Politique de certification et Déclaration des pratiques de certification (PC/DPC) De l'Autorité de certification Damanesign -Signature Simple-

Version 1.0 | Diffusion : public

OID n° 1.3.6.1.4.1.58553.1.7.2.1

Ce document est la propriété exclusive de Damanesign

Historique du document

Version	Date de version	Rédacteur(s)	Approbateur(s)	Modifications
1.0	15/10/2024	Fatimazahrae Jalal	Zouhair HAMDAOUI	Création du document
1.1	05/11/2024	Fatimazahrae Jalal	Zouhair HAMDAOUI	Modifications OID

1 INTRODUCTION 8
1.1 Présentation générale 8
1.2 Identification du document 8
1.3 Entités intervenant dans l'I.G.C. et responsabilités 9
1.3.1 Le Prestataire de services de certification électronique 9
1.3.2 Autorité de certification 9
1.3.3 Autorité d'enregistrement 11
1.3.4 Porteurs de certificats 11
1.3.5 Utilisateurs de certificat 11
1.4 Usage des certificats 12
1.4.1 Domaines d'utilisation applicables 12
1.4.2 Domaines d'utilisation interdits 12
1.5 Gestion de la P.C. 12
1.5.1 Entité gérant la P.C. 12
1.5.2 Point de contact 12
1.5.3 Procédures d'approbation de la conformité de la P.C. / D.P.C. 12
1.6 Définitions et sigles 13
1.6.1 Sigles 13
1.6.2 Définitions 13
2 RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIÉES 16
2.1 Entités chargées de la mise à disposition des informations 16
2.2 Informations devant être publiées 16
2.2.1 Publication du certificat d'AC 16
2.2.2 Publication de la CRL 16
2.3 Délais et fréquences de publication 16
2.4 Contrôle d'accès aux informations publiées 17
2.5 Notification en cas de changement de la DPC, PC et CGU 17
3 IDENTIFICATION ET AUTHENTIFICATION 18
3.1 Nommage 18
3.1.1 Types de noms 18
3.1.2 Nécessité d'utilisation de noms explicites 18
3.1.3 Pseudonymisation des porteurs 18
3.1.4 Règles d'interprétation des différentes formes de nom 18
3.1.5 Unicité des noms 19
3.1.6 Identification, authentification et rôle des marques déposées 19
3.1.7 Validation initiale de l'identité 19
3.1.8 Méthode pour prouver la possession de la clé privée 19
3.1.9 Validation de l'identité d'un organisme 19
3.1.10 Validation de l'identité d'un individu 19
3.1.11 Informations non vérifiées du porteur 19
3.1.12 Validation de l'autorité du demandeur 20
3.1.13 Certification croisée d'A.C. 20
3.2 Identification et validation d'une demande de renouvellement des clés 20
3.2.1 Identification et validation pour un renouvellement courant 20
3.2.2 Identification et validation pour un renouvellement après révocation 20
3.3 Identification et validation d'une demande de révocation 20
4 EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS 21
4.1 Origine de Demande de certificat 21

4.2 Processus et responsabilités pour l'établissement d'une demande de certificat 21
4.3 Traitement d'une demande de certificat 21
4.3.1 Exécution des processus d'identification et de validation de la demande 21
4.3.2 Acceptation ou rejet de la demande 21
4.3.3 Durée d'établissement du certificat 21
4.4 Délivrance du certificat 21
4.4.1 Actions de l'A.C. concernant la délivrance du certificat 21
4.4.2 Notification de la délivrance du certificat au porteur 22
4.5 Acceptation du certificat 22
4.5.1 Démarche d'acceptation du certificat 22
4.5.2 Publication du certificat 22
4.6 Usages de la bi-clé et du certificat 22
4.6.1 Utilisation de la clé privée et du certificat par le porteur 22
4.6.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat 22
4.7 Renouvellement d'un certificat 22
4.8 Délivrance d'un nouveau certificat à la suite du changement de la bi-clé 23
4.8.1 Origine d'une demande d'un nouveau certificat 23
4.8.2 Procédure de traitement d'une demande d'un nouveau certificat 23
4.8.3 Notification au porteur de l'établissement du nouveau certificat 23
4.8.4 Démarche d'acceptation du nouveau certificat 23
4.8.5 Publication du nouveau certificat 23
4.9 Modification du certificat 23
4.10 Révocation et suspension des certificats 23
4.10.1 Causes possibles d'une révocation 23
4.10.2 Origine d'une demande de révocation 24
4.10.3 Procédure de traitement d'une demande de révocation 24
4.10.4 Délai accordé au porteur pour formuler la demande de révocation 25
4.10.5 Délais de traitement par l'A.C. d'une demande de révocation 25
4.10.6 Exigences de vérification de la révocation par les utilisateurs de certificats 25
4.10.7 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats 25
4.10.8 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats 25
4.10.9 Autres moyens disponibles d'information sur les révocations 25
4.10.10 Exigences spécifiques en cas de compromission de la clé privée 25
4.10.11 Suspension de certificats 26
4.11 Fonction d'information sur l'état des certificats 26
4.11.1 Caractéristiques opérationnelles 26
4.11.2 Disponibilité de la fonction 26
4.11.3 Séquestre de clé et recouvrement 26
5 Mesures de sécurité non techniques 27
5.1 Mesures de sécurité physique 27
5.1.1 Situation géographique et construction des sites 27
5.1.2 Accès physique 27
5.1.3 Alimentation électrique et climatisation 28
5.1.4 Vulnérabilités aux dégâts des eaux 28
5.1.5 Prévention et protection incendie 28
5.1.6 Conservation des supports 28
5.1.7 Mise hors de service des supports 28

5.1.8 Sauvegardes hors site 28
5.2 Mesures de sécurité procédurales 28
5.2.1 Rôles de confiance 28
5.2.2 Nombre de personnes requises par tâches 29
5.2.3 Identification et authentification pour chaque rôle 29
5.2.4 Rôles exigeant une séparation des attributions 30
5.3 Mesures de sécurité vis à vis du personnel 30
5.3.1 Qualifications, compétences et habilitations requises 30
5.3.2 Procédures de vérification des antécédents 30
5.3.3 Exigences en matière de formation initiale 30
5.3.4 Exigences en matière de formation continue et fréquences des formations 30
5.3.5 Fréquence et séquence de rotation entre différentes attributions 31
5.3.6 Sanctions en cas d'actions non autorisées 31
5.3.7 Exigences vis-à-vis du personnel des prestataires externes 31
5.3.8 Documentation fournie au personnel 31
5.4 Procédures de constitution des données d'audit 31
5.4.1 Type d'événement à enregistrer 31
5.4.2 Fréquence de traitement des journaux d'événements 32
5.4.3 Période de conservation des journaux d'événements 32
5.4.4 Protection des journaux d'événements 32
5.4.5 Procédure de sauvegarde des journaux d'événements 33
5.4.6 Système de collecte des journaux d'événements 33
5.4.7 Notification de l'enregistrement d'un événement au responsable de l'événement 33
5.4.8 Évaluation des vulnérabilités 33
5.5 Archivage des données 33
5.5.1 Types de données à archiver 33
5.5.2 Période de conservation des archives 33
5.5.3 Protection des archives 33
5.5.4 Procédure de sauvegarde des archives 34
5.5.5 Exigences d'horodatage des données 34
5.5.6 Système de collecte des archives 34
5.6 Procédures de récupération et de vérification des archives 34
5.7 Changement de clé d'AC 34
5.8 Reprise suite à compromission et sinistre 34
5.8.1 Procédures de remontée et de traitement des incidents et des compromissions 34
5.8.2 Procédures de reprise en cas de sinistre 35
5.8.3 Procédures de reprise en cas de compromission de la clé privée d'une composante 35
5.8.4 Capacités de continuité d'activité suite à un sinistre 35
5.9 Fin de vie de l'I.G.C. 35
5.9.1 Transfert d'activité ou cessation d'activité 35
5.9.2 Cessation d'activité affectant l'activité de l'A.C. 36
6 Mesures de sécurité techniques 37
6.1 Génération et installation de bi-clés 37
6.1.1 Génération des bi-clés 37
6.1.2 Transmission de la clé privée à son propriétaire 37
6.1.3 Transmission de la clé publique à l'A.C. 37
6.1.4 Transmission de la clé publique de l'A.C. aux utilisateurs de certificats 37
6.1.5 Tailles des clés 37
6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité 37

6.1.7 Objectifs d'usage de la clé 38
6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques 38
6.2.1 Standards et mesures de sécurité pour les modules cryptographiques 38
6.2.2 Contrôle de la clé privée de l'A.C. par plusieurs personnes 38
6.2.3 Séquestre de la clé privée 38
6.2.4 Copie de secours de la clé privée 38
6.2.5 Archivage de la clé privée 38
6.2.6 Transfert de la clé privée vers / depuis le module cryptographique 38
6.2.7 Stockage de la clé privée dans un module cryptographique 39
6.2.8 Méthode d'activation de la clé privée 39
6.2.9 Méthode de désactivation de la clé privée 39
6.2.10 Méthode de destruction des clés privées 39
6.3 Autres aspects de la gestion des bi-clés 40
6.3.1 Archivage des clés publiques 40
6.3.2 Durées de vie des bi-clés et des certificats 40
6.4 Données d'activation 40
6.4.1 Génération et installation des données d'activation 40
6.4.2 Protection des données d'activation 40
6.5 Mesures de sécurité des systèmes informatiques 41
6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques 41
6.5.2 Niveau d'évaluation sécurité des systèmes informatiques 41
6.6 Mesures de sécurité liées au développement des systèmes 41
6.7 Mesures de sécurité réseau 41
6.8 Horodatage / Système de datation 42
7 Profils des certificats et des L.C.R. 43
7.1 Certificats de l'A.C. 43
7.2 Certificat de signature (1.3.6.1.4.1.58553.1.7.2.1) 43
7.3 Liste de Certificats Révoqués 44
8 Audits de conformité et évaluations 45
8.1 Fréquences et circonstances des évaluations 45
8.2 Identités / qualifications des évaluateurs 45
8.3 Relations entre évaluateurs et entités évaluées 45
8.4 Sujets couverts par les évaluations 45
8.5 Actions prises suite aux conclusions des évaluations 45
8.6 Communication des résultats 45
9 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES 46
9.1 Tarifs 46
9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats 46
9.1.2 Tarifs pour accéder aux certificats 46
9.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats 46
9.1.4 Tarifs pour d'autres services 46
9.1.5 Politique de remboursement 46
9.2 Responsabilité financière 46
9.3 Confidentialité des données 46
9.3.1 Périmètre des informations confidentielles 46
9.3.2 Informations hors du périmètre des informations confidentielles 46
9.3.3 Responsabilités en termes de protection des informations confidentielles 46
9.4 Protection des données personnelles 47

9.4.1 Politique de protection des données personnelles 47
9.4.2 Informations à caractère personnel 47
9.4.3 Informations à caractère non personnel 47
9.4.4 Responsabilité en termes de protection des données personnelles 47
9.4.5 Notification et consentement d'utilisation des données personnelles 47
9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives 47
9.4.7 Autres circonstances de divulgation d'informations personnelles 48
9.5 Droits sur la propriété intellectuelle et industrielle 48
9.6 Interprétations contractuelles et garanties 48
9.7 Limite de garantie 48
9.8 Limite de responsabilité 48
9.9 Indemnités 48
9.10 Durée et fin anticipée de validité de la P.C. 48
9.10.1 Durée de validité 48
9.10.2 Fin anticipée de validité 48
9.10.3 Effets de la fin de validité et clauses restant applicables 48
9.11 Notifications individuelles et communications entre les participants 48
9.12 Amendements à la P.C. 48
9.13 Dispositions concernant la résolution de conflits 49
9.14 Juridictions compétentes 49
9.15 Conformité aux législations et réglementations 49
9.16 Transfert d'activités 49
10 Annexe 1 : Exigences de sécurité du module cryptographique de l'A.C. 50
10.1 Exigences sur les objectifs de sécurité 50

1 INTRODUCTION

1.1 Présentation générale

Le document intitulé "Politique de certification et Déclaration des pratiques de certification (PC/DPC) De l'Autorité de certification Damanesign pour la Signature Simple" expose les pratiques que la société DAMANESIGN applique dans le cadre de la fourniture de certificats de signature.

Dans le cadre de son offre de services de confiance, Damanesign fournit un service de génération et de délivrance des Certificats pour la signature simple, délivrés par une Autorité de Certification appartenant à l'Infrastructure de Gestion de Clés (IGC) Damanesign.

Une demande de génération de Certificat est effectuée par un Client pour une personne physique, appelée Signataire, qui sera le porteur du Certificat délivré.

Cette Autorité de Certification est dénommée « Damanesign Signature CA » et sera nommée

« AC » dans le reste du document.

L'AC est délivrée par l'Autorité de Certification racine « Damanesign ROOT CA ».

1.2 Identification du document

Le présent document est dénommé Politique de certification et Déclaration des pratiques de certification des certificats de signature simple. 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 du présent document est : 1.3.6.1.4.1.58553.1.7.2.1

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

- Produire des certificats de signature simple ;
- Produire des Listes des Certificats Révoqués (LCR) ;

Lorsque Damanesign a l'intention d'apporter des changements à ses pratiques qui pourraient affecter l'acceptation du service par le sujet, l'abonné ou les parties qui se fient au service,

Damanesign doit dûment informer les abonnés ou les parties qui se fient au service des changements en publiant les pratiques mises à jour ;

Damanesign met rapidement à jour les pratiques et les politiques, chaque nouvelle version des documents étant approuvée par la direction et publiée sur le site web de la société ;

Damanesign publie sans délai chaque nouvelle édition de ses pratiques et politiques applicables.

Les Conditions générales relatives aux Services sont disponibles sur le site web Damanesign (https://pki.damanesign.ma/#1-CGU).

Les Abonnés ou les Utilisateurs devront lire et accepter ces Conditions générales avant de pouvoir utiliser les Services. Les présentes Conditions générales font partie intégrante de l'Accord conclu avec l'Abonné ou l'Utilisateur.

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

1.3.1 Le Prestataire de services de certification électronique

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

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

1.3.2 Autorité de certification

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).

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.).
- 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 et de LCR), 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

Les responsabilités de l'AE dans le cadre de la présente PC/DPC sont les suivantes :

- L'établissement et la transmission de la demande de certificat à la fonction adéquate de l'I.G.C. suivant l'organisation de cette dernière et les prestations offertes,
- L'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage),
- La conservation et la protection en confidentialité et en intégrité des données personnelles des demandeurs de certificats, 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).
- La prise en compte et la vérification des informations du futur porteur et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;

L'AE est gérée et opérée par Damanesign. Elle peut faire l'objet d'une délégation par voie contractuelle au responsable d'une application Métier qui utilise les plateformes Damanesign.
Dans le cas d'une délégation d'une partie et/ou de la totalité de l'AE à un client, les missions et les obligations du client vis-à-vis l'AC Damanesign feront l'objet une convention à part entre les deux parties.

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

L'utilisateur de certificat désigne une personne, responsable d'une application métier en ligne qui utilise des certificats générés par l'AC pour réaliser des signatures électroniques.

1.4 Usage des certificats

L'AC « Damanesign Signature CA » délivre des certificats de signature simple.

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Bi-clés et certificats des porteurs

La clé privée associée au certificat sert pour :

- La signature de document au nom du porteur ;
- Les certificats signature permettent à leurs Porteurs de signer électroniquement en ligne leurs contrats.

1.4.1.2 Bi-clés et certificats d'A.C.

La clé privée associée à la clé publique du certificat de l'AC déléguée est utilisée pour signer :

- Les Certificats des porteurs de certificats ;
- Les LCR ;

1.4.2 Domaines d'utilisation interdits

Les usages autres que ceux listés dans la section 1.4.1 sont interdits.

De plus, les Certificats doivent être utilisés dans la limite des lois et réglementations en vigueur.

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

Les demandes d'informations ou commentaires sur ce document doivent être adressés au responsable de l'IGC à l'adresse suivante :

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 P.C. / D.P.C.

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

L'approbation suit une procédure bien précise. La PC/ DPC est revue régulièrement, au minimum une fois par an, afin :

- D'assurer sa conformité aux normes de sécurité attendues par les applications qui référencent des familles de certificat porteur ;
- De mettre à jour la liste des applications concernées par la PC ;
- De s'adapter aux évolutions technologiques.

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*
IGC	Infrastructure de Gestion de Clés
L.C.R.	Liste des Certificats Révoqués
M.C.	Mandataire de Certification
O.C.	Opérateur de Certification
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
P.C.	Politique de Certification
D.P.C	Déclaration des pratiques de certification
P.S.C.O.	Prestataire de Services de Confiance
D.G.S.S.I.	Direction Générale de la Sécurité des Systèmes d'Informations
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.

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 PSCo 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.

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 autre que 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.

Moyen d'authentification : Moyen connu ou utilisable uniquement par le Signataire pour s'authentifier auprès de l'AE afin d'utiliser le Service de signature pour signer des documents.

Exemples : mot de passe, OTP envoyé par courriel, OTP envoyé par SMS, etc.

Service de signature : Service de confiance de création de signatures et de délivrance de certificats de signature mis à disposition par Damanesign à ses clients pour leur permettre de faire signer des documents à des personnes physiques. Dans le cadre de la présente PC, le Service de signature est une composante de l'AE. Il identifie et authentifie les Signataires afin de leur délivrer un Certificat **de signature simple** dédié à une Transaction de signature particulière.

La Clé Privée du Signataire, associée au Certificat, est générée et utilisée de manière sécurisée par le Service de signature pour signer les documents de la Transaction de signature et est immédiatement détruite une fois les documents signés.

Transaction de signature : Opération de courte durée, gérée par le Service de signature, durant laquelle un Signataire doit s'authentifier auprès de l'AE pour obtenir un Certificat et pouvoir signer électroniquement les documents de cette transaction avec sa Clé Privée associée à son Certificat et opérée par le Service de signature.

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, etc.) sont précisées ci-après.

2.2 Informations devant être publiées

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

- La présente PC/DPC ;
- Les certificats de l'Autorité de Certification « Damanesign Root CA » ;
- La liste des certificats révoqués (LCR) ;
- La liste des autorités révoquées (LAR) ;

Compte tenu de la complexité de lecture d'une PC pour des porteurs ou des utilisateurs de certificats non spécialistes du domaine, il est obligatoire que l'AC publie également des conditions générales d'utilisation (CGU).

2.2.1 Publication du certificat d'AC

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

https://pki.damanesign.ma/CertData/DamaneSign%20signature%20CA.crt

2.2.2 Publication de la CRL

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

http://pki.damanesign.ma/CertData/DamaneSign%20signature%20CA.crl

La CRL est signée par l'AC correspondante

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/DPC Signature) et de Déclaration des Pratiques de Certification (DPC/ PC 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 par un email, Hubspot ou d’autre canal, 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 identités utilisées dans un certificat sont décrites suivant la norme X.500. Dans chaque certificat

X.509, le fournisseur (Issuer) et le porteur (subject) sont identifiés par un Distinguished Name (DN).

3.1.2 Nécessité d'utilisation de noms explicites

3.1.2.1 A.C. Signature

C = MA	Pays
O= DamaneSign SA	Nom déposé de l'organisation
OU=154609	Numéro du registre du commerce
CN= DamaneSign signature CA	**N**om 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)	(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)	(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

Ces pratiques sont interdites par cette PC/DPC.

3.1.4 Règles d'interprétation des différentes formes de nom

Les éléments contenus dans les sections 3.1.1, 3.1.2 et 3.1.3 fournissent les explications permettant d'interpréter correctement les différentes formes de nom.

Les certificats de test sont identifiés par la présence du préfixe « TEST- » dans les attributs CN et O du sujet.

3.1.5 Unicité des noms

L'attribut serialNumber contenu dans le champ subject du Certificat permet de garantir l'unicité des noms.

Le DN de chaque certificat de porteur permet d'identifier de façon unique le porteur correspondant au sein du domaine de l'AC. De plus, l'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC et UID.

3.1.6 Identification, authentification et rôle des marques déposées

L'AC ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par des Clients de marques déposées, de marques notoires et de signes distinctifs, ainsi que de noms de domaine. Si un tel cas se produit, l'AE pourra refuser de délivrer le Certificat au Signataire ou l'AC pourra prendre la décision de révoquer le Certificat.

3.1.7 Validation initiale de l'identité

L'enregistrement d'un utilisateur se réalise lors de la souscription initiale auprès de l'AE, avant la signature d'un document.

L'agent chargé de la signature avec le client est préalablement enregistré et clairement identifié au sein de la plateforme de signature, avec toutes ses informations d'identité consignées dans le système de l'organisation.

Les seuls éléments d'identification nécessaires à transmettre à l'AC lors de la demande de certificat sont le nom, le prénom, l'adresse e-mail, le numéro de téléphone du porteur.

Lors de la demande de certificat, l'adresse e-mail et le numéro de téléphone du demandeur est validé par l'envoi de plusieurs OTP MAIL/SMS. Ces e-mails permettent au porteur d'accéder à son espace Damanesign app de signature et à certaines données de workflow de signature.

3.1.8 Méthode pour prouver la possession de la clé privée

La Clé Privée du Signataire est générée et stockée de manière sécurisée par le Service de signature à la suite de l'identification et de l'authentification du Signataire par l'AE. La Clé Privée est ensuite utilisée par le Service de signature pour générer une requête de certificat et l'envoyer à l'AC après s'être authentifié auprès d'elle.

En aucun cas Damanesign ne pourra utiliser cette Clé Privée pour son propre usage ou pour le compte d'une autre personne que le Signataire.

3.1.9 Validation de l'identité d'un organisme

Sans objet.

3.1.10 Validation de l'identité d'un individu

L'AE délègue au Client la vérification de l'identité du Signataire.

3.1.11 Informations non vérifiées du porteur

Le choix de vérifier ou non les informations fournies par le porteur relève de la discrétion de l'AE délégué.

3.1.12 Validation de l'autorité du demandeur

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

3.1.13 Certification croisée d'A.C.

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

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

3.2.1 Identification et validation pour un renouvellement courant

Si le Signataire a déjà demandé un Certificat à l'AE, alors le Signataire a la possibilité de demander un nouveau Certificat en s'authentifiant auprès de l'AE à condition que les informations utilisées initialement par l'AE pour vérifier l'identité et les attributs du Signataire soient toujours valides.

Si tout ou partie des informations du Signataire à mettre dans le Certificat (voir la section 3.1.1 ci-dessus) ou des moyens d'authentification associés ont changé, alors l'enregistrement doit être réalisé avec la procédure définie dans la section 3.1.7 ci-dessus.

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

La demande est effectuée par le porteur via des moyens informatiques : le porteur peut demander la révocation de son certificat depuis les plateformes de services de signature Damanesign. La révocation sera traitée automatiquement.

4 EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Origine de Demande de certificat

L'AC publie sur son site web toutes les procédures et les exigences concernant une demande de certificat. Les demandeurs doivent suivre et respecter les procédures publiées.

Un certificat ne peut être demandé que par le futur porteur ou par le représentant d'un incapable majeur ou d'un mineur.

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

L'établissement de la demande de Certificat est effectué au niveau de la plateforme ou de l'application utilisatrice, la demande est transmise automatiquement, si elle est correcte, à la fonction adéquate de l'IGC pour la génération du certificat.

Pour un certificat, les informations suivantes doivent au moins faire partie de la demande de certificat :

- Les nom et prénom du porteur à utiliser dans le certificat ;
- Une adresse courriel où le porteur peut être joint ;
- Un numéro de téléphone GSM.

L'AE valide les informations du dossier d'enregistrement en conformité avec la présente PC/DPC, et transmet de manière sécurisée à l'AC la demande de Certificat.

4.3 Traitement d'une demande de certificat

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

La demande est authentifiée et validée par l'AE.
L'AE identifie et authentifie le Porteur.
L'AE s'assure que le porteur a pris connaissance des conditions générales d'utilisation.
L'AE conserve dans ses journaux l'ensemble des pièces qui composent le dossier d'enregistrement.

4.3.2 Acceptation ou rejet de la demande

Pour que la demande de Certificat soit acceptée, toutes les étapes du processus décrit dans la section précédente doivent être effectuées avec succès.
Dans le cas contraire, l'AE rejette la demande de Certificat et en informe le porteur dans les meilleurs délais.

4.3.3 Durée d'établissement du certificat

La demande de certificat reste active tant qu'elle n'est pas validée ou rejetée. Une fois la demande de Certificat validée, l'AC émet le Certificat dans les meilleurs délais.

4.4 Délivrance du certificat

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

Les actions de l'AC concernant la délivrance du Certificat sont les suivantes :

- Le Service de signature génère la bi-clé du porteur ;

- Le Service de signature crée la requête de certificat ;
- Le Service de signature s'authentifie auprès de l'AC et lui transmet la requête de certificat ;
- L'AC vérifie la signature de la requête de certificat transmise par le Service de signature ;
- L'AC crée le Certificat, en conformité avec le profil du Certificat défini dans la section 7.2 en certifiant, avec la Clé Privée de l'AC, l'association de la Clé Publique récupérée avec les informations d'identification du Signataire contenues dans la demande.

4.4.2 Notification de la délivrance du certificat au porteur

Une fois généré, le porteur est notifié par un SMS/MAIL de la délivrance du certificat.

4.5 Acceptation du certificat

4.5.1 Démarche d'acceptation du certificat

Juste avant sa création, les informations du Porteur, qui seront contenues dans le champ « subject » du Certificat, sont portées à la connaissance du Signataire afin qu'il puisse les accepter explicitement avant de déclencher la création ou l'utilisation de la Clé Privée associé à son Certificat. L'acceptation d'un Certificat par le Signataire emporte le consentement par le Signataire à la publication par l'AC du Certificat.

4.5.2 Publication du certificat

Les certificats de signature ne sont pas publiés après leur délivrance.

4.6 Usages de la bi-clé et du certificat

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

Les usages autorisés de la bi-clé et du certificat associé sont indiqués dans le certificat lui-même, via les extensions.
Ces usages doivent également être clairement explicités dans les conditions générales d'utilisation.

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

Les applications Métier utilisatrices de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée. Elles doivent respecter obligatoirement :

- Vérifier que l'extension « KeyUsage » contenue dans le certificat est conforme à l'utilisation du Certificat,
- Vérifier que l'OID de la présente PC/DPC est contenu dans l'extension « Certificate Policies » du Certificat ;
- Vérifier la validité de la chaîne de certification (dates de validité, signature des certificats, statut de révocation) en partant du certificat porteur et en remontant jusqu'au certificat de l'AC Racine.

4.7 Renouvellement d'un certificat

Le renouvellement d'un Certificat qui consiste à la délivrance d'un nouveau Certificat pour lequel seules les dates de validité changent, toutes les autres informations restantes identiques au certificat précédent.

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

La délivrance d'un nouveau certificat au bénéficiaire lié à la génération d'une nouvelle bi-clé.

4.8.1 Origine d'une demande d'un nouveau certificat

Lors de la demande initiale, les informations fournis par le porteur qui sont validés par l'AE seront conservés et pourront être réutilisés si le demandeur ne déclare aucune modification et si l'AE n'a pas la connaissance d'une modification.

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

Voir 4.3

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

Voir 4.3.2

4.8.5 Publication du nouveau certificat

Les certificats des porteurs ne sont pas publiés après leur délivrance.

4.9 Modification du certificat

La modification de certificat n'est pas autorisée dans le cadre de la présente PC /DPC.

4.10 Révocation et suspension des certificats

4.10.1 Causes possibles d'une révocation

4.10.1.1 Certificats de signature

Les circonstances ci-dessus peuvent être à l'origine de la révocation du certificat de signature du Porteur :

- Les informations du Porteur figurant dans son certificat ne sont pas en conformité avec son identité,
- Le Certificat de signature de l'AC « Damanesign Signature CA » est révoquée (ce qui entraîne la révocation des Certificats signés par la clé privée correspondante).
- Le porteur n'a pas respecté, ou ne respecte plus les obligations découlant de la présente PC/DPC, ainsi que les modalités applicables d'utilisation du certificat ;
- La clé privée du porteur est suspectée de compromission, est compromise,

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

Les cas suivants peuvent entrainer la révocation d'un Certificat d'une composante de l'IGC (y compris un certificat de l'AC «Damanesign Signature CA » pour la génération de Certificats :

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

- Révocation du certificat de l'AC ROOT ;

4.10.2 Origine d'une demande de révocation

4.10.2.1 Certificats de porteur

Les personnes / entités qui peuvent demander la révocation d'un Certificat Porteur sont les suivantes :

- Le Porteur, s'il constate que les données de son certificat ne sont pas conformes à son identité,
- L'AC «Damanesign Signature CA », émettrice du Certificat.

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

Les demandes de révocation des certificats émis par l'AC Root sont réalisées en face-à-face avec l'AE de l'AC Root sur présentation d'un formulaire signé par l'entité responsable de l'AC subordonnée.

La validation de l'identité et de l'autorité de la personne physique à l'origine de la demande sont vérifiées par l'AE. La révocation d'un certificat d'AC subordonnée émis par l'AC Root peut être aussi déclenchée par l'entité responsable de l'AC Root dans le cas de non-respect des exigences de l'IGC par cette AC subordonnée.

L'entité responsable de l'AC subordonnée est ensuite prévenue dans les plus brefs délais de cette décision.

La révocation d'un certificat d'AC subordonnée nécessite une cérémonie des clés. L'AC Root vérifie l'origine et l'intégrité de la demande de révocation du certificat. Si la demande est correcte, L'AC met à jour le dossier du porteur dans sa propre base de données et ajoute le numéro de série du certificat à la Liste des Certificats Révoqués (CRL).

4.10.3 Procédure de traitement d'une demande de révocation

4.10.3.1 Révocation d'un certificat de signature

Une demande de révocation peut être transmise à l'AE par le Signataire ou le Client. Le traitement d'une demande de révocation se déroule de la façon suivante :

- L'AE authentifie le demandeur ;
- L'AE demande à l'AC de procéder à la révocation du Certificat ;
- L'AC révoque le Certificat de manière définitive.

La demande de révocation de certificat comprend au minimum :

- L'identification du certificat concerné via au minimum :
- Son numéro de série, - l'identification de l'émetteur (champ DN de l'émetteur du certificat),
- La raison de révocation.

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.

La procédure à suivre est décrite dans la documentation interne de l'IGC.

4.10.4 Délai accordé au porteur pour formuler la demande de révocation

Dès qu'une entité autorisée (cf 4.10.2 « Origine d'une demande de révocation ») 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

Une demande de révocation du Certificat d'un Signataire est traitée dans un délai inférieur à 24 heures après l'authentification effective du demandeur de la révocation.

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

Il n'y a pas de période de grâce dans le cas d'une révocation d'une AC. L'entité autorisée demande la révocation d'un certificat dès lors qu'elle en identifie une cause de révocation.

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 du chemin de certification correspondante.

Pour un certificat racine, l'utilisateur fait confiance à ce certificat, à moins d'être averti d'une manière ou d'une autre (par exemple par voie de presse) que le certificat racine auto-signé a été compromis. Auquel cas, il doit supprimer ce certificat racine auto-signé de la liste de ses points de confiance.

Pour les autres certificats constituant le chemin de certification, selon l'information de révocation disponible et les contraintes liées à son application, l'utilisateur doit utiliser des LAR, des LCR.

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

La fréquence d'établissement des LCR est de 24 heures à minima.

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

Aucun service OCSP n'est mis en œuvre.

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

Pour le Certificat d'un Signataire, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la Clé Privée.

Pour le certificat d'un AC, la révocation suite à une compromission de la Clé Privée fait l'objet d'une information clairement diffusée par l'AC. En cas de révocation de l'AC, tous les certificats délivrés par cette AC et qui sont encore en cours de validité sont révoqués.

4.10.11 Suspension de certificats

La suspension de Certificat n'est pas autorisée dans la présente PC/DPC.

4.11 Fonction d'information sur l'état des certificats

4.11.1 Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats de signature simple doit au moins mettre à la disposition des utilisateurs de ces certificats un mécanisme de consultation libre de LCR. Ces LCR sont des LCR au format V2, publiées au moins sur un site web accessible en mode http.

4.11.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24 7j/7.

4.11.3 Séquestre de clé et recouvrement

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

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physique

Ce chapitre traite des mesures de sécurité non techniques (c. à d. concernant la sécurité physique, les procédures et la gestion du personnel) appliquées dans le but de sécuriser les fonctions de génération de clé, de délivrance des certificats, de révocation des certificats, d'audit et d'archivage. Suite à une analyse de risque menée par Damanesign, différents contrôles sont mis en place afin d'assurer un haut niveau de confiance dans le fonctionnement de l'AC.
Les exigences définies dans la suite de ce chapitre sont les exigences minimales que l'AC «Damanesign Signature CA». Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement de travail et des résultats de l'analyse de risque pour garantir un niveau de sécurité homogène.

5.1.1 Situation géographique et construction des sites

Une analyse de risque a été menée par DAMANESIGN. Les exigences de sécurité sont décrites dans la Politique de Sécurité de System Informatique (PSSI).

5.1.2 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'A.C., 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).

5.1.3 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'I.G.C. telles que fixées par leurs fournisseurs.

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

5.1.4 Vulnérabilités aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences et engagement de l'A.C. dans la présente P.C., 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 Prévention et protection incendie

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

5.1.6 Conservation des supports

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

5.1.7 Mise hors de 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)

5.1.8 Sauvegardes hors site

Les sauvegardes sont stockées sur les différents sites de production de l'hébergeur de l'I.G.C. : 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

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

5.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC fait 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 ;
- Que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- Le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- Éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.

Chaque attribution d'un rôle à un membre du personnel de l'IGC est notifiée par écrit. Ce rôle est clairement mentionné et décrit dans sa fiche de poste.

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

Avant la nomination d'une personne à un Rôle de Confiance, l'A.C. procède à la vérification de ses antécédents judiciaires et ses compétences professionnelles, de manière à valider son adéquation au poste à pourvoir. Il est notamment vérifié que :

- La personne n'a pas de conflit d'intérêt préjudiciable à l'impartialité des tâches qui lui sont attribuées ;
- La personne n'a pas commis d'infraction en contradiction avec son Rôle de Confiance.

L'A.C. sélectionne les personnes remplissant les Rôles de Confiance en tenant compte de leur loyauté, leur sérieux et leur intégrité.

Ces vérifications sont menées par l'A.C. dans le respect de la réglementation en vigueur et préalablement à l'affectation à un Rôle de Confiance. Elles sont revues au minimum tous les 3 ans

5.3.3 Exigences en matière de formation initiale

Le personnel est préalablement formé ou sensibilisé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, au sein de la composante de l'I.G.C dans laquelle il opère. En particulier, un ensemble de ressources documentaires est mis à disposition du personnel.

Les personnels ont connaissance et comprennent les implications des opérations dont ils ont la responsabilité.

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

Des sanctions d'ordre légal ou disciplinaire sont applicables en cas d'abus de droit. Damanesign ne saurait être responsable des actions non autorisées menées.

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

La journalisation d'événements consiste à enregistrer les évènements manuellement ou électroniquement par saisie ou par génération automatique.
Les fichiers résultants, sous forme papier et / ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées

5.4.1 Type d'événement à enregistrer

L'AC journalisent les évènements concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de l'I.G.C. :

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

D'autres évènements sont également recueillis. Il s'agit d'évènements concernant la sécurité qui ne sont pas produits automatiquement par les systèmes mis en œuvre :

- Les accès physiques aux zones sensibles ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel ayant des rôles de confiance ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les utilisateurs, ...).

En plus de ces exigences de journalisation communes à toutes les composantes et à toutes les fonctions de l'I.G.C. , des évènements spécifiques aux différentes fonctions de l'I.G.C. sont également journalisés :

- Réception d'une demande de certificat (initiale et renouvellement) ; Validation / rejet d'une demande de certificat ;

- Evènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, destruction, ...) ;
- Génération des certificats de porteurs ;
- Transmission des certificats aux porteurs et selon les cas, acceptations / rejets par les Porteurs ;
- Publication et mise à jour des informations liées à l'AC ;
- Génération d'information de statut d'un certificat (porteur).

Chaque enregistrement d'un évènement dans un journal contient les champs suivants (La structure de l'enregistrement peut varier selon le type de l'événement.) :

- Type de l'évènement ;
- Nom de l'exécutant ou référence du système déclenchant l'évènement ;
- Date et heure de l'évènement ;
- Résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'évènements.

Selon le type de l'évènement concerné, les champs suivants peuvent être enregistrés : Destinataire de l'opération ;

- Nom ou identifiant du demandeur de l'opération ou référence du système effectuant la demande
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- Cause de l'évènement ;
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

5.4.2 Fréquence de traitement des journaux d'événements

L'analyse du contenu des journaux d'événements est effectuée de manière régulière par l'AC déléguée. La fréquence de traitement des journaux d'évènements est décrite dans une procédure de journalisation des évènements du prestataire de service de confiance numérique Damanesign.

5.4.3 Période de conservation des journaux d'événements

Les journaux d'évènements sont conservés sur site pendant au moins 1 mois et doivent être archivés au plus tard sous le délai d'un (1) mois.

5.4.4 Protection des journaux d'événements

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

Pour prévenir toute tentative de modification, l'AC effectue un hachage de ses journaux les plus sensibles, chaque entrée faisant elle-même l'objet d'une signature.

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'A.C...

L'A.C. décrit dans ses procédures internes la procédure de sauvegarde des journaux d'événements.

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.

Les pratiques mises en œuvre sont décrites plus en détails dans la "Procédure de journalisation" et la "Politique de gestion de vulnérabilité".

5.5 Archivage des données

L'archivage des données permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'I.G.C. .

5.5.1 Types de données à archiver

Les données archivées au niveau de chaque composante, sont les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- La PC/DPC ;
- Les CGUs
- Le dossier d'enregistrement du porteur, ainsi que son acceptation d'utiliser le certificat ;
- Les certificats tels qu'émis ou publiés ;
- Les certificats AC Racine et subordonnées, et les LCR ;
- Les journaux d'évènements des différentes entités de l'I.G.C. .

5.5.2 Période de conservation des archives

Ces archives sont conservées pendant toute la durée de vie de l'AC à l'exception des journaux d'événements et des dossiers d'enregistrement qui sont conservés pendant 7 ans.

5.5.3 Protection des archives

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

- Seront protégées en intégrité ;
- Seront accessibles aux seules personnes autorisées ;
- Pourront être consultées et exploitées.

Une copie de tout le matériel informatique archivé ou sauvegardé est protégée soit par des mesures de sécurité physique seulement, soit par une combinaison de mesures physiques et

cryptographiques. Le site d'archivage protège adéquatement le matériel contre les dangers naturels, par exemple les excès de température, d'humidité et de magnétisme.

L'AC vérifiera l'intégrité de ses archives au moins tous les six (6) mois.

De plus, les informations conservées ou sauvegardées par l'AC peuvent être assujetties aux lois et règlements en vigueur et applicables à l'archivage et la conservation.

5.5.4 Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes est équivalent au niveau de protection des archives.

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

Les systèmes de collecte des archives de l'A.C. sont internes, respecte les exigences de protection des archives concernées.

5.6 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) peuvent être récupérées dans un délai inférieur à deux jours ouvrés. Ces archives sont conservées et traitées par des équipes de l'A.C. conformément aux procédures internes de l'A.C.

5.7 Changement de clé d'AC

Un AC ne peut pas générer des certificats pour les AC subordonnées ou les porteurs dont les dates de fin seraient postérieures à la date d'expiration du certificat de l'AC «Damanesign Signature CA». De ce fait, la période de validité du certificat de l'AC est supérieure à celle des certificats des AC subordonnées ou des porteurs.

Lorsqu'un nouveau certificat d'AC « Damanesign Signature CA » est émis, le certificat de l'AC « Damanesign Signature CA » précédent peut toujours être utilisé pour vérifier l'authenticité des certificats d'AC subordonnées ou des porteurs émis sous cet ancien certificat, et ce jusqu'à ce que ces certificats d'AC subordonnées ou des porteurs aient expiré.

5.8 Reprise suite à compromission et sinistre

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

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'événement 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 et la publication de l'information de révocation du certificat, s'il y a lieu, sera faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé, etc.).

De même, si l'un des algorithmes, ou des paramètres associés, utilisés par l'A.C. ou ses serveurs devient insuffisant pour son utilisation prévue restante, alors l'AC :

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

- Informera 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 doit être mise à disposition des autres utilisateurs de certificats ;
- Révoquera tout certificat concerné.

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'I.G.C. 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'I.G.C. 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.

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 :

- Elle assure la continuité du service d'archivage (notamment, archivage des certificats 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 LAR et LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC. À défaut, les applications de

l'Administration refuseront les certificats émis par des AC dont les LCR en cours de validité ne seraient plus accessibles, même si le certificat est encore valide ;
- Elle prévient les Mandataires de Certification dans le cas où les changements envisagés peuvent avoir des répercussions sur les engagements pris.
- Communiquer au point de contact identifié au sein de la DGSSI les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité.
- Tenir informée la DGSSI de tout obstacle ou délai non prévu rencontrés dans le déroulement du processus.

La « Procédure de gestion des incidents » et les « Plans de continuité d'activité » décrivent en détails les dispositions mises en œuvre

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, 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.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés de l'A.C.

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé.

Les clés de signature d'AC sont générées lors d'une cérémonie des clés à l'aide d'une ressource cryptographique matérielle.

Les rôles des personnes impliquées dans les cérémonies de clés. Suite à leur génération, les parts de secrets (données d'activation) sont remises à des porteurs de données d'activation désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'un même AC à un moment donné. Chaque part de secrets est mise en œuvre par son porteur.

6.1.1.2 Clés porteurs générées par l'A.C.

La génération de la bi-clé d'un Signataire est réalisée par le Service de signature dans un conteneur sécurisé de manière à garantir l'intégrité, la confidentialité et le contrôle exclusif de sa Clé Privée.

6.1.2 Transmission de la clé privée à son propriétaire

Damanesign ne transmis pas les clés privées des porteurs.

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 0.

6.1.5 Tailles des clés

La clé RSA de l'A.C. Racine a une taille de 4096 bits et sont associées à la fonction d'empreinte SHA-256.

Les clés RSA des A.C. filles ont une taille de 4096 bits et sont associées à la fonction d'empreinte SHA-256.

Les clés RSA des certificats de signature des porteurs ont une taille de 2048 bits et sont associées à la fonction d'empreinte SHA-256.

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

Les équipements utilisés pour la génération des bi-clés d'A.C. sont des ressources cryptographiques matérielles évaluées certifiées EAL 4+ et qualifié renforcé.

Le matériel cryptographique de sécurité utilisé pour la génération de bi-clés porteurs 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 d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR ;

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la fonction de signature.

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.

Les dispositifs cryptographiques utilisés pour la génération et la mise en œuvre des bi-clés de l'AC sont des HSM certifiés satisfaisant aux exigences.

Les HSM de l'AC sont hébergés dans les sites sécurisés de l'IGC et sont gérés exclusivement par les personnes ayant les rôles de confiance requis.

L'A.C. s'assure que :

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

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

L'activation de la clé privée de l'AC déléguée est contrôlée par les porteurs de secret détenant des secrets d'activations et qui sont dans des rôles de confiance. Les personnes de confiance participant à l'activation de la clé privée de l'AC déléguée font l'objet d'une authentification forte. L'AC déléguée est activée dans un boîtier cryptographique afin qu'elle puisse être utilisée par les seuls rôles de confiances qui peuvent émettre des certificats.

6.2.3 Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des Utilisateurs ne sont séquestrées.

6.2.4 Copie de secours de la clé privée

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

6.2.5 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.

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

Les clés de l'AC sont générées, activées et stockées dans des ressources cryptographiques matérielles ou sous forme chiffrées. Quand elles ne sont pas stockées dans des ressources cryptographiques ou lors de leur transfert, les clés privées d'AC sont chiffrées au moyen de la clé de wrap du HSM.

Une clé privée de l'AC chiffrée ne peut être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle et la présence de multiples personnes dans des rôles de confiance.

6.2.7 Stockage de la clé privée dans un module cryptographique

Voir ci-après.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'A.C.

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

6.2.8.2 Clés privées des porteurs

La clé privée du porteur est activée par la plateforme Damanesign , après la saisie par le porteur du code secret d'activation qui lui a été transmis par un OTP SMS dans son portable GSM ou par MAIL dans son boite email.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'A.C.

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

Les modalités de désactivation sont propres à la technologie du module ; elles sont détaillées dans la documentation constructrice.

6.2.9.2 Clés privées des porteurs

Sans Objet

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées d'A.C.

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

Les mesures mises en œuvre sont décrites dans la « Procédure de gestion des clés cryptographiques ».

6.2.10.2 Clés privées des porteurs

Les clés privées des porteurs sont détruites après la révocation des certificats.

6.2.10.3 Niveau de qualification du module cryptographique

Les modules cryptographiques utilisés par l'A.C. sont évalués selon les critères communs au niveau EAL 4+. Ils sont parmi Liste des Dispositifs de signature électronique sécurisée disposant d'un certificat de conformité déclaré par la DGSSI.

Ces exigences sont précisées au chapitre 10 et 11.

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 par archivage des certificats correspondants et ce dans le cadre de la politique d'archivage.

6.3.2 Durées de vie des bi-clés et des certificats

Comme un AC ne peut émettre de certificats porteurs d'une durée de vie supérieure à celle de son propre certificat, la bi-clé et le certificat auquel elle correspond sont renouvelés au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats porteurs émis.

La durée de validité d'un certificat de l'AC est 30 ans

Les bi-clés et les certificats des porteurs couverts par la présente PC/DPC ont la même durée de vie, au moins égale à 1 ans, et au maximum de 6 ans La durée de vie des clés.

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.

Les données d'activation des clés privées d'AC sont générées durant la cérémonie de clés.

Les données d'activation sont générées automatiquement selon un schéma de type M of N.

Les données d'activation sont remises à leurs porteurs après génération pendant la cérémonie des clés. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance

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

Le type de données d'activation qu'utilise le porteur est décrit dans la politique de signature. Les données d'activation sont générées par l'AE et distribuées de manière sécurisée au Client de façon à avoir l'assurance que seul le Client pourra signer un contrat à l'aide de la donnée d'activation

6.4.2 Protection des données d'activation

Les données d'activation des dispositifs de création de signature des porteurs générées par l'A.C. sont protégées en intégrité et en confidentialité jusqu'à la remise aux porteurs. Ces données ne sont pas sauvegardées par l'A.C. et sont modifiées par le porteur après réception.

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

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique. Les porteurs de données d'activation sont responsables de leur gestion et de leur protection. Un porteur de données d'activation ne peut détenir plus d'une donnée d'activation d'un même A.C. à un même instant.

6.4.2.2 Protection des données d'activation correspondant aux clés privées des porteurs

Les données d'activation des clés privées des Porteurs sont placées sous leur responsabilité.
Les modalités de protection des données d'activation des clés privées des porteurs dépendent de la méthode choisie. Le détail de ces modalités est fourni dans les conditions d'utilisation du service de signature électronique.

Une méthode d'authentification forte est requise pour activer le processus de génération du Bi-clé et du Certificat de Signature.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

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

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

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

Les procédures de sécurité des systèmes informatiques est décrite dans la documentation interne de l'I.G.C.

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Sans objet

6.6 Mesures de sécurité liées au développement des systèmes

Tous les composants logiciels de l'A.C. sont développés dans des conditions et suivant des processus de développement garantissant leur sécurité. L'A.C. met en œuvre des processus qualité au cours de la conception et du développement de ses logiciels. L'A.C. s'assure, lors de la mise en production d'un élément logiciel, de son origine et de son intégrité et assure une traçabilité de l'ensemble des modifications apportées sur son système d'information.

Les infrastructures de développement et d'essai sont distinctes des infrastructures de production de l'A.C.

6.7 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées qui n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC. Les échanges entre composantes au sein de l'IGC 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.). Une analyse de risque relative à l'interconnexion a été menée afin d'établir les objectifs et les solutions de sécurité adaptées. A défaut le dispositif cryptographique dans lequel les clés de l'AC sont activées est isolé.

6.8 Horodatage / Système de datation

Les systèmes de datation sont synchronisés par rapport à une source fiable du temps universel (UTC) et un système de synchronisation temporelle (NTP) avec une précision au moins égale à une second.

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

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 SA`
	`C = MA`

Validity	30 ans

Subject	`C=MA`
	`O=DamaneSign SA`
	`OU=154609`
	`CN=DamaneSign 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/CertData/DamaneSign%20Root%20CA.crl`
Authority Information Access	N	`CA:` `https://pki.damanesign.ma/CertData/DamaneSign%20signature%20CA.crt`

7.2 Certificat de signature (1.3.6.1.4.1.58553.1.7.2.1)

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	Entre 1 ans à 6 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.

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
Basic Constraints	O	CA: FALSE
Certificate Policies	N	OID: 1.3.6.1.4.1.58553.1.7.2.1 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/CertData/DamaneSign%20signature%20CA.crl
Authority Information Access	N	CA: https://pki.damanesign.ma/CertData/DamaneSign%20signature%20CA.crt

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 SA OU=154609 CN=DamaneSign signature CA
thisUpdate	Date et heure UTC
nextUpdate	Date et heure UTC (1 jour 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.

8 Audits de conformité et évaluations

Les audits et évaluations ont pour objectif de s'assurer que l'implémentation faite de l'IGC est conforme aux dispositions écrites dans la présente PC / DPC.

8.1 Fréquences et circonstances des évaluations

Un contrôle de conformité à la PC est réalisé tous les 3 ans. Toute évolution majeure de l'IGC donne lieu à un nouvel audit de conformité.

Les audits sont axés sur la base des éléments suivants :

- Les orientations stratégiques de Damanesign ;
- L'analyse des risques, par l'exploitation, notamment de la cartographie des risques et de la base des incidents ;
- La couverture suffisante de l'univers d'audit (Missions thématiques, Audit de processus, Audit de fonctions) ;
- Le champ d'intervention des auditeurs externes ou consultants et le cas échéant, des autorités de contrôle et de supervision.

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

L'objectif de l'audit de conformité est de vérifier qu'une composante de l'AC opère ses services en conformité avec la présente PC/DPC.

8.5 Actions prises suite aux conclusions des évaluations

A la constatation d'une non-conformité par rapport aux exigences de la PC/DPC de l'AC , l'auditeur de conformité procède aux actions suivantes :

- Documenter la non-conformité ;
- Notifier l'entité concernée par la non-conformité ;
- L'entité responsable de la correction de la non-conformité détermine quelles sont les mesures à prendre en fonction des exigences de la présente PC/DPC, et les effectue sans délai avec l'approbation.

Selon le degré de criticité de la non-conformité, et la rapidité avec laquelle elle peut être corrigée, Damanesign peut décider de suspendre temporairement le fonctionnement de l'AC, de révoquer le certificat émis par l'AC, ou de prendre toute autre mesure qu'il juge opportune.

8.6 Communication des résultats

Le Rapport de la mission d'audit de Conformité, incluant l'état de réalisation des mesures correctives (réalisé, validé, en cours) est remis à Damanesign.

9 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

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

9.1.2 Tarifs pour accéder aux certificats

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

9.1.5 Politique de remboursement

La présente PC/DPC 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 :

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

9.4.3 Informations à caractère non personnel

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

9.4.4 Responsabilité en termes de protection des données personnelles

L'A.C. a mis en place et respecte des procédures de protection des données personnelles pour garantir la sécurité des informations caractérisées comme personnelles au sens de l'article 9.4.1 ci-dessus dans le cadre de la délivrance et la gestion d'un certificat de porteur.

A cet égard, l'A.C. respecte notamment la législation et 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 PC/DPC ne formule pas d'exigence spécifique sur le sujet.

9.5 Droits sur la propriété intellectuelle et industrielle

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

9.6 Interprétations contractuelles et garanties

Sans objet.

9.7 Limite de garantie

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

9.8 Limite de responsabilité

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

9.9 Indemnités

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

9.10.2 Fin anticipée de validité

La cessation d'activité de l'I.G.C., programmée ou suite à sinistre, entraîne la fin de validité de la présente PC/DPC

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./DPC de l'A.C. étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC/DPC 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 DPC/PC évoluera dès lors qu'un changement majeur intervient dans les exigences de la PC Type applicable à la famille de certificats considérée.

9.13 Dispositions concernant la résolution de conflits

La validité de la présente P.C. et toute autre question ou litiges relatifs à son interprétation, à son exécution ou à sa résiliation seront régis par le droit marocain.

L'A.C. et le Porteur s'engagent à consacrer leurs meilleurs efforts à la résolution amiable de toutes les questions ou de tous les litiges qui pourraient les diviser, préalablement à la saisie de la juridiction ci-après désignée.

L'A.C. et le Porteur convient, pour le cas où un accord amiable serait impossible à arrêter, que les juridictions de Rabat auront compétences exclusives pour connaître de tout différend résultant de la validité, de l'interprétation, de l'exécution ou de la résiliation des présentes, et plus généralement de tout litige procédant des présentes qui pourrait les diviser, nonobstant pluralités des défendeurs ou appel en garantie.

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 et des L.C.R. / L.A.R.), 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.