



Politique de certification – Signature avancée

Version 1.0 | Diffusion : public

OID n° 1.3.6.1.4.1.58553.1.7.1.3

Ce document est la propriété exclusive de Damanesign

Historique du document

Version	Date de version	Rédacteur(s)	Approbateur(s)	Modifications
1.0	18/07/2023	Fatimazahrae Jalal	Zouhair Hamdaoui	Création du document

Table des matières

1	Introduction.....	8
1.1	Présentation générale.....	8
1.2	Identification du document	8
1.3	Entités intervenant dans l'I.G.C. et responsabilités.....	9
1.3.1	Le Prestataire de services de certification électronique	9
1.3.2	Autorité de certification	9
1.3.3	Utilisateurs de certificat :.....	9
1.3.4	Autorité d'enregistrement	10
1.3.5	Porteurs de certificats	11
1.4	Usage des certificats	11
1.4.1	Domaines d'utilisation applicables	11
1.4.2	Bi-clés et certificats des porteurs.....	11
1.4.3	Bi-clés et certificats d'A.C.	11
1.5	Domaines d'utilisation interdits	11
1.6	Gestion de la Politique de certification	12
1.6.1	Entité gérant la P.C.	12
1.6.2	Point de contact.....	12
1.6.3	Procédures d'approbation de la conformité de la D.P.C/P.C.....	12
1.7	Définitions et sigles	12
1.7.1	Sigles.....	12
1.7.2	Définitions	12
2	RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIÉES	14
2.1	Entités chargées de la mise à disposition des informations	14
2.2	Informations devant être publiées.....	14
2.2.1	Publication du certificat d'AC	14
2.2.2	Publication de la CRL	15
2.3	Délais et fréquences de publication.....	15
2.4	Contrôle d'accès aux informations publiées	15
3	IDENTIFICATION ET AUTHENTIFICATION	15
	Nommage	15
3.1.1	Types de noms	15
3.1.2	Nécessité d'utilisation de noms explicites.....	15
3.1.3	Anonymisation ou pseudonymisation des Porteurs	16
3.1.4	Certificats de test	16
3.1.5	Unicité des noms.....	16
3.1.6	Identification, authentification et rôle des marques déposées	16
3.1.7	Validation initiale de l'identité.....	16
3.1.8	Méthode pour prouver la possession de la clé privée.....	16
3.1.9	Validation de l'identité d'un organisme	16
3.1.10	Validation de l'identité d'un individu	17
3.1.11	Informations non vérifiées du porteur	17
3.1.12	Validation de l'autorité du demandeur	17
3.1.13	Certification croisée d'A.C.	17
3.2	Identification et validation d'une demande de renouvellement des clés.....	17
3.2.1	Identification et validation pour un renouvellement courant.....	17
3.2.2	Identification et validation pour un renouvellement après révocation	17
4	Identification et validation d'une demande de révocation	17

5	EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	18
5.1	Demande de certificat.....	18
5.1.1	Origine d'une demande de certificat	18
5.1.2	Processus et responsabilités pour l'établissement d'une demande de certificat	18
5.2	Traitement d'une demande de certificat	18
5.2.1	Exécution des processus d'identification et de validation de la demande	18
5.2.2	Acceptation ou rejet de la demande.....	19
5.3	Délivrance du certificat	19
5.3.1	Actions de l'A.C. concernant la délivrance du certificat	19
5.3.2	Notification de la délivrance du certificat au porteur	19
5.4	Acceptation du certificat	19
5.4.1	Démarche d'acceptation du certificat	19
5.5	Publication du certificat	19
5.5.1	Notification aux autres entités de la délivrance du certificat	19
5.6	Usages de la bi-clé et du certificat.....	20
5.6.1	Utilisation de la clé publique et du certificat par l'utilisateur du certificat.....	20
5.7	Renouvellement d'un certificat.....	20
5.8	Délivrance d'un nouveau certificat à la suite du changement de la bi-clé.....	20
5.9	Modification du certificat	20
5.10	Révocation et suspension des certificats	20
5.10.1	Causes possibles d'une révocation	20
5.10.2	Origine d'une demande de révocation	21
5.10.3	Procédure de traitement d'une demande de révocation.....	21
5.10.4	Délai accordé au porteur pour formuler la demande de révocation	22
5.10.5	Délais de traitement par l'A.C. d'une demande de révocation	22
5.10.6	Exigences de vérification de la révocation par les utilisateurs de certificats.....	23
5.10.7	Fréquence d'établissement des LCR.....	23
5.10.8	Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats.....	23
5.10.9	Délai maximum de publication d'une LCR.....	23
5.10.10	Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats	23
5.10.11	Autres moyens disponibles d'information sur les révocations	23
5.10.12	Exigences spécifiques en cas de compromission de la clé privée.....	23
5.10.13	Suspension de certificats.....	23
5.11	Fonction d'information sur l'état des certificats	23
5.11.1	Caractéristiques opérationnelles	23
5.11.2	Disponibilité de la fonction.....	24
5.11.3	Fin de la relation entre le porteur et l'AC	24
5.11.4	Séquestre de clé et recouvrement.....	24
6	MESURES DE SECURIE NON TECHNIQUES	24
6.1	Mesures de sécurité physique	24
6.1.1	Accès physique.....	25
6.1.2	Alimentation électrique et climatisation	25
6.1.3	Vulnérabilité aux dégâts des eaux	25
6.1.4	Prévention et protection incendie	25
6.1.5	Conservation des supports.....	25
6.1.6	Mise hors service des supports.....	25
6.1.7	Sauvegardes hors site	26

6.2	Mesures de sécurité procédurales	26
6.2.1	Rôles de confiance	26
6.2.2	Nombre de personnes requises par tâches.....	27
6.2.3	Identification et authentification pour chaque rôle	27
6.2.4	Rôles exigeant une séparation des attributions	27
6.3	Mesures de sécurité vis à vis du personnel.....	27
6.3.1	Qualifications, compétences et habilitations requises	27
6.3.2	Procédures de vérification des antécédents.....	28
6.3.3	Exigences en matière de formation initiale.....	28
6.3.4	Exigences en matière de formation continue et fréquences des formations.....	28
6.3.5	Fréquence et séquence de rotation entre différentes attributions	28
6.3.6	Sanctions en cas d'actions non autorisées.....	28
6.3.7	Exigences vis-à-vis du personnel des prestataires externes	28
6.3.8	Documentation fournie au personnel	28
6.4	Procédures de constitution des données d'audit	29
6.4.1	Type d'événement à enregistrer	29
6.4.2	Fréquence de traitement des journaux d'événements	29
6.4.3	Période de conservation des journaux d'événements	29
6.4.4	Protection des journaux d'événements	29
6.4.5	Procédure de sauvegarde des journaux d'événements	29
6.4.6	Système de collecte des journaux d'événements	29
6.4.7	Notification de l'enregistrement d'un événement au responsable de l'événement..	30
6.4.8	Évaluation des vulnérabilités.....	30
6.5	Archivage des données.....	30
6.5.1	Types de données à archiver	30
6.5.2	Période de conservation des archives	30
6.5.3	Certificats, LAR et LCR émis par l'AC	31
6.5.4	Protection des archives	31
6.5.5	Procédure de sauvegarde des archives	31
6.5.6	Exigences d'horodatage des données.....	31
6.5.7	Système de collecte des archives	31
6.6	Procédures de récupération et de vérification des archives	31
6.7	Changement de clé d'AC.....	31
6.8	Reprise suite à compromission et sinistre	32
6.8.1	Procédures de remontée et de traitement des incidents et des compromissions.....	32
6.8.2	Procédures de reprise en cas de sinistre	33
6.8.3	Procédures de reprise en cas de compromission de la clé privée d'une composante	33
6.8.4	Capacités de continuité d'activité suite à un sinistre.....	33
6.9	Fin de vie de l'I.G.C.	33
6.9.1	Transfert d'activité ou cessation d'activité	33
6.9.2	Cessation d'activité affectant l'activité de l'A.C.	33
7	MESURES DE SECURITE TECHNIQUES	34
7.1	Génération et installation de bi-clés.....	34
7.1.1	Génération des bi-clés.....	34
7.1.2	Transmission de la clé privée à son propriétaire	35
7.1.3	Transmission de la clé publique à l'A.C.	35
7.1.4	Transmission de la clé publique de l'A.C. aux utilisateurs de certificats.....	35
7.1.5	Tailles des clés	35
7.1.6	Vérification de la génération des paramètres des bi-clés et de leur qualité	35

7.1.7	Objectifs d'usage de la clé	35
7.2	Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques	35
7.2.1	Standards et mesures de sécurité pour les modules cryptographiques	35
7.2.2	Contrôle de la clé privée de l'A.C. par plusieurs personnes	36
7.2.3	Contrôle de la clé privée de porteur par plusieurs personnes	36
7.2.4	Séquestre de la clé privée.....	36
7.2.5	Copie de secours de la clé privée D'AC :	36
7.2.6	Copie de secours de la clé privée des porteurs :	36
7.2.7	Archivage de la clé privée	36
7.2.8	Transfert de la clé privée vers / depuis le module cryptographique.....	36
7.2.9	Stockage de la clé privée dans un module cryptographique	36
7.2.10	Méthode d'activation de la clé privée	37
7.2.11	Méthode de désactivation de la clé privée.....	37
7.2.12	Méthode de destruction des clés privées	37
7.3	Autres aspects de la gestion des bi-clés.....	37
7.3.1	Archivage des clés publiques	37
7.3.2	Durées de vie des bi-clés et des certificats	37
7.4	Données d'activation	38
7.4.1	Génération et installation des données d'activation	38
7.4.2	Protection des données d'activation	38
7.5	Mesures de sécurité des systèmes informatiques	38
7.5.1	Niveau d'évaluation sécurité des systèmes informatiques	39
7.6	Mesures de sécurité liées au développement des systèmes.....	39
7.7	Mesures de sécurité réseau.....	39
7.8	Horodatage / Système de datation	39
8	PROFILS DES CERTIFICATS ET DES L.C.R.	39
8.1	Certificats de l'A.C.	39
8.2	Certificat de signature (1.3.6.1.4.1.58553.1.7.1.3).....	40
8.3	Liste de Certificats Révoqués	41
9	AUDITS DE CONFORMITE ET EVALUATIONS.....	41
9.1	Fréquences et circonstances des évaluations	41
9.2	Identités / qualifications des évaluateurs	41
9.3	Relations entre évaluateurs et entités évaluées	41
9.4	Sujets couverts par les évaluations	41
9.5	Actions prises suite aux conclusions des évaluations	42
9.6	Communication des résultats	42
10	AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES.....	42
10.1	Tarifs.....	42
10.1.1	Tarifs pour la fourniture ou le renouvellement de certificats	42
10.1.2	Tarifs pour accéder aux certificats.....	42
10.1.3	Tarifs pour accéder aux informations d'état et de révocation des certificats	42
10.1.4	Tarifs pour d'autres services	42
10.1.5	Politique de remboursement	42
10.2	Responsabilité financière.....	42
10.3	Confidentialité des données	42
10.3.1	Périmètre des informations confidentielles	42
10.3.2	Informations hors du périmètre des informations confidentielles	43
10.3.3	Responsabilités en termes de protection des informations confidentielles	43

10.4	Protection des données personnelles	43
10.4.1	Politique de protection des données personnelles	43
10.4.2	Informations à caractère personnel	43
10.4.3	Informations à caractère non personnel	43
10.4.4	Responsabilité en termes de protection des données personnelles	44
10.4.5	Notification et consentement d'utilisation des données personnelles.....	44
10.4.6	Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives	44
10.4.7	Autres circonstances de divulgation d'informations personnelles	44
10.5	Droits sur la propriété intellectuelle et industrielle.....	44
10.6	Interprétations contractuelles et garanties	44
10.7	Limite de garantie	44
10.8	Limite de responsabilité.....	44
10.9	Indemnités	44
10.10	Durée et fin anticipée de validité de la P.C.	44
10.10.1	Durée de validité	44
10.10.2	Fin anticipée de validité	44
10.10.3	Effets de la fin de validité et clauses restant applicables	44
10.11	Notifications individuelles et communications entre les participants	45
10.12	Amendements à la P.C.	45
10.13	Dispositions concernant la résolution de conflits	45
10.14	Juridictions compétentes	45
10.15	Conformité aux législations et réglementations	45
10.16	Transfert d'activités	45
Annexe 1 : Exigences de sécurité du module cryptographique de l'A.C.		45
Exigences sur les objectifs de sécurité.....		45

1 Introduction

1.1 Présentation générale

Ce document constitue la politique de certification mise en œuvre par la société Damanesign pour la fourniture de certificats de signature de type « avancée » pour des personnes physiques.

La présente Politique de Certification (PC) décrit les règles que Damanesign, les Clients et les Porteurs aussi appelé Utilisateur ou Signataire doivent respecter pour assurer la gestion du cycle de vie de Certificats électroniques et de bi-clés destinés à la signature électronique de Documents métier par les Porteurs.

La signature des Documents est réalisée en utilisant les services de signature suivants :

- Web App Damanesign sur le site : <https://webapp.damanesign.ma/>
- L'API Damanesign

Dans les deux cas, le Certificat est émis par la même Autorité de Certification et la présente PC s'applique.

Damanesign a mis en place l'Autorité de Certification dénommée « Damanesign Signature CA » (appelée « AC » dans le présent document), pour la délivrance de Certificats Porteurs (appelés « Certificats » dans le présent document), qui s'appuie sur une Infrastructure de Gestion de Clés (IGC). L'AC « Damanesign Signature CA » est certifiée par l'AC racine « Damanesign Root CA ».

Le service de signature permet aux Porteurs de signer des Documents au format PDF à l'aide des clés privées associées aux Certificats délivrés par l'AC.

La présente PC a pour objet de décrire la gestion du cycle de vie des : - Certificats des Porteurs délivrés par l'AC et des bi-clés associées ;

1.2 Identification du document

La présente P.C. est dénommée *Politique de certification de Signature Avancée*. Elle est identifiée par son numéro d'identifiant d'objet, ainsi que par le nom, numéro de version, la date de mise à jour.

La présente P.C. constitue aussi la partie publique de la D.P.C. (Déclaration des pratiques de certification) pour l'A.C. et les différentes familles de certificats.

L'OID de la présente PC est : 1.3.6.1.4.1.58553.1.7.1.3

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

1.3.1 Le Prestataire de services de certification électronique

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

Le P.S.Co. 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

Une Autorité de Certification (AC) désigne l'autorité en charge de la création, la délivrance, la gestion et la révocation des Certificats au titre de la Politique de Certification 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 la présente politique de certification, l'A.C. est la société Damanesign.

1.3.3 Utilisateurs de certificat :

Les Parties Utilisatrices désignent les individus ou les entreprises qui souhaitent utiliser les informations contenues dans un Certificat à des fins personnelles ou professionnelles. Il est de la responsabilité des Parties Utilisatrices de vérifier les informations concernant le statut de révocation du Certificat.

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 d'enregistrement : Cette fonction vérifie les informations d'identification du futur Porteur d'un, 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. Elle a également en charge, lorsque cela est nécessaire, la re-vérification des informations du Client lors du renouvellement du Certificat de celui-ci.

Service de demande de certificat : ce service crée une demande de certificat, à l'aide des informations fournies par le service d'enregistrement dans le but de créer et de transmettre une demande de certificat au service de génération de certificat ;

Fonction de génération des certificats : ce service génère les certificats électroniques des porteurs à partir des informations transmises par le service de demande de certificat ;

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 (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

Fonction d'information sur l'état des certificats : Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) et éventuellement également selon un mode requête / réponse temps réel (OCSP).

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.Co.), 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 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.
- Être en relation par voie contractuelle / hiérarchique / réglementaire avec le porteur pour la gestion de ses certificats ;
- Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse ;
- Les certificats d'AC doivent être diffusés préalablement à toute diffusion de certificats de porteurs ou de LCR correspondants sous 24 h.

1.3.4 Autorité d'enregistrement

L'AE a en charge :

- La vérification d'identité du demandeur
- Le contrôle de son habilitation à demander un certificat
- La vérification de l'identité apparaissant dans le certificat
- 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).

Pour les porteurs, l'AE est l'interface Web App Damanesign.

1.3.5 Porteurs de certificats

Le Porteur de Certificat est la personne physique détentrice du Certificat. Le Porteur a nécessairement adhéré aux conditions prévues par l'Accord de Souscription.

Le porteur respecte les conditions qui lui incombent telles que définies dans la présente PC. Les Parties Utilisatrices sont soumises aux stipulations de l'Accord d'Utilisation.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

Dans le cadre de la présente D.P.C., il s'agit de produire une signature électronique avancée des données (documents), conformément à la loi marocaine 43-20.

1.4.2 Bi-clés et certificats des porteurs

La présente P.C. traite des bi-clés et des certificats à destination des catégories de porteurs afin que ces derniers puissent signer électroniquement des données (documents) dans le cadre d'échanges, ou les authentifier. Une signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

L'utilisation de la clé privée du porteur et du certificat associé doit rester strictement limitée au service de signature électronique. L'utilisateur du certificat a ainsi l'assurance que le porteur identifié dans le certificat a manifesté son consentement quant au contenu des données signées électroniquement à l'aide de la clé privée correspondante.

Dans le cadre d'une application d'échanges dématérialisés de niveau avancée, les certificats de signature électronique objets de la présente PC sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité afin de pouvoir signer indûment des données sont très forts (intérêt pour les usurpateurs, effets de la signature, etc.).

1.4.3 Bi-clés et certificats d'A.C.

Pour tous les certificats, une unique bi-clés est utilisée pour la signature des certificats porteurs et de la L.C.R. sous la responsabilité de l'AC.

Les bi-clés associées aux Certificats des AC peuvent être utilisées pour signer :

- Les Certificats des AC Intermédiaires (pour les AC Primaires) ;
- Les Certificats des Porteurs (pour les AC Intermédiaires) ;
- Les LCR et/ou les réponses OCSP de l'AC ;
- Les Certificats des composants techniques de son infrastructure.

1.5 Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 5.6 ci-dessous. L'A.C. respecte ces restrictions et impose leur respect par ses porteurs et ses utilisateurs de certificats.

À cette fin, elle communique à tous les porteurs et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

1.6 Gestion de la Politique de certification

1.6.1 Entité gérant la P.C.

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

1.6.2 Point de contact

La rédaction, la modification et la diffusion de la P.C. est confiée à Damanesign.

Adresse postale	Damanesign 4 RUE OUED ZIZ 3e ETAGE APPT 7 AGDAL, Rabat
Adresse courriel	contact@damanesign.ma
Numéro de téléphone	+212 5 37 68 68 01
Site internet	https://www.damanesign.ma/

1.6.3 Procédures d'approbation de la conformité de la D.P.C/P.C.

Cette PC sera revue périodiquement, a minima annuellement, chaque changement majeur et au vu des résultats des audits internes effectués, par le comité de pilotage de l'AC pour assurer sa conformité aux normes de la loi marocaine.

1.7 Définitions et sigles

1.7.1 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	<i>Distinguished Name</i>
D.P.C.	Déclaration des Pratiques de Certification
ETSI	<i>Européen Télécommunications Standards Institute</i>
L.C.R.	Liste des Certificats Révoqués
O.E.	Opérateur d'Enregistrement
O.C.	Opérateur de Certification
OCSP	<i>Online Certificat Statu Protocol</i>
OID	<i>Object Identifier</i>
P.C.	Politique de Certification
P.S.C.E.	Prestataire de Services de Certification Électronique
P.S.Co.	Prestataire de Services de Confiance
S.S.I.	Sécurité des Systèmes d'Information
URL	<i>Uniform Resource Locator</i>

1.7.2 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.

Mandataire de certification (M.C.) : Un mandataire de certification peut être désigné par l'entité cliente et placé sous sa responsabilité. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications

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 Clés publiques et qui certifie les autorités de certification filles.

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, 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.

Online Certificate Status Protocol (OCSP) : 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 d'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.

Prestataire de services de confiance (P.S.Co.) : une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié”.

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

2.1 Entités chargées de la mise à disposition des informations

L'AC met en œuvre une fonction de publication et une fonction d'information sur l'état des certificats à destination des porteurs et des utilisateurs de certificats (cf. chapitre 1.4.2 ci-dessus). Les méthodes de mise à disposition et les adresses correspondantes sont précisées ci-après.

2.2 Informations devant être publiées

L'AC s'engage à porter à la connaissance des Porteurs et des Parties Utilisatrices :

- La politique de certification, établie par le P.S.Co. 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)
- Les différentes P.C. des A.C.

Ces documents sont publiés à l'adresse :

<https://pki.damansign.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.damansign.ma/CertData/DamaneSign%20signature%20CA.crt>

2.2.2 Publication de la CRL

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

<http://pki.damane-sign.ma/CertData/DamaneSign%20signature%20CA.crl>

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 effectives 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 5.10 et 5.11.

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.

Les ajouts, suppressions et modifications de ces informations sont limités aux personnes autorisées par l'entité en charge des informations publiées.

3 IDENTIFICATION ET AUTHENTIFICATION

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.

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les Porteurs de Certificats doivent être explicites, ils doivent permettre d'identifier de manière directe ou indirecte le Porteur du Certificat.

A.C. Signature :

C = MA	Pays
O=DamaneSign SA	Nom déposé de l'organisation
OU=154609	Numéro du registre du commerce
CN= DamaneSign signature CA	Nom de l'A.C.

Certificat de signature :

Le DN du porteur est construit à partir des nom et prénom, de son état civil tel que porté sur les documents d'identité présentés lors de son enregistrement auprès de l'AE, comme suit.

CN	Nom et prénom de la personne
givenName	Prénom de la personne

surName	Nom de la personne
serialNumber	Valeur aléatoire assurant l'unicité du certificat
C	MA

3.1.3 Anonymisation ou pseudonymisation des Porteurs

L'anonymisation et la pseudonymisation des Porteurs sont interdites.

3.1.4 Certificats de test

Les certificats de test sont identifiables par le fait que leur CN contient le mot « TEST », précédant un prénom et un nom fictifs.

Règles d'interprétation des différentes formes de nom

Sans objet.

3.1.5 Unicité des noms

Le DN du champ "subject" de chaque certificat de porteur permet d'identifier de façon unique le porteur correspondant au sein du domaine de l'AC.

Ce DN respecte les règles d'homonymie au sein du domaine de l'AC.

Dans chaque certificat X509v3, l'AC émettrice (issuer) et le porteur (subject) sont identifiés par un "Distinguished Name" (DN) de type X.501.

L'unicité des noms au sein de la présente AC est assuré par le champ serialNumber du DN (y compris pour les certificats de test).

L'anonymat ou le pseudonyme des porteurs ne sont pas supportés par la présente AC.

3.1.6 Identification, authentification et rôle des marques déposées

L'AE se réserve le droit de suspendre la génération d'un certificat si le CN est susceptible d'être lié ou de porter préjudice à un quelconque titre ou droit de propriété intellectuelle.

Si un tel cas arrive, l'AE demandera au porteur les informations et documents démontrant la légitimité de son CN. A défaut, le porteur devra demander la génération d'un nouveau certificat avec une modification du CN permettant d'éviter la reprise et résoudre le litige.

3.1.7 Validation initiale de l'identité

L'enregistrement d'un porteur se fait directement auprès de l'A.E. de Damanesign, qui est responsable et en charge de la validation de l'identité.

3.1.8 Méthode pour prouver la possession de la clé privée

L'AC génère la bi-clé du certificat.

Damanesign met en œuvre des moyens techniques et organisationnels afin d'assurer que la clé privée ne sera utilisée que par le porteur. En aucun cas Damanesign ne pourra utiliser cette clé pour son propre usage ou pour le compte d'une autre personne que le porteur

3.1.9 Validation de l'identité d'un organisme

Sans objet.

3.1.10 Validation de l'identité d'un individu

La validation initiale de l'identité du porteur est ainsi réalisée : l'AE valide une pièce d'identité, un numéro de téléphone et, le cas échéant, une adresse mail.

Les pièces d'identité acceptées sont :

- La carte d'identité ;
- Le passeport ;
- La carte de séjour.

Pour ce faire, nous réaliserons le processus suivant :

- utilisation d'une URL unique ;
- vérification de la pièce d'identité envoyée par le porteur ;
- envoi d'un code d'authentification transmis par téléphone (SMS).

Lorsque le futur porteur s'est rendu sur l'URL unique, qu'il a téléchargé sa pièce d'identité, que celle-ci a été vérifiée, son identité est validée.

3.1.11 Informations non vérifiées du porteur

Aucune.

3.1.12 Validation de l'autorité du demandeur

Sans objet, le demandeur et le signataire sont la même personne.

3.1.13 Certification croisée d'A.C.

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

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

3.2.1 Identification et validation pour un renouvellement courant

L'identification et la validation de l'identité du porteur pour un renouvellement correspond à une nouvelle demande de certificat. Nous suivrons le processus spécifié dans le chapitre Validation initiale de l'identité.

3.2.2 Identification et validation pour un renouvellement après révocation

L'identification et la validation de l'identité du porteur pour un renouvellement après révocation correspond à une nouvelle demande de certificat. Nous suivrons le processus spécifié dans le chapitre Validation initiale de l'identité.

4 Identification et validation d'une demande de révocation

La demande de révocation d'un certificat pourra se faire par téléphone ou par courriel. Voici la procédure à suivre :

- Révocation via téléphone : l'utilisateur pourra contacter Damanesign par téléphone afin de demander la révocation de son certificat. Pour ce faire, Damanesign s'assure de son identité. Une série de 2 questions aléatoires concernant son identité sera posée au porteur. Ces questions seront fondées sur les informations en possession de Damanesign. La

validation sera effective, suite à une confirmation obtenue via un autre canal que l'appel téléphonique. Par exemple, nous pouvons lui envoyer un lien de confirmation sur son adresse courrier électronique.

- Révocation par courriel : l'utilisateur pourra contacter Damanesign par mail afin de demander la révocation de son certificat. Pour ce faire, Damanesign s'assure de son identité. Une série de 2 questions aléatoires concernant son identité sera posée au porteur. Ces questions seront fondées sur les informations en possession de Damanesign. La validation sera effective, suite à une confirmation obtenue via un autre canal que le mail. Par exemple, nous pouvons :
 - Lui envoyer un code sur son numéro de téléphone
 - Effectuer un appel téléphonique pour avoir une confirmation

Remarque : La demande de révocation n'est recevable que durant la durée de vie du certificat électronique qui est de 15 minutes. En dehors de cette période le certificat aura expiré et il ne sera pas possible de réaliser une opération de révocation.

5 EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

5.1 Demande de certificat

5.1.1 Origine d'une demande de certificat

La demande de certificat provient du besoin de faire signer par un porteur un document.

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

Les informations suivantes doivent au moins faire partie de la demande de certificat (cf. chapitre Validation initiale de l'identité) :

- Le nom du porteur à utiliser dans le certificat (nom de famille et prénom) ;
- Les données personnelles d'identification du porteur (numéro de téléphone et/ou adresse électronique, le numéro de téléphone) ;
- Une pièce d'identité valide au nom du porteur.

Le dossier d'enregistrement est établi directement par le futur porteur. Le dossier est transmis directement à l'AE par voie électronique. L'AE s'assure de disposer d'une information permettant de contacter le futur porteur du certificat, l'adresse électronique ou le numéro de téléphone étant obligatoire.

Le porteur de certificat est une personne physique.

5.2 Traitement d'une demande de certificat

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

Les identités « personne physique » sont vérifiées conformément aux exigences du chapitre Validation initiale de l'identité.

Dans tous les cas, l'AE doit de plus s'assurer que le futur porteur a pris connaissance des modalités applicables pour l'utilisation du certificat (voir les conditions générales d'utilisation).

L'AE vérifie la validité de la pièce d'identité et sa correspondance avec le nom et prénom du porteur.

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat et de la bi-clé vers la fonction adéquate de l'IGC.

5.2.2 Acceptation ou rejet de la demande

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

Durée d'établissement du certificat

La demande de génération du certificat et de la bi-clé est générée par l'AC vers la fonction adéquate de l'IGC est produite dans les secondes suivant la validation de la demande.

5.3 Délivrance du certificat

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

Pour donner suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération et de préparation des différents éléments.

L'ordonnancement des opérations est assuré ainsi que l'intégrité et l'authentification des échanges entre les composantes en fonction de l'architecture de l'IGC.

Les conditions de génération des certificats et la génération des bi-clés, ainsi que les mesures de sécurité à respecter sont précisés aux chapitres ci-dessous.

5.3.2 Notification de la délivrance du certificat au porteur

Pas de notification au porteur.

5.4 Acceptation du certificat

5.4.1 Démarche d'acceptation du certificat

L'acceptation d'un certificat émis par l'AC est tacite dès la signature effectuée via le système de signature Damanesign. Avant cette utilisation, le porteur peut refuser la génération du certificat en interrompant le processus de signature. Si la bi-clé avait déjà été générée, cette dernière est détruite de manière automatique par un processus technique.

L'AC conserve une trace de l'acceptation (action de la signature) du certificat par le porteur.

5.5 Publication du certificat

L'AC ne publie pas les certificats des porteurs émis. Néanmoins les certificats sont insérés dans les signatures réalisées par le processus de signature Damanesign.

5.5.1 Notification aux autres entités de la délivrance du certificat

L'AC informe l'AE de l'émission du certificat.

5.6 Usages de la bi-clé et du certificat

Utilisation de la clé privée et du certificat par le porteur

Le certificat étant éphémère, la clé privée n'est utilisée que dans le cadre du processus de signature. La clé privée correspondante est détruite en fin de ce processus.

Le certificat de signature peut être utilisé par des tiers (les utilisateurs) pour vérifier une signature.

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

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

Les utilisateurs de certificats seront informés par l'AC qu'ils doivent respecter strictement les usages autorisés des certificats et que dans le cas contraire, leur responsabilité pourrait être engagée.

5.7 Renouvellement d'un certificat

Dans la cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante.

L'AC générant les bi-clés des porteurs, garantit qu'un certificat correspondant à une bi-clé existante ne peut pas être renouvelé au sens du [RFC3647].

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

Le processus est le même qu'en cas de demande initiale.

5.9 Modification du certificat

Sans objet.

5.10 Révocation et suspension des certificats

5.10.1 Causes possibles d'une révocation

5.10.1.1 Certificats de porteur

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

- Les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, 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 leurs obligations découlant de la PC de l'AC ou des CGU correspondantes ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur ;
- La clé privée du porteur est suspectée de compromission, est compromise ou, est perdue.
- Les données d'authentification du porteur ont été compromises ;
- Le porteur demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du porteur) ;
- Le décès du porteur ;
- Une modification des informations du certificat doit être réalisée ;
- Un certificat de l'AC « Damanesign Signature CA » est révoqué, entraînant de fait la révocation de tous les certificats porteurs qui ont été émis par cette AC.

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

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

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats et de LCR / LAR) :

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

5.10.2 Origine d'une demande de révocation

5.10.2.1 *Certificats de porteur*

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

- Le porteur du certificat ;
- L'AC émettrice du certificat ou l'une de ses composantes (AE).

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

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

5.10.3 Procédure de traitement d'une demande de révocation

5.10.3.1 *Révocation d'un certificat de porteur*

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

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

- L'identité du porteur telle qu'elle apparaît dans le certificat, ou toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série, identifiant du porteur) ;
- Le nom du demandeur de la révocation ;
- La cause de révocation.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats.

L'information de révocation sera diffusée au minimum via une LCR signée par une entité désignée par l'AC. Le demandeur de la révocation sera informé du bon déroulement de l'opération et de la

révocation effective du certificat. De plus, si le porteur du certificat n'est pas le demandeur, il sera également informé de la révocation effective de son certificat.

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

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

- Révocation du certificat d'A.C.
- Signature d'une nouvelle L.A.R.

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

Le point de contact identifié au sein de la D.G.S.S.I. sera immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés que leurs certificats ne sont plus valides. Pour cela, l'IGC devra informer les porteurs de certificats en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide. Afin de faciliter la révocation du certificat de l'AC, celle-ci est signée par une autorité supérieure racine.

5.10.4 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.

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

5.10.5.1 Révocation d'un certificat porteur

Par nature, une demande de révocation doit être traitée en urgence. La fonction de gestion des révocations est disponible 24h/24h 7j/7j.

Toute demande de révocation d'un certificat porteur sera traitée dans un délai inférieur à 24h, ce délai s'entend entre la réception de la demande de révocation et la mise à disposition de l'information de révocation auprès des utilisateurs

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

La révocation d'un certificat d'une composante de l'IGC doit être 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 (LAR) 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 et de LCR / LAR) sera effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

Le point de contact identifié au sein de la DGSSI doit être immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification.

5.10.6 Exigences de vérification de la révocation 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. Il pourra utiliser la dernière LCR publiée par l'AC afin de vérifier le statut de révocation du certificat de porteur. L'utilisateur doit aussi vérifier le statut de révocation des AC de la chaîne de certification en utilisant pour chacune la dernière LAR émise par l'AC de niveau supérieur.

5.10.7 Fréquence d'établissement des LCR

Les LCR sont générées, à minima, toutes les 24h.

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

La fonction de gestion des révocations est disponible 24h/24 et 7J/7.

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 48 (quarante-huit) heures.

5.10.9 Délai maximum de publication d'une LCR

Les LCR sont publiées le plus rapidement possible après leur établissement. Au maximum le délai de publication sera de 30 minutes.

5.10.10 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 5.10.6 ci-dessus.

5.10.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

5.10.12 Exigences spécifiques en cas de compromission de la clé privée

En cas de compromission ou de soupçon de compromission de sa clé privée, l'AC informe les participants de Damanesign par des moyens appropriés des effets préjudiciables d'un tel incident.

5.10.13 Suspension de certificats

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

5.11 Fonction d'information sur l'état des certificats

5.11.1 Caractéristiques opérationnelles

Damanesign fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC Racine), c'est-à-dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR/LAR et l'état du certificat de l'AC Racine.

Les LCR / LAR sont publiées à l'adresse spécifiée dans le chapitre Entités chargées de la mise à disposition des informations, et à l'adresse contenue dans les certificats émis.

La L.C.R. est accessible à l'adresse indiquée en **Erreur ! Source du renvoi introuvable.**

5.11.2 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 1 heures et une durée maximale totale d'indisponibilité par mois de 4 heures.

En cas de fin de relation contractuelle, hiérarchique ou 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.

5.11.3 Fin de la relation entre le porteur et l'AC

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

5.11.4 Séquestre de clé et recouvrement

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

6 MESURES DE SECURIE NON TECHNIQUES

6.1 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
- Prévention et protection incendie
- Conservation des supports
- Mise hors service des supports
- Sauvegardes hors site

6.1.1 Accès physique

L'accès est 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 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, éléments actifs 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).

6.1.2 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 matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

6.1.3 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.

6.1.4 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.

6.1.5 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.

6.1.6 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 être conservés au moins pendant la durée de validité du certificat d'entité (en cas de renouvellement, la durée sera prolongée)

6.1.7 Sauvegardes hors site

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

6.2 Mesures de sécurité procédurales

6.2.1 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. Ces descriptions figurent dans la documentation interne de l'A.C.

6.2.2 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, est précisé dans la documentation interne de l'A.C.

6.2.3 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.

6.2.4 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

6.3 Mesures de sécurité vis à vis du personnel

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC. C'est pourquoi elles doivent être précisées, notamment sur les points suivants :

- Qualifications, compétences et habilitations requises
- Procédures de vérification des antécédents
- Exigences en matière de formation initiale
- Exigences et fréquence en matière de formation continue
- Fréquence et séquence de rotation entre différentes attributions
- Sanctions en cas d'actions non autorisées
- Exigences vis-à-vis du personnel des prestataires externes
- Documentation fournie au personnel

6.3.1 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.

6.3.2 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. Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

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

6.3.3 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.

6.3.4 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.

6.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

6.3.6 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.

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

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

6.3.8 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.

6.4 Procédures de constitution des données d'audit

6.4.1 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, en particulier en cas de demande émanant d'une autorité judiciaire ou administrative. L'AC décrit dans ses procédures internes le détail des événements et des données enregistrées. Les procédures de traçabilité mises en place par l'AC sont robustes et permettent l'agrégation des traces issues de différentes sources, la détection d'intrusion et un plan de monitoring.

6.4.2 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.

6.4.3 Période de conservation des journaux d'événements

La période de conservation des journaux d'événement est de :

- 1 mois pour les événements systèmes et techniques ;
- 1 mois pour les événements fonctionnels.

6.4.4 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.

6.4.5 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.

6.4.6 Système de collecte des journaux d'événements

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

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

Aucune notification n'est délivrée suite à l'enregistrement d'un événement.

6.4.8 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.

6.5 Archivage des données

6.5.1 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 les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- Les PC ;
- Les DPC ;
- Les certificats, LAR et LCR tels qu'émis ou publiés ;
- Les engagements signés par le responsable du Comité de Direction Technique ;
- Les journaux d'évènements des différentes entités de l'IGC, incluant en particulier les événements relatifs au cycle de vie des certificats et des clés pour les porteurs et les AC ;
- Les dossiers d'enregistrement ;
- La trace d'acceptation du certificat par le porteur.

6.5.2 Période de conservation des archives

6.5.2.1 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 sept 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 sept ans après leur expiration.

La durée de conservation des dossiers d'enregistrement doit être portée à la connaissance du porteur.

Au cours de cette durée d'opposabilité des documents, le dossier d'enregistrement doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées.

Ce dossier doit permettre de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

6.5.2.2 Journaux d'événements et autres

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

6.5.3 Certificats, LAR et LCR émis par l'AC

Les certificats de porteurs et d'AC, ainsi que les LCR / LAR produites, doivent être archivés pendant au moins 7 années après leur expiration.

6.5.4 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 documentation interne de l'A.C. décrit les moyens mis en œuvre pour archiver les pièces en toute sécurité.

Dans le cadre d'un transfert ou d'une cessation d'activité, l'ensemble des archives peuvent être confiées à un tiers chargé d'en assurer, pour la durée initialement prévue, la disponibilité et la protection dans les termes décrits dans ce paragraphe.

6.5.5 Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes, qui est équivalent au niveau de protection des archives, est précisé dans la documentation interne de l'A.C.

6.5.6 Exigences d'horodatage des données

Chaque événement contient la date et l'heure précise de réalisation.

Les composants en charge de la fonction de révocation sont synchronisés quotidiennement avec une source de temps UTC.

6.5.7 Système de collecte des archives

L'archivage est réalisé soit de manière automatique, soit de manière manuelle par du personnel autorisé.

La documentation interne de l'A.C. décrit le système de collecte des archives, interne ou externe, qui doit respecter les exigences de protection des archives concernées.

6.6 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).

6.7 Changement de clé 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 qu'elle signe. Au regard de la date de fin de validité de ce certificat, son renouvellement sera 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 sera 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.

6.8 Reprise suite à compromission et sinistre

Chaque entité opérant une composante de l'IGC doit mettre 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 et au travers de l'analyse des différents journaux d'évènements.

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'A.C., l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'A.C. Le cas de l'incident majeur est impérativement traité dès détection ; la publication de l'information de révocation du certificat est réalisée dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé...).

L'A.C. prévient directement et sans délai le point de contact identifié au sein de la D.G.S.S.I.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'A.C. ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors l'A.C. s'engage à :

- Informer tous les porteurs et les tiers utilisateurs de certificats avec lesquels l'A.C. a passé des accords ou à d'autres formes de relations établies. En complément, cette information est mise à disposition des autres utilisateurs de certificats.
- Révoquer tout certificat concerné.

6.8.1 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'évènement 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.

6.8.2 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.

6.8.3 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. § 5.8.2 > Procédures de reprise en cas de sinistre). Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué.

En outre, l'AC respecte les engagements suivants :

- Informer tous les porteurs ;
- Indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables ;
- Informer l'organe de contrôle national dans les vingt-quatre heures

6.8.4 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. § 5.8.2 > Procédures de reprise en cas de sinistre).

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

Damanesign informera la D.G.S.S.I. dans un délai maximum de deux (02) mois son intention de cesser ses activités ou de transférer son activité, et sans délai en cas de liquidation judiciaire.

6.9.1 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 événements, l'A.C. prend les mesures suivantes :

- Elle assure la continuité du service d'archivage
- Elle assure la continuité du service de Révocation

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

6.9.2 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.

Damaneign communiquera au point de contact identifié au sein de la D.G.S.S.I. 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. Ce plan présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans la présente P.C. Damaneign communiquera à la D.G.S.S.I., selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. Damaneign mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet événement. Damaneign présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les porteurs et les utilisateurs de certificats.

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

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.

Damaneign s'engage à tenir informée la D.G.S.S.I. de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

7 MESURES DE SECURITE 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.

7.1 Génération et installation de bi-clés

7.1.1 Génération des bi-clés

7.1.1.1 Clés de l'A.C.

Les clés de l'A.C. 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.

7.1.1.2 Clés porteurs générées par l'A.C.

Damaneign met en œuvre des moyens techniques et organisationnels afin d'assurer que la clé privée ne sera utilisée que par le porteur.

En aucun cas Damaneign ne pourra utiliser cette clé pour son propre usage ou pour le compte d'une autre personne que le porteur.

7.1.2 Transmission de la clé privée à son propriétaire

La clé privée n'est pas transmise au porteur. Elle est stockée par l'IGC au sein d'un module cryptographique. Son utilisation est unique et ne peut être réalisée que par le porteur qui doit utiliser un code d'authentification.

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

Sans objet.

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

La clé publique des AC est enveloppée dans un certificat signé par l'AC racine. Sa diffusion s'accompagne de l'empreinte numérique du certificat ainsi que d'une déclaration qu'il s'agit bien d'une clé publique de l'AC.

La clé publique de l'AC, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) pourront aisément être récupérées par les utilisateurs de certificats, via l'interface publique (cf. chapitre Entités chargées de la mise à disposition des informations).

7.1.5 Tailles des clés

Les clés d'AC auront ces caractéristiques :

- Algorithme utilisé : RSA.
- Taille minimale des clés : 4096 bits.

Les clés des porteurs auront ces caractéristiques :

- Algorithme utilisé : RSA.
- Taille minimale des clés : 2048 bits.

7.1.6 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.

7.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la signature électronique (voir 1.4.1).

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

7.2.1 Standards et mesures de sécurité pour les modules cryptographiques

7.2.1.1 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

Les dispositifs de création de signature, pour la mise en œuvre des clés privées d'A.C., respectent les exigences du chapitre 11 ci-dessous.

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

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

7.2.3 Contrôle de la clé privée de porteur par plusieurs personnes

Damanesign ne dispose pas des éléments permettant d'accéder et d'utiliser la clé privée d'un porteur durant le processus de signature. Le processus technique garantit que seule la clé privée générée pour le porteur durant le processus de signature est utilisée.

7.2.4 Séquestre de la clé privée

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

7.2.5 Copie de secours de la clé privée D'AC :

Les clés privées d'AC font l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences dans le chapitre Annexe 1 Exigences de sécurité du module cryptographique de l'AC ci-dessous, soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité.

Le chiffrement utilisé offre un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuie sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée.

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 soient à aucun moment en clair en dehors du module cryptographique.

7.2.6 Copie de secours de la clé privée des porteurs :

Les clés privées des porteurs ne font pas l'objet de copie de secours.

7.2.7 Archivage de la clé privée

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

7.2.8 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 **Erreur ! Source du renvoi introuvable.**

7.2.9 Stockage de la clé privée dans un module cryptographique

Le stockage des clés privées d'AC et des porteurs est réalisé dans un module cryptographique répondant aux exigences du chapitre Annexe 1 Exigences de sécurité du module cryptographique de l'AC. Cependant, dans le cas des copies de secours, le stockage peut être effectué en dehors d'un

module cryptographique moyennant le respect des exigences du chapitre Copie de secours de la clé privée.

DAMANESIGN met les moyens en place afin de garantir que les clés privées du matériel cryptographique ne sont pas compromises pendant leur stockage ou leur transport.

7.2.10 Méthode d'activation de la clé privée

7.2.10.1 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. 7.2.10) et doit faire intervenir au moins trois personnes dans des rôles de confiance.

7.2.10.2 Clés privées des porteurs

L'activation de la clé privée du porteur est liée au processus de signature réalisé par le porteur. L'identification et l'authentification du porteur réussies permettent la génération de la clé privée correspondante et son activation est immédiate.

7.2.11 Méthode de désactivation de la clé privée

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 11.

7.2.12 Méthode de destruction des clés privées

En fin de vie d'une clé privée d'AC ou de porteur, normale ou anticipée (révocation ou mise au rebut du module cryptographique), cette clé sera systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

Les clés privées des porteurs sont automatiquement détruites à la fin du processus de signature. Une fois détruites, les clés privées ne sont de fait plus utilisables.

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

Ces exigences sont précisées au chapitre 11.

7.3 Autres aspects de la gestion des bi-clés

7.3.1 Archivage des clés publiques

Voir [Archivage de la clé privée](#)

7.3.2 Durées de vie des bi-clés et des certificats

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

Les clés de signatures de l'AC auront une durée de vie de maximum 30 ans.

Les certificats des porteurs ont une durée de validité de 15 minutes. Les clés privées correspondantes ont une durée de vie équivalente à la durée du processus de signature.

7.4 Données d'activation

7.4.1 Génération et installation des données d'activation

7.4.1.1 *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.

7.4.1.2 *Génération et installation des données d'activation correspondant à la clé privée d'un certificat de signature*

Les données d'activation du porteur sont générées par :

- L'URL à usage unique lui permettant d'accéder au processus de signature ;
- Le code d'authentification saisi préalablement à l'opération de signature.

7.4.2 Protection des données d'activation

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

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique.

Les porteurs de données d'activation sont responsables de leur gestion et de leur protection.

Un porteur de données d'activation ne peut détenir plus d'une donnée d'activation d'un même A.C. à un même instant.

7.4.2.2 *Protection des données d'activation correspondant aux clés privées des porteurs*

Les éléments d'activation sont propres aux porteurs et ne sont valables que pour un processus de signature précis.

7.5 Mesures de sécurité des 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.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramètres du système (en particulier des éléments de routage) sont mis en place.

7.5.1 Niveau d'évaluation sécurité des systèmes informatiques

Sans objet

7.6 Mesures de sécurité liées au développement des systèmes

Le système mis en œuvre pour l'implémentation de l'IGC est documenté. La configuration du système des composantes de l'IGC, ainsi que toute modification et mise à niveau, sont documentées et contrôlées.

7.7 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.).

7.8 Horodatage / Système de datation

Pour dater les événements, les différentes composantes de l'IGC recourt à l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près. Pour les opérations faites hors ligne (ex : administration d'une AC Racine), cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système devra toutefois pouvoir ordonner les événements avec une précision suffisante.

8

9 PROFILS DES CERTIFICATS ET DES L.C.R.

9.1 Certificats de l'A.C.

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	cn=DamaneSign Root CA ou=154,609 o=DamaneSign SA c=MA
Validity	30 ans
Subject	cn=DamaneSign signature CA ou=154,609 o=DamaneSign SA c=MA

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	Signature numérique Liste de révocation de certificat Signature de certificat (CA)
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:http://pki.damansign.ma/CertData/DamaneSign%20Root%20CA.crl
Authority Information Access	N	CA: http://pki.damansign.ma/CertData/DamaneSign%20Root%20CA.crt

9.2 Certificat de signature (1.3.6.1.4.1.58553.1.7.1.3)

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 Erreur ! Source du renvoi introuvable.
Validity	15 min
Subject	Voir Erreur ! Source du renvoi introuvable.
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	nonRepudiation1
Basic Constraints	O	CA : FALSE
Certificate Policies	N	OID: 1.3.6.1.4.1.58553.1.7.1.3 CPS: https://pki.damansign.ma/cps.html
Issuer Alternative Name	N	Non utilisé
CRL Distribution Points		http://pki.damansign.ma/CertData/DamaneSign signature CA.crl
Authority Information Access	N	CA:http://pki.damansign.ma/CertData/DamaneSign%20signature%20CA.crt

¹ Se nomme contentCommitment dans la version récente de la norme.

9.3 Liste de Certificats Révoqués

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Signature	sha256WithRSAEncryption
Issuer	CN = DamaneSign signature CA OU = 154609 O = DamaneSign SA C = MA
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.

10 AUDITS DE CONFORMITE ET EVALUATIONS

Les audits sont réalisés afin de s'assurer que l'ensemble de l'I.G.C. est bien conforme à la réglementation en vigueur et notamment aux engagements affichés dans sa P.C.

10.1 Fréquences et 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.

Les audits sont réalisés sous la forme d'une prestation auprès d'acteurs spécialistes de la sécurité des systèmes d'information et ayant des compétences reconnues dans le domaine de la signature électronique. Dans le cadre d'obtention de certifications des services de l'IGC, l'audit de certification est réalisé par une société externe dûment accréditée.

10.2 Identités / qualifications des évaluateurs

Le contrôle d'une composante est réalisé par la D.G.S.S.I. ou par des experts désignés par elle, compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

10.3 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.

10.4 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 documentation interne de l'A.C. qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

10.5 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.

10.6 Communication des résultats

Les résultats des audits sont tenus à la disposition de la D.G.S.S.I. et de Damanesign.

11 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

11.1 Tarifs

11.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

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

11.1.2 Tarifs pour accéder aux certificats

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

11.1.3 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.

11.1.4 Tarifs pour d'autres services

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

11.1.5 Politique de remboursement

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

11.2 Responsabilité financière

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

11.3 Confidentialité des données

11.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :

- La documentation interne 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.

11.3.2 Informations hors du périmètre des informations confidentielles

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

11.3.3 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.

11.4 Protection des données personnelles

11.4.1 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 1.6.2.

11.4.2 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.

11.4.3 Informations à caractère non personnel

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

11.4.4 Responsabilité en termes de protection des données personnelles

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

11.4.5 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.

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

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

11.4.7 Autres circonstances de divulgation d'informations personnelles

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

11.5 Droits sur la propriété intellectuelle et industrielle

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

11.6 Interprétations contractuelles et garanties

Sans objet.

11.7 Limite de garantie

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

11.8 Limite de responsabilité

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

11.9 Indemnités

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

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

11.10.1 Durée de validité

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

11.10.2 Fin anticipée de validité

Sans objet

11.10.3 Effets de la fin de validité et clauses restant applicables

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

11.11 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.

11.12 Amendements à la P.C.

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

Tout changement à la P.C. ou aux pratiques de l'A.C. est communiqué à la D.G.S.S.I. avant la mise en œuvre dudit changement.

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.

11.13 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.

11.14 Juridictions compétentes

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

11.15 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.

11.16 Transfert d'activités

Cf. section 6.9.

Annexe 1 : Exigences de sécurité du module cryptographique de l'A.C.

Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR / LAR), ainsi que, pour la génération des bi-clés des porteurs, répond 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.
- 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.

Le module cryptographique est déployé selon les préconisations de sa cible de sécurité pour la qualification du matériel. La communication avec le module cryptographique est réalisée sur un canal chiffré après authentification mutuelle