Politique de certification Qualified Signature CA

Version 1.3 | Diffusion : public

***OID n°* 1.3.6.1.4.1.58553.1.3.1.3**

Historique du document

Version	Date de version	Rédacteur(s)	Approbateur(s)	Modifications
1.0	**25/04/2022**	**Samuel LACAS**	**Noureddin SOUAD**	**Création du document**
1.1	**05/10/2023**	**Fatimazahrae JALAL**	**Zouhair Hamdaoui**	**Mise à jour par rapport à la loi 43-20**
1.2	**20/08/2024**	**Fatimazahrae JALAL**	**Zouhair Hamdaoui**	**Mise à jour des certificats**
1.3	**15/11/2024**	**Fatimazahrae JALAL**	**Zouhair Hamdaoui**	**Mise à jour des méthodes de révocation**

SOMMAIRE

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 pour des personnes physiques.

1.2 Identification du document

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

Le numéro d'OID des certificats produits sous la présente P.C. est :

Certificat de signature	**1.3.6.1.4.1.58553.1.3.1.3**

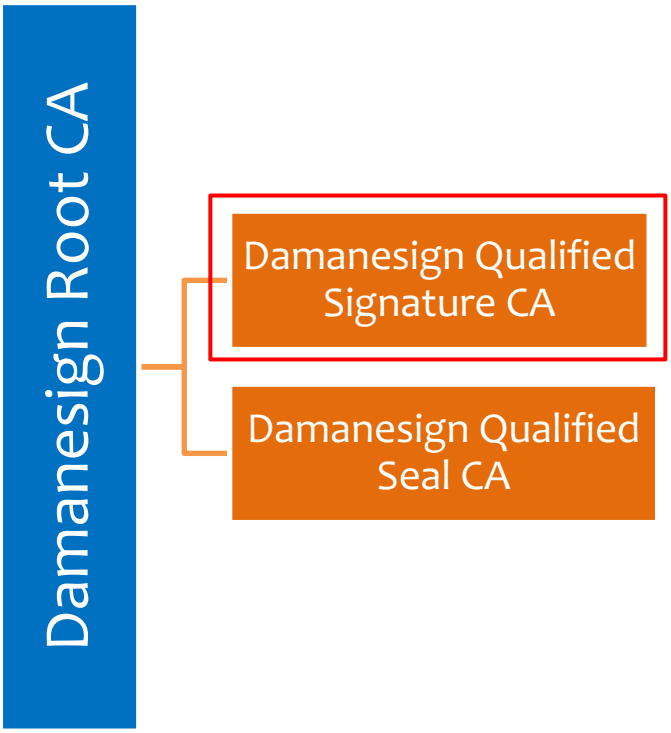
La présente P.C. constitue aussi la partie publique de la D.P.C. (Déclaration des pratiques de certification) pour l'A.C.

L'AC « DAMANESIGN QUALIFIED SIGNATURE CA » ne peut être utilisée que pour :

- Produire des certificats qualifiés de signature ;
- Produire des Listes des Certificats Révoqués (LCR) ;
- Produire des certdgificats pour son répondeur OCSP ;

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

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



Le périmètre de la présente PC est présenté dans le rectangle rouge.

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

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

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

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

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

Fonction d'enregistrement : Cette fonction vérifie les informations d'identification du futur Porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. Elle a également en charge, lorsque cela est nécessaire, la re-vérification des informations du Client lors du renouvellement du Certificat de celui-ci.

Fonction de génération des certificats : Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les Certificats à partir des informations transmises par l'Autorité d'Enregistrement et de la clé publique du Client provenant de la fonction de génération des éléments secrets du Client chargée en particulier de générer la bi-clé du Client.

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

Fonction de remise au porteur : remet au porteur un dispositif de signature contenant la bi-clé et le certificat du porteur.

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.C.O.), les exigences qui incombent à l'A.C. en tant que responsable de l'ensemble de l'I.G.C. sont les suivantes :

- Être une entité juridique au sens de la loi marocaine.
- S'assurer que les exigences de la P.C. et les procédures de la D.P.C. sont appliquées par chacune des composantes de l'I.G.C. et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa P.C., correspondant au minimum aux fonctions obligatoires de la présente P.C., notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats.
- Élaborer, mettre en œuvre, contrôler et maintenir de façon itérative les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa P.C., et correspondant au minimum aux exigences de la présente P.C., notamment en termes de fiabilité, de qualité et de sécurité.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de L.C.R. et de réponses OCSP).
- Diffuser ses certificats d'A.C. aux porteurs et utilisateurs de certificats.
- Être en relation par voie contractuelle / hiérarchique / réglementaire avec le porteur pour la gestion de ses certificats ;
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux porteurs, aux utilisateurs de certificats, … qui mettent en œuvre ses certificats ;
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur ;
- 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 ;
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions obligatoires énoncées dans les référentiels des exigences applicables aux services de confiance qualifiés, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats ;
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, et correspondant au minimum aux exigences énoncées dans les référentiels des exigences applicables aux services de confiance qualifiés, notamment en termes de fiabilité, de qualité et de sécurité ;
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR et de réponses OCSP), ou faire renouveler ses certificats si l'AC est rattaché à un AC hiérarchiquement supérieur. Diffuser ses certificats d'AC aux porteurs et utilisateurs de certificats ;

- Les certificats d'AC doivent être diffusés préalablement à toute diffusion de certificats de porteurs ou de LCR correspondants sous 24 h.

1.3.3 Autorité d'enregistrement

L'A.E. assure les tâches suivantes :

- La prise en compte et la vérification des informations du porteur (Nom complet du porteur, CIN ou passeport ou carte de séjour, Adresse électronique, Téléphone, Fonction ou qualité au sein de l'organisme, Adresse physique complète)
- La constitution du dossier d'enregistrement correspondant
- L'archivage des pièces du dossier d'enregistrement
- 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).

1.3.4 Porteurs de certificats

Un porteur de certificats est une personne physique qui utilise sa clé privée et le certificat correspondant pour son propre compte ou dans le cadre de ses activités en relation avec l'entité identifiée dans le certificat et avec laquelle il a un lien contractuel, hiérarchique ou réglementaire.

1.3.5 Utilisateurs de certificat

Un utilisateur de certificat peut être une application ou une personne physique ou morale destinataire de données électroniquement signées ou authentifiées par le porteur.

1.3.6 Mandataire de certification

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 concernant l'identité et, éventuellement, les attributs des porteurs de cette entité (il assure notamment le face-à-face pour l'identification des porteurs lorsque celui-ci est requis).

1.3.7 Personne autorisée :

Il s'agit d'une personne physique autre que le porteur et le mandataire de certification et qui est autorisée par la politique de certification du PSCO ou par contrat établi avec lui à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, …).

Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.

Le dossier des personnes autorisées clairement identifiées dans la politique de certification. Leur dossier fourni doit comporter à minima les documents suivants :

- Une copie de la carte nationale d'identité électronique en cours de validité de la personne autorisée ou tout document valide justifiant son identité (comportant une photo d'identité et délivré par une autorité compétente)
- Un document justifiant son statut de personne autorisée

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

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 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 ou messages) dans le cadre d'échanges. 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 sécurisé, 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.).
L'AC génère également des certificats spécifiquement destinés aux réponses OCSP de son service. Ces certificats se distinguent des certificats de signatures qualifiées des porteurs.

1.4.1.2 Bi-clés et certificats d'A.C.

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

La signature des réponses OCSP est réalisée par un certificat spécifique émis par l'AC.

1.4.2 Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.6 ci-dessous. L'A.C. respecte ces restrictions et impose leur respect par ses porteurs et ses utilisateurs de certificats.

1.5 Gestion de la P.C.

1.5.1 Entité gérant la P.C.

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

1.5.2 Point de contact

Adresse postale	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

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

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

1.6 Définitions et sigles

1.6.1 Sigles

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

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

1.6.2 Définitions

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

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

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

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 Clé 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

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

Composante : Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'I.G.C. L'entité peut être le P.S.C.O. lui-même ou une entité externe liée au PSCo 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 des autres et/ou liées par des liens hiérarchiques ou autres (A.C. Racines / A.C. filles). Un P.S.C.E. est identifié dans un certificat dont il a la responsabilité au travers de son A.C. ayant émis ce certificat et qui est elle-même directement identifiée dans le champ issuer du certificat.

PSCo : prestataire de service de confiance au sens de la Loi n° 43-20.

PSCo agréé : désigne un PSCo agréé par l'autorité nationale qui fournit un ou plusieurs services de confiance qualifiés conformément à la Loi n° 43-20.

PSCo sans agrément : désigne un PSCo qui fournit un ou plusieurs services de confiance non qualifiés conformément à la Loi n° 43-20.

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

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

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

2.1 Entités chargées de la mise à disposition des informations

L'A.C. met en œuvre une fonction de publication et une fonction d'information sur l'état des certificats sur les informations devant être publiées à destination des porteurs et des utilisateurs de certificats.

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

2.2 Informations devant être publiées

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

- La politique de certification, établie par le P.S.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.damanesign.ma/cps.html dont la déclaration de divulgation est prise en considération et il s'agit plus précisément d'un document qui décrit les détails importants et les politiques liées à l'infrastructure de clés publiques mise en place (Certificat Qualifiée de Signature, Certificat Root et les CRLs) ainsi qu'une chaine de confiance qui est respectée et bien ficelée.

2.2.1 Publication du certificat d'AC

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

`http://pki.damanesign.ma/certs/ca_qsig_2024.crt`

2.2.2 Publication de la CRL

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

`http://pki.damanesign.ma/crl/ca_qsig_2024.crl`

2.2.3 URL d'OCSP

Le service OCSP (limité au statut de révocation des certificats de porteurs) est disponible à l'adresse :

http://ocsp.damanesign.ma/ca_qsig

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 4.10 et 4.11.

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.

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

2.5 Notification en cas de changement de la DPC, PC et CGU

Damanesign peut être amené à ajuster et à apporter des modifications aux dispositions des Conditions Générales d'Utilisation (CGU) et des documents de Politique de Certification (PC QCP Signature) et de Déclaration des Pratiques de Certification (DPC QCP Signature) relatifs au Certificat qui lui sembleraient nécessaires pour répondre aux évolutions techniques et commerciales de son offre et en vue de l'amélioration de la qualité des services de Certification ou qui seraient rendues nécessaires par la modification de la législation de la réglementation en vigueur.

Les éventuelles modifications des dispositions contractuelles seront publiées sur le site Internet de l'AC.

Les changements apportés à un document contractuel seront portés à la connaissance du Client, au moins un mois avant leur entrée en vigueur, le client ayant alors la possibilité de résilier son Contrat en cas de désaccord sans aucune pénalité. En l'absence de résiliation et si le(s) Porteurs continuent à utiliser les Certificats dépassant les un mois prévu, le Client sera réputé tacitement avoir accepté les modifications.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

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

Dans chaque certificat conforme à la norme X.509, l'A.C. émettrice (*issuer*) et le porteur (*subject*) sont identifiés par un *Distinguished Name* (DN) de type X.501.

3.1.2 Nécessité d'utilisation de noms explicites

3.1.2.1 A.C. Signature qualifié

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

3.1.2.2 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.

CommonName (CN)	Nom et prénom de la personne
GivenName (GN)	Prénom de la personne
SurName	Nom de la personne
SerialNumber	Valeur aléatoire assurant l'unicité du porteur
Country (C)	MA
OrganizationName(O)	(Obligatoire si le certificat est délivré au titulaire dans le cadre de son appartenance à une entité donnée, interdit sinon) Dénomination officielle ou raison sociale de l'entité.
OrganizationIdentifier(OI)	(Obligatoire si le certificat est délivré au titulaire dans le cadre de son appartenance à une entité donnée, interdit sinon) Numéro d'immatriculation officiel de l'entité.

3.1.3 Pseudonymisation des porteurs

Sans objet

3.1.4 Règles d'interprétation des différentes formes de nom

Sans objet.

3.1.5 Unicité des noms

Les identités portées par l'AC dans les certificats (Se reporter au § 3.1.1) sont uniques au sein du domaine de certification de l'AC. Durant toute la durée de vie de l'AC, une identité attribuée à un porteur (Se reporter au § 3.1.2.2) de certificat ne peut être attribué à un autre porteur.
A noter que l'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de certification de l'AC, mais que ce numéro est propre au certificat et non pas au porteur et ne permet donc pas d'assurer une continuité de l'identification dans les certificats successifs d'un porteur donné.
L'AE assure cette unicité au moyen de son processus d'enregistrement et de la valeur unique du champ SN attribué à un porteur (se reporter au § 3.1.2.2). En cas de différent au sujet de l'utilisation d'un nom pour un certificat, l'E.A. a la responsabilité de résoudre le différend en question. En effet, l'attribut « numéro de série » qui est un numéro unique et généré par l'AC inclus dans le DN différencie en cas d'homonymie.

3.1.6 Identification, authentification et rôle des marques déposées

L'A.C. est responsable de l'unicité des noms de ses porteurs et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

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.

3.1.9 Validation de l'identité d'un organisme

Sans objet.

3.1.10 Validation de l'identité d'un individu

L'enregistrement d'un porteur peut se faire soit directement auprès de l'AE, soit via un mandataire de certification.

Le dossier d'enregistrement, déposé auprès de l'A.E., doit au moins comprendre :

- Justificatifs d'identité des personnes
  - Les formulaires d'abonnement dûment signés, légalisés et datés de moins de trois mois par les personnes nommément désignées, incluant le formulaire de demande de certificat électronique qui doit contenir l'adresse professionnelle, le numéro de téléphone, l'adresse e-mail professionnelle du futur porteur. Le formulaire doit comporter également le cachet de l'organisme ;
  - Une copie certifiée conforme de la CIN ou passeport du bénéficiaire valide (Carte de séjour valide pour les étrangers résidents) ;
  - Une enveloppe par porteur contenant le formulaire des réponses aux questions secrètes fermée et cachetée par l'organisme ;
  - Les conditions générales qui doivent être co-signées par le mandataire et le porteur avec mention d'approbation du mandataire et cachetées par le cachet de l'organisme ;
  - Si nécessaire, Procuration signée et cachetée, conférant mandat à une personne physique pour la gestion des certificats de la personne morale.

- Un Contrat PSCo – Client
- Bon de commande signé et cacheté par l'organisme ;
- Un justificatif de paiement (reçu de paiement, chèque, virement) ;

➢ Justificatifs d'identité de l'organisme

➢ Société de toute forme juridique - Personne Moral :

- Attestation récente qui contient le Numéro ICE, à savoir l'attestation de l'inscription à la taxe professionnelle, (et/ou) le Bulletin De Notification Du N° D'identification Fiscale ou une copie récente et certifiée conforme de l'un des dites documents ;
- Copie certifiée conforme actualisé de l'extrait du registre de commerce modèle J7 ;
- Copie certifiée conforme d'un document (s) justifiant la qualité de la personne signataire en tant que représentant légal de l'organisme (délégation de pouvoir, Procès-Verbal de nomination, Statut, …) actualisé ;

➢ Ministère / Etablissement public :

- Copie certifiée conforme d'un document (s) justifiant la qualité de la personne signataire entant que représentant légal de l'organisme actualisé ;

➢ Association :

- Copie certifiée conforme des Statuts revêtus de la signature légalisée du président ;
- Copie certifiée conforme du procès-verbal légalisé de l'assemblée générale constitutive ou modificative ;
- Liste timbrée et légalisée des membres du bureau ;
- Copie certifiée conforme du récépissé de dépôt ;

➢ Entreprises individuelles et les fonctions réglementées (commerçant, professions libérales...) :

- Attestation récente qui contient le Numéro ICE, à savoir : l'attestation de l'inscription à la taxe professionnelle, (et/ou) le Bulletin De Notification Du N° D'identification Fiscale ou une copie récente et certifiée conforme de l'un des dites documents.

3.1.11 Informations non vérifiées du porteur

Aucune.

3.1.12 Validation de l'autorité du demandeur

Cette étape est réalisée lors de l'enregistrement via l'A.E. ou le M.C. dans le cas échéant.

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

Le renouvellement de certificat nécessite la constitution d'un dossier identique à la demande initiale.

3.2.2 Identification et validation pour un renouvellement après révocation

Pour donner suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial.

3.3 Identification et validation d'une demande de révocation

L'AE authentifie toutes les demandes de révocation.

Le Porteur a quatre méthodes pour révoquer un certificat Damanesign :

- **Révocation en ligne sur la base des réponses aux questions secrètes** : Accédez à la page "https://guichet.damanesign.ma" dans votre navigateur, suivez les étapes indiquées sous "Services" et "Révocation du Certificat", en renseignant les détails requis et en choisissant la raison de la révocation.
- **Révocation en ligne sur la base de la pièce d'identité électronique et la reconnaissance faciale** : Accédez à la page "https://guichet.damanesign.ma" dans votre navigateur, suivez les étapes indiquées sous "Services" et "Révocation du Certificat" en renseignant les détails requis et en choisissant la raison de la révocation.
- **Révocation par appel téléphonique** : Le Porteur peut contacter le service de révocation de Damanesign au +212 5 37 68 68 01 de 8h30 à 18h00 et 7j/7j, répondre à des questions pour l'authentification, préciser le certificat à révoquer et la raison de la révocation.
- **Se déplacer aux bureaux de Damanesign** : Le porteur peut se déplacer aux bureaux de Damanesign de 8h30 à 18h00 et 7j/7j, le chargé de révocation procède à la révocation sur place

Le représentant légal ou le mandataire de certification a une méthode pour révoquer un certificat d'un Porteur :

- **Révocation par courrier** : Envoyer une demande de révocation du certificat cachetée et signée par courrier à l'adresse fournie par Damanesign. Après vérification, Damanesign procède à la révocation et envoie une confirmation au demandeur et au Porteur.

Toute demande de révocation de certificat est enregistrée et sauvegardée conformément aux procédures internes.

Dans le cas où une demande de révocation ne peut être confirmée dans les 24 heures.

Damanesign suit la procédure suivante :

Notification Immédiate : En cas de non-confirmation d'une demande de révocation dans les 24 heures, le personnel de l'autorité de certification (AC) doit être immédiatement informé de la situation.

- **Analyse :** Une analyse de la demande de révocation doit être effectué pour identifier les raisons de la non-confirmation. Cela peut inclure la vérification des systèmes, des journaux d'audit, et des données de la demande de révocation.
- **Communication avec le Demandeur :** Le demandeur de la révocation doit être contacté pour obtenir des informations supplémentaires ou clarifications via l'e-mail et/ou le téléphone.
- **Actions à prendre :** Sur la base de l'analyse, des actions appropriées doivent être mises en œuvre. Cela peut inclure la révocation du certificat concerné et/ou renouvellement selon la procédure décrite dans le présent document.

- **Rapport Post-Action :** Un rapport post-action doit être généré pour documenter toutes les étapes de la procédure de révocation. Ce rapport doit être sauvegarder et archiver avec le dossier de porteur.

Gestion de la révocation de certificat par l'AE du Damanesign suite à un signalement de problème de certificat :

- Les abonnés, les parties faisant confiance, les fournisseurs de logiciels d'application et d'autres tiers peuvent soumettre des rapports de problème de certificat via contact@damanesign.ma. Damanesign publie des instructions relatives à la révocation de certificat dans un guide dédiée faisant partie de son référentiel public.
- Pour tout rapport de problème de certificat, le déclarant est prié d'inclure ses coordonnées, les abus suspectés et le sujet lié (par exemple, FQDN ou IP).
- La AE du Damanesign commence l'enquête sur un rapport de problème de certificat dans les 24 heures suivant la réception et décide si la révocation ou d'autres actions appropriées sont nécessaires, basées au moins sur les critères suivants :
  - La nature du problème allégué,
  - Le nombre de rapports de problème de certificat reçus concernant un certificat particulier ou un sujet,
  - L'entité faisant le rapport (par exemple, une notification d'une organisation anti-logiciels malveillants ou d'une agence de maintien de l'ordre a plus de poids qu'une plainte anonyme),
  - La législation locale pertinente.

  En cas de décision de révoquer un certificat en raison du rapport de problème de certificat, l'AE du Damanesign exécute la procédure de révocation comme spécifié précédemment dans cette section.

4 EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

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

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

Les informations suivantes doivent au moins faire partie de la demande de certificat :

- Le nom du porteur à utiliser dans le certificat ;
- Les données personnelles d'identification du porteur ;
- Les données d'identification de l'entité du porteur le cas échéant ;
- Une série des questions / réponses sur des informations propres au demandeur et qui seront utilisés comme élément d'authentification lors d'une demande de révocation ;
- Les Informations permettant à l'AE de contacter le porteur (numéro de téléphone, courriel, adresse physique …) ;

Le dossier de demande est établi par le futur porteur et transmis à l'AE via le Mandataire le cas échéant.

4.3 Traitement d'une demande de certificat

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

La demande de certificat comporte les éléments mentionnés ci-dessus.

L'A.E. vérifie ensuite l'identité du demandeur conformément aux exigences précédemment décrites. L'AE doit notamment :

- Valider l'identité du futur porteur/Mandataire ;
- Vérifier la cohérence des justificatifs présentés ;
- S'assurer que le futur porteur/Mandataire a pris connaissance des modalités applicables pour l'utilisation du certificat.
- Vérifier que le formulaire de demande de certificat a été bien rempli par le porteur avant de valider la demande.

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat vers la fonction adéquate de l'IGC. L'AE conserve ensuite une trace des justificatifs d'identité présentés :

- Le dossier est au format papier, sous la forme d'une photocopie signée à la fois par le demandeur et par l'A.E., ces signatures étant précédées de la mention « copie certifiée conforme à l'original » ;

4.3.2 Acceptation ou rejet de la demande

En cas de pièces manquantes et après relance quant à la communication de ces pièces, dans un délai de 2 mois, l'Autorité d'Enregistrement se réserve le droit de rejeter la demande de certificat. Il en informe le porteur, le mandataire de certification ou le représentant légal de l'entité par mail et lettre recommandée en justifiant la raison du rejet.

4.3.3 Durée d'établissement du certificat

En cas d'acceptation de la demande, le certificat est établi dans un délai de 7 jours maximum à compter de la remise d'un dossier complet à l'Autorité d'Enregistrement.

4.4 Délivrance du certificat

4.4.1 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 entres les composantes en fonction de l'architecture de l'IGC.

La délivrance du certificat s'effectue en personne avec le porteur/mandataire, moyennant une vérification de la pièce d'identité originale. De plus, le mandataire ne peut accéder à des moyens lui permettant d'activer et d'utiliser la clé privée associée à la clé publique contenue dans le certificat délivré au titulaire.

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.

4.4.2 Notification de la délivrance du certificat au porteur

Le porteur reçoit un courrier contenant le code d'activation (PIN) qui l'invite à retirer son support cryptographique auprès du local Damanesign sur présentation d'une pièce d'identité originale comportant une photographie.

Le support cryptographique contenant le certificat est remis en mains propres au porteur ou au mandataire lors d'un face-à- face au sein de Damanesign sur présentation d'une pièce d'identité originale.

L'autorité de certification fait signer une attestation de délivrance (Document Papier) par le porteur ou le mandataire. Par ailleurs, le mandataire ne peut avoir accès à des moyens qui lui permettraient d'activer et d'utiliser la clé privée associée à la clé publique contenue dans le certificat délivré au titulaire.

En cas d'absence de réponse du porteur, l'autorité de certification rappelle le porteur par l'envoie d'une autre lettre recommandée après 3 mois d'absence de porteur et le certificat est révoqué par cette autorité.

4.5 Acceptation du certificat

4.5.1 Démarche d'acceptation du certificat

Le porteur ou le mandataire doit vérifier que les informations qui sont inscrites sur le certificat sont conformes à ses données personnelles suite à cela il signe l'attestation d'acceptation du certificat pour prendre possession du support cryptographique.

Vérification que le certificat est bien associé à la clé privée correspondante et acceptation explicite du certificat par le porteur.

L'attestation d'acceptation du certificat est renvoyée à l'AC qui la conserve.

4.5.2 Publication du certificat

Les certificats ne sont pas publiés par l'AC.

4.5.3 Notification aux autres entités de la délivrance du certificat

Seules l'AC et l'AE sont notifiées de la délivrance du certificat.

4.6 Usages de la bi-clé et du certificat

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

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la signature de documents. Les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

Cet usage est indiqué explicitement dans les extensions des certificats.

4.6.2 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.

4.7 Renouvellement d'un certificat

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

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

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des porteurs, et les certificats correspondants, seront renouvelés au minimum tous les deux (2) ans.

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

4.8.1 Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat est à l'initiative du porteur.

L'entité, via son Mandataire le cas échéant, peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un porteur qui lui est rattaché.

4.8.2 Procédure de traitement d'une demande d'un nouveau certificat

Le traitement d'une demande d'un nouveau certificat suit la même procédure que pour une demande initiale. Voir 3.2.

4.8.3 Notification au porteur de l'établissement du nouveau certificat

Voir 4.4.2.

4.8.4 Démarche d'acceptation du nouveau certificat

Voir4.5.1

4.8.5 Publication du nouveau certificat

Voir 4.5.2.

4.8.6 Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Voir 4.5.3.

4.9 Modification du certificat

La modification du certificat n'est pas autorisée.

4.10 Révocation et suspension des certificats

4.10.1 Causes possibles d'une révocation

4.10.1.1 Certificats de signature

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

- Les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat
- Le porteur n'a pas respecté les modalités applicables d'utilisation du certificat
- La clé privée du porteur est suspectée de compromission, est compromise, est perdue ou est volée
- Le porteur ou une entité autorisée demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du porteur ou de son support)
- Le décès du porteur ou la cessation d'activité de l'entité du porteur
- Rupture technologique, nécessitant de procéder à la génération de nouveaux bi-clés (longueurs des clés trop faibles, algorithmes de hachage compromis)
- La modification du statut du support cryptographique fournie à l'utilisateur survenant avant la fin de la période de validité du certificat.
- Conformément à la Politique de Certification, le PSCo révoquera tout certificat non expiré qui ne respecte plus les critères énoncés dans ladite politique.

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

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

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

4.10.2 Origine d'une demande de révocation

4.10.2.1 Certificats de signature

Les personnes pouvant demander une révocation de certificat de signature sont :

- Le porteur au nom duquel le certificat a été émis
- Le mandataire
- Un représentant légal de l'entité
- L'AC émettrice du certificat ou l'une de ses composantes (AE)

Le porteur est informé des personnes et entités susceptibles d'effectuer une demande de révocation pour son certificat.

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

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

4.10.3 Procédure de traitement d'une demande de révocation

4.10.3.1 Révocation d'un certificat de signature

Les exigences d'identification et de validation d'une demande de révocation sont décrites au 3.3.

La procédure de révocation de certificats d'un porteur est décrite Procédure de révocation de certificat.

Le porteur de certificat peut révoquer le certificat à tout moment, en se connectent au guichet électronique de Damanesign « https://guichet.damanesign.ma », sur la page de révocation qui est consacré à l'effectuation des révocations du certificat en ligne après validation de Captcha.

Il Renseigne l'adresse courriel et le CIN du porteur de certificat pour s'identifier et Il devra saisir les réponses aux questions secrètes afin de s'authentifier ;

Par la suite le porteur devra choisir le numéro CSN correspondant au certificat à révoquer ainsi il devra indiquer la raison de révocation.

Quand l'opération de révocation est réalisée, le porteur sera notifié par courriel.

Le porteur du certificat a la possibilité aussi de contacter le département de Révocation de Damanesign sur le numéro suivant +212 5 37 68 68 01 qui est joignable et disponible les heures ouvrés. Le porteur doit donner son nom, son prénom, son CIN, et son courriel. Ensuite il va devoir répondre à une série de questions qui seront posées par l'équipe Damanesign afin de s'assurer de son identité.

Le mandataire peut révoquer le certificat d'un porteur par courrier à l'adresse :

4 RUE OUED ZIZ 3 ÉME ÉTAGE APPT 7 AGDAL, 10080 – RABAT.

Le service de révocation Damanesign procède à vérifier l'identité du mandataire et du certificat à révoquer.

Un courriel de confirmation est envoyé au mandataire et au porteur notifiant la révocation effective du certificat.

4.10.3.2 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.

4.10.4 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.

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

4.10.5.1 Révocation d'un certificat de signature

Toute demande de révocation est traitée en urgence.

Il s'écoule au maximum vingt-quatre (24) heures entre la demande de révocation par le porteur et la publication de la nouvelle L.C.R. prenant en compte cette demande.

La L.C.R. est mise à jour quotidiennement et publiée via HTTP.

Toute L.C.R. est publiée dans un délai moins de 30 minutes après sa génération.

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

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

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.

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

L'utilisateur d'un certificat 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 ou son service OCSP 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.

4.10.7 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 30 minutes et une durée maximale totale d'indisponibilité par mois inférieure à 2 heures.

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

L'utilisateur d'un certificat de porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. Cf. chapitre 4.10.6 ci-dessus.

4.10.9 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.10.10 Exigences spécifiques en cas de compromission de la clé privée

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

4.10.11 Suspension de certificats

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

4.11 Fonction d'information sur l'état des certificats

4.11.1 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 2.2, et à l'adresse contenue dans les certificats émis.

Le service OCSP (limité au statut de révocation des certificats de porteurs) est disponible à l'adresse http://ocsp.damanesign.ma/ca_qsig, qui est aussi indiquée dans les certificats émis.

4.11.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats (CRL et OCSP) 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 30 min et une durée maximale totale d'indisponibilité par mois de 2 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.

4.11.3 Séquestre de clé et recouvrement

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

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physique

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

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

5.1.1 Accès physique

L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la 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).

5.1.2 Alimentation électrique et climatisation

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

5.1.3 Vulnérabilité aux dégâts des eaux

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

5.1.4 Prévention et protection incendie

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

5.1.5 Conservation des supports

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

5.1.6 Mise hors service des supports

Les supports papiers et magnétiques en fin de vie sont systématiquement détruits par des moyens appropriés, permettant d'éviter toute perte de confidentialité. Les dossiers

d'enregistrement devront êtreconservés au moins pendant la durée de validité du certificat d'entité (en cas de renouvellement, la durée sera prolongée)

5.1.7 Sauvegardes hors site

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

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

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

Responsable de sécurité : Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc.

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.

5.2.2 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, il est demandé de répartir les fonctions sensibles sur plusieurs personnes.

5.2.3 Identification et authentification pour chaque rôle

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

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

5.2.4 Rôles exigeant une séparation des attributions

Les cumuls suivants sont interdits :

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

5.3 Mesures de sécurité vis à vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

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

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

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

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

5.3.2 Procédures de vérification des antécédents

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

5.3.3 Exigences en matière de formation initiale

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

5.3.4 Exigences en matière de formation continue et fréquences des formations

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

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

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

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

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

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

5.3.8 Documentation fournie au personnel

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

5.4 Procédures de constitution des données d'audit

5.4.1 Type d'événement à enregistrer

Les événements suivants sont enregistrés :

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

Ces journaux permettent d'assurer la traçabilité et l'imputabilité des actions effectuées, en particulier en cas de demande émanant d'une autorité judiciaire ou administrative. L'AC décrit dans ses procédures internes le détail des évènements 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.

5.4.2 Fréquence de traitement des journaux d'événements

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

5.4.3 Période de conservation des journaux d'événements

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

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

5.4.4 Protection des journaux d'événements

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

5.4.5 Procédure de sauvegarde des journaux d'événements

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

5.4.6 Système de collecte des journaux d'événements

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

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

Sans objet.

5.4.8 Évaluation des vulnérabilités

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

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

5.5 Archivage des données

5.5.1 Types de données à archiver

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

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

Les données à archiver sont au moins les suivantes :

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

5.5.2 Période de conservation des archives

5.5.2.1 Dossiers de demande de certificat

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

En ce qui concerne les certificats de l'AC, les dossiers d'enregistrement (demandes de certificats) sont archivés pendant 12 ans au minimum 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 12 ans après leur expiration.

5.5.2.2 Journaux d'événements et autres

La durée minimale d'archivage des journaux d'événements et autres est de 12 ans après l'événement.

5.5.3 Protection des archives

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

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

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

5.5.4 Procédure de sauvegarde des archives

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

5.5.5 Exigences d'horodatage des données

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

5.5.6 Système de collecte des archives

La 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.

5.6 Procédures de récupération et de vérification des archives

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

L'A.C. ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'A.C. Pour cela la période de validité de ce certificat de l'A.C. doit être supérieure à celle des certificats qu'elle signe. Au regard de la date de fin de validité de ce certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'A.C. est générée, seule la nouvelle clé privée doit être utilisée pour signer des certificats. Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce au moins jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7 Changement de clé d'AC

La période de validité de la clé de l'AC est de 30 ans.

La durée de vie des certificats Porteur est (2) ans, le renouvellement de cette clé devra intervenir au plus tard (2) ans avant la fin de sa validité. L'AC se réserve la possibilité de la renouveler avant sa limite de validité. La décision de son renouvellement pourra être prise plus tôt en fonction de divers critères (évolution de la technique cryptographique, allongement de la longueur, …).

La nouvelle bi-clé générée servira à signer les nouveaux Certificats Porteurs émis ainsi que la LCR.

Le certificat précédent restera utilisable pour la validation de certificats émis avant le renouvellement et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.8 Reprise suite à compromission et sinistre

Chaque entité opérant une composante de l'IGC doit met 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.

5.8.1 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'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. L'AC

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

5.8.2 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.

5.8.3 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'A.C. ou de compromission des algorithmes et des paramètres utilisés pour générer les clés privées correspondant aux certificats, ceux-ci doivent être immédiatement révoqués.

En cas de compromission des clés privées ou de compromission des algorithmes et des paramètres utilisés pour générer les clés privées correspondant aux certificats d'entité finale, tous les certificats d'abonnés associés sont révoqués par l'autorité de certification et de nouvelles clés et certificats sont délivrés sans interruption du service.

Suite à la révocation du certificat correspondant, toute service sur l'état de certificat n'est plus valide.

5.8.4 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).

5.9 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.

L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

5.9.1 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 évènements, l'A.C. prend les mesures suivantes :

- Communiquer au point de contact identifié au sein de la DGSSI les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité.
- Mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats) ;
- Elle assure la continuité du service de Révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC. A défaut, les applications de l'administration refuseront les certificats émis par des ACs dont les LCRs en cours de validité ne seraient plus accessibles, même si le certificat du porteur est encore valide.
- Elle prévient les Mandataires de Certification / porteurs dans le cas où les changements envisagés peuvent avoir des répercussions sur les engagements pris.
- Tenir informée la DGSSI de tout obstacle ou délai non prévu rencontrés dans le déroulement du processus.
- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des porteurs ou des utilisateurs de certificats, l'AC doit les en aviser aussitôt que nécessaire sous le délai (1 mois).
- Communiquer avant une date donnée son intention de transfert d'activité ;
- Mettre en œuvre tous les moyens dont elle dispose pour informer ses partenaires (utilisateurs finaux, les abonnés, les parties prenantes, autres composantes, autres IGC, etc.) de ses intentions de fin d'activité.
- Transférer les obligations (fourniture de services de confiance) à un tiers fiable identifié.

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

5.9.2 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.

Damanesign 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.

Damanesign communiquera à la D.G.S.S.I., selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. Damanesign mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Damanesign 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
- Tous les mandataires de certification, porteurs, utilisateur de certificat, les parties prenantes, responsables des certificats révoqués ou à révoquer seront tenus informés.

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.

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

De plus, en cas de fin de vie de l'AC, notamment dans le cas d'une suspicion de compromission de la clé privée de l'AC, les opérations suivantes sont réalisées :

- Arrêt immédiat de la production des certificats finaux concernés
- Révocation au plus tôt de tous les certificats finaux restants émis par l'AC concernée
- Production d'une dernière LCR par l'AC avant sa révocation :
- Damanesign s'engage suite à cela à générer une dernière LCR (contenant donc tous les numéros de série des certificats qu'elle a produits et qu'elle a révoqués depuis son début d'activité) dont la date d'expiration est positionnée au 31 décembre 9999.
- Prégénération de toutes les réponses OCSP des certificats émis avec une date de fin de validité positionnée au 31 décembre 9999, 23h59m59s (« 99991231235959Z »)
- Génération d'une nouvelle LAR et suppression de toutes les LAR prégénérées (s'il en existe) Publication de la dernière LCR de l'AC concernée et publication de la LAR à jour

6 Mesures de sécurité techniques

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

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés de l'A.C.

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

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

6.1.1.2 Clés porteurs générées par l'A.C.

La génération des clés des porteurs est effectuée dans un environnement sécurisé.

Les bi-clés des porteurs sont générées directement dans le dispositif de création de signature destiné au porteur.

6.1.1.3 Clés ocsp générées par l'A.C.

La génération des clés des certificats de service OCSP est effectuée dans un environnement sécurisé.

6.1.2 Transmission de la clé privée à son propriétaire

La clé privée, résidant dans le dispositif de création de signature, est transmise au porteur en même temps que celui-ci (remise en mains propres, voir 4.5).

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

Sans objet.

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

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

6.1.5 Tailles des clés

La clé RSA de l'A.C. Racine a une taille de 4096 bits.

Les clés RSA des A.C. filles ont une taille de 4096 bits.

Les clés RSA des certificats de signature ont une taille de 2048 bits.

Les clés des certificats OCSP ont ces caractéristiques :

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

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

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

6.1.7 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).

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'A.C.

L'A.C. s'assure que :

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

Les dispositifs de création de la signature, pour la mise en œuvre des clés privées d'A.C., respectent les exigences du chapitre 9 ci-dessous.

6.2.1.2 Dispositifs de création de signature des porteurs

Les dispositifs de création de signature, pour la mise en œuvre de leurs clés privées, respectent les exigences du chapitre 11 ci-dessous.

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

Voir 6.2.2 de la DPC.

6.2.3 Contrôle de la clé privée du porteur par plusieurs personnes

Voir 6.2.3 de la DPC.

6.2.4 Séquestre de la clé privée

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

6.2.5 Copie de secours de la clé privée

Les clés privées des porteurs ne font l'objet d'aucune copie de secours par l'AC.

6.2.6 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.

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

Pour les clés privées d'A.C., tout transfert doit se faire sous forme chiffrée, conformément aux exigences du chapitre 6.2.5.

6.2.8 Stockage de la clé privée dans un module cryptographique

Voir ci-après.

6.2.9 Méthode d'activation de la clé privée

6.2.9.1 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.* 6.2.9) et doit faire intervenir au moins trois personnes dans des rôles de confiance.

6.2.9.2 Clés privées des porteurs

L'activation des clés privées des porteurs est contrôlée via des données d'activation sous la responsabilité du porteur (code PIN).

6.2.10 Méthode de désactivation de la clé privée

6.2.10.1 Clés privées d'A.C.

La désactivation des clés privées d'A.C. dans un module cryptographique doit être automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc. Une clé privée d'A.C. peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation doivent permettre de répondre aux exigences définies dans le chapitre 9.

6.2.10.2 Clés privées des porteurs

La désactivation de la clé privée du porteur est effectuée de façon à garantir que la clé privée, contenue dans le support matériel, est toujours sous le contrôle du porteur.

6.2.11 Méthode de destruction des clés privées

6.2.11.1 Clés privées d'A.C.

La méthode de destruction des clés privées d'A.C. doit permettre de répondre aux exigences définies dans le chapitre 11. En fin de vie d'une clé privée d'A.C., normale ou anticipée (révocation), cette clé doit être systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.11.2 Clés privées des porteurs

La destruction de sa clé privée par le porteur est de son ressort. Ce dernier s'engage à assurer la sécurité des conditions de destruction dont il est propriétaire.

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

Ces exigences sont précisées au chapitre 9.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

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

6.3.2 Durées de vie des bi-clés et des certificats

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

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

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

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

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

L'A.C. transmet au porteur les données d'activation de sa clé par un canal séparé dans le temps et dans l'espace de la remise de la clé privée : le code PIN sera envoyé par courrier recommandé à l'utilisateur en invitant le Porteur à récupérer le Support chez Damanesign.

Le porteur doit obligatoirement modifier le code PIN d'activation de la clé privée lors de sa première utilisation.

6.4.2 Protection des données d'activation

Les données d'activation des dispositifs de création de signature des porteurs générées par l'AC sont protégées en intégrité et en confidentialité jusqu'à la remise aux porteurs. Ces données ne sont pas sauvegardées par l'AC.

6.5 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 paramétrages du système (en particulier des éléments de routage) sont mis en place.

6.6 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.

6.7 Mesures de sécurité réseau

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

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

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

6.8 Horodatage / Système de datation

Pour dater les évènements, 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 évènements avec une précision suffisante.

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

7.1 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 = 154609`
	`O = Damanesign`
	`C = MA`

Validity	30 ans

Subject	`C=MA`
	`O=Damanesign`
	`OI=NTRMA-154609`
	`OU=154609`
	`CN=Damanesign Qualified Signature CA`

Subject Public Key Info	RSA 4096 bits

Champ	Criticité	Général
Authority Key Identifier	N	Contient l'identifiant de clé de la clé publique de l'AC émettrice (champ *Subject Key Identifier* du certificat de l'AC émettrice). Méthode 1 définie dans la RFC 5280, § 4.2.1.2.
Subject Key Identifier	N	Identifiant de la clé du sujet (AC) Méthode 1 définie dans la RFC 5280, § 4.2.1.2.
Key Usage	O	`keyCertSign, CRLSign`
Basic Constraints	O	`CA : TRUE` `pathlen :0`
Certificate Policies	N	anyPolicy (2.5.29.32.0) PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1) http://pki.damanesign.ma/cps.html
Subject Alternative Name ***Issuer Alternative Name***	N	Non utilisée
CRL Distribution Points	N	`http://pki.damanesign.ma/crl/ca_root_2024.crl`
Authority Information Access	N	`CA:` `http://pki.damanesign.ma/cert/ca_root_2024.crt`

7.2 Certificat de signature (1.3.6.1.4.1.58553.1.3.1.3)

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 3.1.2.1
Validity	2 ans
Subject	Voir 3.1.2.2
Subject Public Key Info	RSA 2048 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.

Champ	Criticité	Général
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	nonRepudiation[1]
Basic Constraints	O	CA: FALSE
Certificate Policies	N	OID: 1.3.6.1.4.1.58553.1.3.1.3 CPS: https://pki.damanesign.ma/cps.html
Subject Alternative Name	N	(Optionnel) RFC822NAME : ‹ Courriel de la personne ›
Issuer Alternative Name	N	Non utilisé
CRL Distribution Points	N	http://pki.damanesign.ma/crl/ca_qsig_2024.crl
Authority Information Access	N	CA:http://pki.damanesign.ma/cert/ca_qsig_2024.crt OCSP : http://ocsp.damanesign.ma/ca_qsig

Champ	Criticité	Général
Qc Compliance	N	id-etsi-qcs 1
QcSSCD	N	id-etsi-qcs 4
QcType	N	id-etsi-qct-esign

7.3 Liste de Certificats Révoqués

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Signature	sha256WithRSAEncryption
Issuer	C=MA O=Damanesign OI=NTRMA-154609 OU=154609 CN=Damanesign Qualified Signature CA
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*)
ExpiredCertsOnCRL	Date à partir de laquelle tous les certificats révoqués sont conservés dans la CRL. Il s'agit de la date de début de validité du certificat de l'AC émettrice.
Numéro de LCR	Entier
AuthorityKeyIdentifier	Identifiant de la clé de l'A.C.

7.4 Certificats du service OCSP

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Signature	sha256WithRSAEncryption
Issuer	C=MA

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

	O=Damanesign OI=NTRMA-154609 OU=154609 CN=Damanesign Qualified Signature CA
thisUpdate	Date et heure UTC
nextUpdate	Date et heure UTC (2 ans de validité)
Numéro de série	Défini par l'outil et comprenant une part aléatoire
Longueur des clés	2048 bits
Key Usage	Digital Signature
Extended Key Usage	id-kp-OCSPSigning
Basic Constraints	"CA:false"
Subject Alternative Name	Un ou plusieurs noms de domaine contrôlés par le demandeur

7.5 Répondeur OCSP

7.5.1 Requêtes OCSP

Les requêtes OCSP acceptées sont celles qui respectent le format décrit par la RFC 6960.
Le service OCSP ignore la signature si elle est présente.
Les requêtes attendues sont de la forme :

Champ	Commentaires	Valeur attendue
Version	Version de la requête	0 (version 1)
requestorName	Nom de l'émetteur de la requête	Valeur absente ou ignorée
requestList • **ReqCert** • **SingleRequest Extensions**	Liste des certificats à vérifier	Un ou plusieurs identifiants de certificats sont acceptés. La valeur des extensions est ignorée
requestExtensions	Extensions	Seule l'extension Nonce est prise en compte, les autres sont ignorées

Les algorithmes d'empreinte acceptés pour les identifiants de certificats sont SHA-256, SHA-384 et SHA-512.

7.5.2 Réponses OCSP

Les réponses OCSP respectent le format décrit par la RFC 6960.
Elles sont signées par le service sauf si une erreur s'est produite (requête rejetée ou échec de traitement).
Les certificats révoqués, même ceux expirés, sont signalés révoqués. Les réponses sont de la forme BasicOCSPResponse :

Champ	Commentaires	Valeur attendue
Version	Version de la requête	0 (version 1)
responderID	Nom du répondeur	Hash de la clé publique du répondeur
producedAt	Heure de production de la réponse	Heure de production à la seconde près
responses – **certID** – **certStatus**	Statut des certificats identifiés dans la requête	Le statut du certificat est le statut actuel du certificat (thisUpdate est la date

– **revocationDate** – **ThisUpdate** – **Next Update** – **Archive Cutoff**		courante). La date de révocation est fournie le cas échéant, mais pas la raison de révocation, Date de début de validité du certificat de l'AC (Autorité de Certification)

8 Audits de conformité et évaluations

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.

8.1 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 PSCo doit procéder à un contrôle de conformité de cette composante. L'A.C. doit également procéder régulièrement à un contrôle de conformité de l'ensemble de son I.G.C., une fois par an.

8.2 Identités / qualifications des évaluateurs

Le contrôle d'une composante 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.

8.3 Relations entre évaluateurs et entités évaluées

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

8.4 Sujets couverts par les évaluations

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

8.5 Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend au PSCo , 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.

8.6 Communication des résultats

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

9 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

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

9.1.2 Tarifs pour accéder aux certificats

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

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

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

9.1.4 Tarifs pour d'autres services

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

9.1.5 Politique de remboursement

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

9.2 Responsabilité financière

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

9.3 Confidentialité des données

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :

- La 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.

9.3.2 Informations hors du périmètre des informations confidentielles

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

9.3.3 Responsabilités en termes de protection des informations confidentielles

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

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

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

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

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

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

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

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

9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

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

9.4.3 Informations à caractère non personnel

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

9.4.4 Responsabilité en termes de protection des données personnelles

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

9.4.5 Notification et consentement d'utilisation des données personnelles

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

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

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

9.4.7 Autres circonstances de divulgation d'informations personnelles

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

9.5 Droits sur la propriété intellectuelle et industrielle

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

9.6 Interprétations contractuelles et garanties

Sans objet.

9.7 Limite de garantie

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

9.8 Limite de responsabilité

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

9.9 Indemnités

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

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

9.10.1 Durée de validité

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

9.10.2 Fin anticipée de validité

Sans objet

9.10.3 Effets de la fin de validité et clauses restant applicables

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

9.11 Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'I.G.C., l'A.C. devra :

- Au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'A.C. et de ses différentes composantes.
- Au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

9.12 Amendements à la P.C.

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

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.

9.13 Dispositions concernant la résolution de conflits

Damanesign a mis en place des politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles il fournit des services électroniques de confiance ou d'autres points qui y sont liés.

9.14 Juridictions compétentes

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

9.15 Conformité aux législations et réglementations

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

9.16 Transfert d'activités

Cf. section 5.9.

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

10.1 Exigences sur les objectifs de sécurité

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

- Si les bi-clés de signature des porteurs sont générées par ce module, garantir que ces générations sont réalisées exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées
- Si les bi-clés de signature des porteurs sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques des porteurs lorsqu'elles sont sous la responsabilité de l'A.C. et pendant leur transfert vers le dispositif de création de signature du porteur et assurer leur destruction sûre après ce transfert
- Assurer la confidentialité et l'intégrité des clés privées de signature de l'A.C. durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie
- Être capable d'identifier et d'authentifier ses utilisateurs
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné
- Être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur
- Permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'A.C., qui ne révèle pas les clés privées de l'A.C. et qui ne peut pas être falsifiée sans la connaissance de ces clés privées
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité
- Si une fonction de sauvegarde et de restauration des clés privées de l'A.C. est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

11 Annexe 2 : Exigences sur les objectifs de sécurité du dispositif de création de signature

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

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