC) Méthode 1 définie dans la RFC 5280, § 4.2.1.2.
Key Usage	O	`keyCertSign, CRLSign`
Basic Constraints	O	`CA:TRUE` `pathlen :0`
Certificate Policies	N	`anyPolicy` (2.5.29.32.0)
Subject Alternative Name ***Issuer Alternative Name***	N	Non utilisée
CRL Distribution Points	N	`http://pki.damanesign.ma/crl/ca_root_2022.crl`
Authority Information Access	N	`CA:`

Champ	Criticité	Général
		http://pki.damanesign.ma/certs/ca_root_2022.crt

7.3 Liste de Certificats Révoqués

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Signature	sha256WithRSAEncryption
Issuer	Voir 3.1.2.1
thisUpdate	Date et heure UTC
nextUpdate	Date et heure UTC (1 an de validité)
RevokedCertificates	Liste des numéros de série des certificats révoqués (couples *UserCertificate-RevocationDate*)
Numéro de LCR	Entier
AuthorityKeyIdentifier	Identifiant de la clé de l'A.C.

8 Audits de conformité et évaluations

Les audits et les évaluations concernent,

- Ceux que doit réaliser, ou faire réaliser, le P.S.C.E. afin de s'assurer que l'ensemble de son I.G.C. est bien conforme à ses engagements affichés dans sa P.C. et aux pratiques identifiées dans sa D.P.C.

La suite du présent chapitre ne concerne donc que les audits et évaluation de la responsabilité de l'A.C. afin de s'assurer du bon fonctionnement de son I.G.C.

8.1 Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de son I.G.C. ou à la suite de toute modification significative au sein d'une composante, le P.S.C.E. doit procéder à un contrôle de conformité de cette composante. L'A.C. doit également procéder régulièrement à un contrôle de conformité de l'ensemble de son I.G.C., une fois par an.

8.2 Identités / qualifications des évaluateurs

Le contrôle d'une composante doit être assigné à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'I.G.C. contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'I.G.C. (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'I.G.C. (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la P.C. de l'A.C. et dans la D.P.C. qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5 Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend au P.S.C.E., 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'A.C. 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'A.C. et doit respecter ses politiques de sécurité internes.
- En cas de résultat « à confirmer », l'A.C. 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'A.C. confirme à la composante contrôlée la conformité aux exigences de la P.C. et la D.P.C.

8.6 Communication des résultats

Les résultats des audits de conformité doivent être tenus à la disposition de l'organisme de qualification en charge de la qualification de l'A.C.

9 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

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

9.1.2 Tarifs pour accéder aux certificats

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

9.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats

L'accès aux L.C.R. doit être en accès libre en lecture.

9.1.4 Tarifs pour d'autres services

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

9.1.5 Politique de remboursement

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

9.2 Responsabilité financière

Sans objet, les A.C. filles appartiennent à la même entité que l'A.C. racine.

9.3 Confidentialité des données

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :

- La partie non-publique de la D.P.C. de l'A.C.,
- Les clés privées de l'A.C., des composantes et des porteurs de certificats,
- Les données d'activation associées aux clés privées d'A.C. et des porteurs,

- Tous les secrets de l'I.G.C.,
- Les journaux d'événements des composantes de l'I.G.C.,
- Les dossiers d'enregistrement des porteurs,
- Les causes de révocations, sauf accord explicite du porteur ou la cause de perte du statut de membre de l'ordre.

9.3.2 Informations hors du périmètre des informations confidentielles

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

9.3.3 Responsabilités en termes de protection des informations confidentielles

L'A.C. applique des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, l'A.C. en garantit l'intégrité.

L'A.C. respecte la législation et la réglementation en vigueur sur le territoire marocain. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des porteurs à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations au porteur.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

Toute collecte et tout usage de données à caractère personnel par l'A.C. et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire marocain.

Toute collecte de données à caractère personnel dans le cadre de l'activité de l'I.G.C. Damanesign est réalisée dans le strict respect de la loi N° 09-08.

Peuvent seuls, dans les limites de leurs attributions respectives, être destinataires des données collectées précitées : le personnel chargé de la fourniture du service, l'autorité nationale d'agrément et de surveillance de la certification électronique, les dispositifs de contrôle interne et externe, les donneurs d'ordres pour lesquels le bénéficiaire utilisera son certificat pour exploiter leurs services dématérialisés en cas de besoin et toutes les autorités habilitées conformément à la réglementation en vigueur.

Conformément à la loi n° 09-08, vous pouvez accéder aux données à caractère personnel vous concernant, les rectifier ou vous opposer au traitement de vos données à caractère personnel pour des motifs légitimes, par courrier avec accusé de réception à l'adresse postale de l'A.C. fournie en 1.5.2.

9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- Les causes de révocation des certificats des porteurs
- Le dossier d'enregistrement du porteur.

9.4.3 Informations à caractère non personnel

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

9.4.4 Responsabilité en termes de protection des données personnelles

Application de la législation et de la réglementation en vigueur sur le territoire marocain.

9.4.5 Notification et consentement d'utilisation des données personnelles

Conformément à la législation et réglementation en vigueur sur le territoire marocain, les informations personnelles remises par les porteurs à l'A.C. ne doivent ni être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

Cf. législation et réglementation en vigueur sur le territoire marocain.

9.4.7 Autres circonstances de divulgation d'informations personnelles

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

9.5 Droits sur la propriété intellectuelle et industrielle

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

9.6 Interprétations contractuelles et garanties

Sans objet.

9.7 Limite de garantie

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

9.8 Limite de responsabilité

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

9.9 Indemnités

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

9.10 Durée et fin anticipée de validité de la P.C.

9.10.1 Durée de validité

La P.C. de l'A.C. doit rester en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette P.C.

9.10.2 Fin anticipée de validité

Sans objet

9.10.3 Effets de la fin de validité et clauses restant applicables

La présente P.C. 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'I.G.C., l'A.C. 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'A.C. 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 à la P.C.

Les amendements à la P.C. ne peuvent être apportés que par l'A.C.

L'OID de la P.C. de l'A.C. étant inscrit dans les certificats qu'elle émet, toute évolution de cette P.C. ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) donnera lieu à une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

En particulier, l'OID de la présente P.C. évoluera dès lors qu'un changement majeur intervient dans les exigences de la P.C. Type applicable à la famille de certificats considérée.

9.13 Dispositions concernant la résolution de conflits

Le P.S.C.E. doit mettre en place des politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles il fournit des services électroniques de confiance ou d'autres points qui y sont liés.

9.14 Juridictions compétentes

Application de la législation et de la réglementation en vigueur sur le territoire marocain.

9.15 Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente P.C. sont, notamment, ceux indiqués au chapitre 10 ci-dessous.

9.16 Transfert d'activités

Cf. section 5.8.

10 Annexe 2 : Exigences de sécurité du module cryptographique de l'A.C.

Dans la mesure où les certificats émis par la présente A.C. sont des certificats d'A.C. filles, les exigences de ce chapitre s'appliquent indifféremment à l'A.C. Racine et aux A.C. filles.

10.1 Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'A.C. pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des L.C.R. / L.A.R. et, éventuellement, des réponses OCSP), ainsi que, le cas échéant, générer les bi-clés des porteurs, doit répondre aux exigences de sécurité suivantes :

- Si les bi-clés de signature des porteurs sont générées par ce module, garantir que ces générations sont réalisées exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées
- Si les bi-clés de signature des porteurs sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques des porteurs lorsqu'elles sont sous la responsabilité de l'A.C. et pendant leur transfert vers le dispositif de création de signature du porteur et assurer leur destruction sûre après ce transfert
- Assurer la confidentialité et l'intégrité des clés privées de signature de l'A.C. durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie
- Être capable d'identifier et d'authentifier ses utilisateurs
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné
- Être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur

- Permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'A.C., qui ne révèle pas les clés privées de l'A.C. et qui ne peut pas être falsifiée sans la connaissance de ces clés privées
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité
- Si une fonction de sauvegarde et de restauration des clés privées de l'A.C. est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.