Politique de Certification AC Qualifié Cachet

Version 1.1

OID n° 1.3.6.1.4.1.58553.1.2.1.1 / 1.3.6.1.4.1.58553.1.2.1.2

Historique du document

Indice	Date de création	Rédacteur(s)	Modifications
0.2	21/04/2022	Samuel LUCAS	Création du modèle
1.0	13/10/2023	Fatimazahrae JALAL	Mise à jour conformément à la loi 43.20
1.1	15/10/2023	Fatimazahrae JALAL	Mise à jour des extensions gabarit de certificat

Sommaire

1 Introduction 6
1.1 Présentation générale 6
1.2 Identification du document 6
1.3 Entités intervenant dans l'I.G.C. et responsabilités 7
1.3.1 Le prestataire de service de confiance (PSCo) 7
1.3.2 Autorité de certification 7
1.3.3 Autorité d'enregistrement 9
1.3.4 Porteurs de certificats 9
1.3.5 Responsables de Certificat de Cachet (RCC) 10
1.3.6 Responsables d'unité d'horodatage 10
1.3.7 Utilisateurs de certificat 10
1.3.8 Mandataire de certification 11
1.4 Usage des certificats 11
1.4.1 Domaines d'utilisation applicables 11
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 D.P.C. 12
1.6 Définitions et sigles 12
1.6.1 Sigles 12
1.6.2 Définitions 13
2 RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIÉES 15
2.1 Entités chargées de la mise à disposition des informations 15
2.2 Informations devant être publiées 15
2.2.1 Publication du certificat d'AC 15
2.2.2 Publication de la CRL 15
2.2.3 URL d'OCSP 15
2.3 Délais et fréquences de publication 15
2.4 Contrôle d'accès aux informations publiées 16
3 IDENTIFICATION ET AUTHENTIFICATION 17
3.1 Nommage 17
3.1.1 Types de noms 17
3.1.2 Nécessité d'utilisation de noms explicites 17
3.1.3 Pseudonymisation des porteurs 17
3.1.4 Règles d'interprétation des différentes formes de nom 17
3.1.5 Unicité des noms 17
3.1.6 Identification, authentification et rôle des marques déposées 18
3.1.7 Validation initiale de l'identité 18
3.1.8 Méthode pour prouver la possession de la clé privée 18
3.1.9 Validation de l'identité d'un organisme 18
3.1.10 Validation de l'identité d'un individu 18
3.1.11 Informations non vérifiées du porteur 19
3.1.12 Validation de l'autorité du demandeur 19
3.1.13 Certification croisée d'A.C. 19
3.2 Identification et validation d'une demande de renouvellement des clés 19
3.2.1 Identification et validation pour un renouvellement courant 19

3.2.2 Identification et validation pour un renouvellement après révocation 19
3.3 Identification et validation d'une demande de révocation 19
4 EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS 22
4.1 Demande de certificat 22
4.2 Processus et responsabilités pour l'établissement d'une demande de certificat 22
4.3 Traitement d'une demande de certificat 22
4.3.1 Exécution des processus d'identification et de validation de la demande 22
4.3.2 Acceptation ou rejet de la demande 23
4.3.3 Durée d'établissement du certificat 23
4.4 Délivrance du certificat 23
4.4.1 Actions de l'A.C. concernant la délivrance du certificat 23
4.4.2 Notification de la délivrance du certificat au porteur 24
4.5 Acceptation du certificat 24
4.5.1 Démarche d'acceptation du certificat 24
4.5.2 Publication du certificat 24
4.5.3 Notification aux autres entités de la délivrance du certificat 24
4.6 Usages de la bi-clé et du certificat 24
4.6.1 Utilisation de la clé privée et du certificat par le porteur 24
4.6.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat 24
4.7 Renouvellement d'un certificat 25
4.8 Délivrance d'un nouveau certificat à la suite du changement de la bi-clé 25
4.8.1 Origine d'une demande d'un nouveau certificat 25
4.8.2 Procédure de traitement d'une demande d'un nouveau certificat 25
4.8.3 Notification au RCC de l'établissement du nouveau certificat 25
4.8.4 Démarche d'acceptation du nouveau certificat 25
4.8.5 Publication du nouveau certificat 25
4.8.6 Notification par l'AC aux autres entités de la délivrance du nouveau certificat 25
4.9 Modification du certificat 25
4.10 Révocation et suspension des certificats 26
4.10.1 Causes possibles d'une révocation 26
4.10.2 Origine d'une demande de révocation 27
4.10.3 Procédure de traitement d'une demande de révocation 27
4.10.4 Délai accordé au porteur pour formuler la demande de révocation 28
4.10.5 Délais de traitement par l'A.C. d'une demande de révocation 28
4.10.6 Exigences de vérification de la révocation par les utilisateurs de certificats 28
4.10.7 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats 29
4.10.8 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats 29
4.10.9 Autres moyens disponibles d'information sur les révocations 29
4.10.10 Exigences spécifiques en cas de compromission de la clé privée 29
4.10.11 Suspension de certificats 29
4.11 Fonction d'information sur l'état des certificats 29
4.11.1 Caractéristiques opérationnelles 29
4.11.2 Disponibilité de la fonction 29
4.11.3 Séquestre de clé et recouvrement 30
5 Mesures de sécurité non techniques 31
6 Mesures de sécurité techniques 32
6.1 Génération et installation de bi-clés 32

6.1.1 Génération des bi-clés....32
6.1.2 Transmission de la clé privée à son propriétaire....32
6.1.3 Transmission de la clé publique à l'A.C. 32
6.1.4 Transmission de la clé publique de l'A.C. aux utilisateurs de certificats....32
6.1.5 Tailles des clés 32
6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité 33
6.1.7 Objectifs d'usage de la clé 33
6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques 33
6.2.1 Standards et mesures de sécurité pour les modules cryptographiques 33
6.2.2 Contrôle de la clé privée de l'A.C. par plusieurs personnes....33
6.2.3 Séquestre de la clé privée....33
6.2.4 Copie de secours de la clé privée 34
6.2.5 Archivage de la clé privée 34
6.2.6 Transfert de la clé privée vers / depuis le module cryptographique....34
6.2.7 Stockage de la clé privée dans un module cryptographique 34
6.2.8 Méthode d'activation de la clé privée 34
6.2.9 Méthode de désactivation de la clé privée....35
6.2.10 Méthode de destruction des clés privées 35
6.3 Autres aspects de la gestion des bi-clés....35
6.3.1 Archivage des clés publiques 35
6.3.2 Durées de vie des bi-clés et des certificats 36
6.4 Données d'activation 36
6.4.1 Génération et installation des données d'activation 36
6.4.2 Protection des données d'activation.... 36
6.5 Mesures de sécurité des systèmes informatiques 36
6.6 Mesures de sécurité liées au développement des systèmes....37
6.7 Mesures de sécurité réseau....37
6.8 Horodatage / Système de datation 37
7 Profils des certificats et des L.C.R.....38
7.1 Certificats de l'A.C. 38
7.2 Certificat de cachet (**1.3.6.1.4.1.58553.1.2.1.1**).... 38
7.3 Certificat d'horodatage (1.3.6.1.4.1.58553.1.2.1.2).... 39
7.4 Liste de Certificats Révoqués 39
7.5 Certificat OCSP 40
8 Audits de conformité et évaluations 42
9 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES.....43
10 Annexe 1 : Exigences de sécurité du module cryptographique de l'A.C. 44
10.1 Exigences sur les objectifs de sécurité.... 44
11 Annexe 2 : Exigences de sécurité du module cryptographique des services de cachet.....45

1 Introduction

1.1 Présentation générale

Ce document constitue la politique de certification mise en œuvre par la société Damanesign pour la fourniture de certificats électroniques qualifiés pour le cachet électronique et de certificats électroniques qualifiés pour l'horodatage. Elle réunit l'ensemble des obligations et engagements des différents acteurs relatifs à la délivrance et l'usage de ces certificats.

L'autorité de certification fait partie de l'I.G.C. de Damanesign et partage donc avec les autres A.C. l'organisation et les mesures techniques et non-techniques mises en œuvre par la société. C'est pourquoi le présent document fait référence, en ce qui concerne les éléments communs, à la politique suivante : Politique de certification Qualified Signature CA (OID 1.3.6.1.4.1.58553.1.3.1.3). Cette politique sera désignée par [PCQSIGN] dans la suite du document.

1.2 Identification du document

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

Le numéro d'OID des certificats produits sous la présente P.C. est : **1.3.6.1.4.1.58553.1.2.1.1** / **1.3.6.1.4.1.58553.1.2.1.2**

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

Dans la présente PC, les types de certificats gérés en tant que cachet qualifié sont les suivants :

OID : 1.3.6.1.4.1.58553.1.2.1.1 pour les certificats électroniques qualifiés pour le cachet électronique

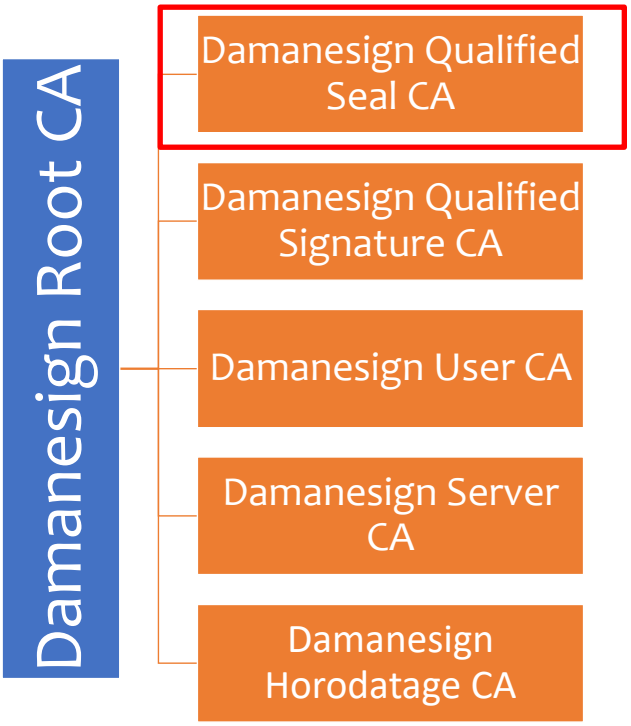
OID : 1.3.6.1.4.1.58553.1.2.1.2 pour les certificats d'horodatage qualifiés ;

Et les certificats OCSP de l'AC.

Les éléments spécifiques à une politique seront précédés de l'OID de cette politique entre crochets : [OID]. Plusieurs OID peuvent être spécifiés, ils sont séparés par des points-virgules.

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

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



1.3.1 Le prestataire de service de confiance (PSCo)

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

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

1.3.2 Autorité de certification

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

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

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

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

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

Fonction de génération des certificats : Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les Certificats à partir des informations transmises par

l'Autorité d'Enregistrement et de la clé publique du Client provenant de la fonction de génération des éléments secrets du Client chargée en particulier de générer la bi-clé du Client.

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

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

Fonction de publication : Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides de ses porteurs.

Fonction de gestion des révocations : Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

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

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

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

- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux porteurs, aux utilisateurs de certificats, … qui mettent en œuvre ses certificats ;
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur
- Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse ;
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions obligatoires énoncées dans les référentiels des exigences applicables aux services de confiance qualifiés, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats ;
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, et correspondant au minimum aux exigences énoncées dans les référentiels des exigences applicables aux services de confiance qualifiés, notamment en termes de fiabilité, de qualité et de sécurité ;
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (certificats, de LCR et de réponses OCSP), ou faire renouveler ses certificats si l'AC est rattaché à un AC hiérarchiquement supérieur. Diffuser ses certificats d'AC aux porteurs et utilisateurs de certificats ;
- Les personnels Damanesign peuvent demander un certificat en suivant la procédure nominale.

1.3.3 Autorité d'enregistrement

L'A.E. assure les tâches suivantes :

- La prise en compte et la vérification des informations du porteur
- La constitution du dossier d'enregistrement correspondant
- L'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage)
- La conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du porteur y compris lors des échanges de ces données avec les autres fonctions de l'I.G.C. (notamment, elle respecte la législation relative à la protection des données personnelles).

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

L'Autorité d'Enregistrement (AE) a pour rôle de vérifier l'identité du futur porteur de certificat.

L'AE de l'AC est opérée par un service interne à Damanesign.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

L'Autorité d'Enregistrement (AE) a pour rôle de vérifier l'identité du service interne de

Damanesign auquel est délivré le certificat. L'AE est opérée par un service interne à Damanesign.

1.3.4 Porteurs de certificats

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

Personne morale identifiée dans le certificat, représentée par une personne physique pour tout ce qui touche au cycle de vie du certificat (RCC), détentrice de la clé privée correspondant à la clé publique qui est dans ce certificat.

Remarque : Damanesign est susceptible de produire des certificats de cachet pour ses propres services de confiance (scellement de documents).

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

Les porteurs sont les unités d'horodatage du service Damanesign, représentés par le responsable des unités d'horodatage.

1.3.5 Responsables de Certificat de Cachet (RCC)

Un RCC est une personne physique qui est responsable de l'utilisation du certificat cachet / horodatage électronique identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité également identifiée dans ce certificat. Le RCC a un lien contractuel, hiérarchique ou réglementaire avec cette entité.

Le RCC respecte les conditions qui lui incombent définies dans la présente P.C.

Le certificat étant attaché au serveur informatique et non au RCC, ce dernier peut être amené à changer en cours de validité du certificat : départ du RCC de l'entité, changement d'affectation et de responsabilité au sein de l'entité, etc.

L'entité doit signaler à l'A.C. préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RCC de ses fonctions et lui désigner un successeur. L'A.C. révoquera un certificat cachet/horodatage électronique pour lequel il n'y a plus de RCC explicitement identifié.

1.3.6 Responsables d'unité d'horodatage

Un RUH est une personne physique qui est responsable de l'utilisation du service identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte du service d'horodatage de Damanesign.

Le RUH respecte les conditions qui lui incombent définies dans la présente P.C.

Le certificat étant attaché au serveur informatique et non au RUH, ce dernier peut être amené à changer en cours de validité du certificat : départ du RUH de l'entité, changement d'affectation et de responsabilité au sein de l'entité, etc.

L'entité doit signaler à l'A.C. préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RUH de ses fonctions et lui désigner un successeur. L'A.C. révoquera un certificat électronique pour lequel il n'y a plus de RUH explicitement identifié.

1.3.7 Utilisateurs de certificat

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

Un utilisateur de certificat peut être une application ou une personne physique ou morale destinataire de données électroniquement signées ou authentifiées par la personne morale porteuse d'un certificat émis par la présente A.C. Cet utilisateur souhaite vérifier l'authenticité ou la validité du cachet électronique apposé sur ces données.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

Un utilisateur de certificat peut être une application ou une personne physique ou morale destinataire de données électroniquement horodaté par le service d'horodatage de Damanesign. Cet utilisateur souhaite vérifier l'authenticité ou la validité de la contremarque de temps qualifié apposée sur ces données.

1.3.8 Mandataire de certification

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

Le rôle du MC consiste à effectuer certaines taches de l'AE, en particulier :

- A réceptionner les formulaires de demande et à collecter la copie des documents permettant de s'assurer de l'identification du futur RCC ;
- A vérifier en face à face les informations d'identification du futur RCC, les originaux des documents collectés et la conformité des informations qu'ils contiennent par rapport aux copies fournies ;
- A constituer le dossier de demande de Certificat et à faire signer le formulaire de demande de Certificat par le futur RCC de Certificat ;
- A informer le futur RCC de ses obligations contractuelles et à faire signer les Conditions Générales d'Utilisation du Certificat ;
- A transmettre le dossier de demande de Certificat à l'Autorité d'enregistrement ;
- A mettre en place les moyens permettant de garantir la remise et l'acceptation explicite du Certificat et du Dispositif sécurisé de création de signature lors de sa délivrance au RCC ;
- A transmettre à l'AE à des fins d'archivage, les dossiers d'enregistrement et toute information relative aux Certificats électroniques délivrés qui pourrait s'avérer nécessaires pour faire la preuve en justice de la certification électronique ;

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

Sans objet.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Bi-clés et certificats des porteurs

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

La présente PC traite des bi-clés et des certificats utilisés par des services applicatifs déployés sur des serveurs informatiques dont la fonction est de sceller électroniquement des données (apposition d'un cachet électronique). Les usages de certificat de cachet sont donc :

- Apposition d'un cachet sur des données par un serveur informatique appartenant à une personne morale et vérification de ce cachet par un tiers (OID **1.3.6.1.4.1.58553.1.2.1.1**)
- Aucun autre usage de la bi-clé n'est autorisé.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

Les certificats d'horodatage ne sont utilisables que pour signer les contremarques de temps qualifiées produites par les unités d'horodatage du service Damanesign. Le service d'horodatage dont dépendent ces unités d'horodatage est un service qualifié.

L'AC génère également des certificats spécifiquement destinés aux réponses OCSP de son service. Aucun autre usage de la bi-clé n'est autorisé.

1.4.1.2 *Bi-clés et certificats d'A.C.*

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

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

1.4.2 Domaines d'utilisation interdits

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

1.5 Gestion de la P.C.

1.5.1 Entité gérant la P.C.

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

1.5.2 Point de contact

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

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

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

1.6 Définitions et sigles

1.6.1 Sigles

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

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

URL *Uniform Resource Locator*

1.6.2 Définitions

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

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

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

Autorité d'horodatage : Autorité responsable de la gestion d'un service d'horodatage.

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

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

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

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

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

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

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

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

Infrastructure à Clés Publiques (**I.G.C.**) : désigne un ensemble de moyens organisationnels, techniques (matériels et logiciels), humains, documentaires et contractuels pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques. L'I.G.C. génère, distribue, gère et archive les Certificats. Chacune des composantes de l'I.G.C. est

décrite dans la politique de certification définissant le niveau de confiance confié à chacune d'entre elles.

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

Personne autorisée : Il s'agit d'une personne autre que le porteur qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du porteur.

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 certificsats.

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

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

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

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

2.1 Entités chargées de la mise à disposition des informations

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

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

2.2 Informations devant être publiées

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

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

Ces documents sont publiés à l'adresse :

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

2.2.1 Publication du certificat d'AC

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

`http://pki.damanesign.ma/cert/ca_qseal_2022.crt`

2.2.2 Publication de la CRL

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

`http://pki.damanesign.ma/crl/ca_qseal_2022.crl`

2.2.3 URL d'OCSP

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

http://ocsp.damanesign.ma/ca_qsig

2.3 Délais et fréquences de publication

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

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

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

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

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

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

3.1.2 Nécessité d'utilisation de noms explicites

3.1.2.1 A.C. Cachet qualifié

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

3.1.2.2 Certificat de cachet

Les noms choisis pour désigner les porteurs de cachet doivent être explicites.

Les porteurs de cachet sont identifiables par leurs DN, comme suit.

CN=	Nom significatif du service mettant en œuvre le cachet
OI=	Numéro d'immatriculation officiel de l'entité
O=	Dénomination officielle ou raison sociale de l'entité
C=MA	Pays

3.1.2.3 Certificat d'horodatage

C = MA	Pays
O=Damanesign	Nom déposé de l'organisation tel qu'enregistré au registre du commerce
OI=NTRMA-154609	organizationIdentifier : NTRFR- 154609
OU=154609	organizationalUnitName : champ contenant une information facultative.
serialNumber= ‹ numéro de série ›	Numéro aléatoire
CN=Damanesign Horodatage U- ‹ numéro de l'UH ›	Nom commun de l'unité d'horodatage Damanesign

3.1.3 Pseudonymisation des porteurs

La présente PC n'autorise pas l'utilisation de pseudonyme dans les certificats.

3.1.4 Règles d'interprétation des différentes formes de nom

Sans objet.

3.1.5 Unicité des noms

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

L'A.C. est garante de l'unicité des noms contenus dans les certificats de cachet.

3.1.6 Identification, authentification et rôle des marques déposées

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

3.1.7 Validation initiale de l'identité

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

L'enregistrement d'un service de création de cachet d'une entité auquel un certificat doit être délivré se fait via l'enregistrement du RCC correspondant auprès de l'AE. L'enregistrement d'un RCC, et l'entité correspondante, se fait directement auprès de l'AE. L'AE valide l'identité "personne morale" de l'entité de rattachement du RCC.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

La validation initiale de l'identité d'une entité interne (Damanesign) est nécessaire pour la création d'un certificat d'horodatage. L'enregistrement du responsable de cette entité interne, et l'entité correspondante, se fait directement auprès de l'AE.

3.1.8 Méthode pour prouver la possession de la clé privée

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

L'Autorité de Certification (AC) génère la paire de clés du certificat dans des dispositifs sécurisés et certifiés.
Le RCC est le seul à posséder les données d'activation.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

La clé privée est entièrement gérée, stockée et protégée par l'IGC Damanesign. Néanmoins, nous mettons en œuvre des moyens techniques et organisationnels afin d'assurer que la clé privée ne sera utilisée que par l'utilisateur de certificat d'horodatage.

3.1.9 Validation de l'identité d'un organisme

Voir ci-dessous.

3.1.10 Validation de l'identité d'un individu

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

L'enregistrement du futur RCC (personne physique) représentant une entité nécessite l'identification de cette entité et l'identification de la personne physique. Le RCC doit être habilité en tant que RCC pour le service de création de cachet considéré.

Le dossier d'enregistrement, déposé auprès de l'AE, doit au moins comprendre :

- Une demande de certificat écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le nom du service de création de cachet concerné par cette demande,
- Un mandat, daté de moins de 3 mois, désignant le futur RCC comme étant habilité à être RCC pour le service de création de cachet pour lequel le certificat de cachet doit être délivré. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RCC,
- Les conditions générales d'utilisation signées par le RCC

- Un document officiel d'identité en cours de validité du RCC comportant une photographie d'identité notamment la carte d'identité nationale, le passeport, qui est présenté à l'AE, qui en conserve une copie.
- Une photocopie d'un justificatif d'identité du représentant légal
- Une pièce valide au moment de l'enregistrement portant le numéro d'identification de l'entreprise
- Information de contact du RCC

L'authentification du RCC par l'A.E. est réalisée lors d'un face-à-face physique ou par une méthode apportant un degré d'assurance équivalent.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

Le responsable de l'unité d'horodatage Damanesign s'adresse à l'AE pour l'obtention d'un certificat d'UH. L'AE valide l'identité du demandeur par vérification en face à face d'une pièce d'identité (carte d'identité ou passeport) puis vérifie dans l'organigramme interne que le demandeur est bien responsable de l'unité d'horodatage et donc de son certificat.

3.1.11 Informations non vérifiées du porteur

Aucune.

3.1.12 Validation de l'autorité du demandeur

Cette étape est effectuée en même temps que la validation de l'identité d'un individu.

3.1.13 Certification croisée d'A.C.

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

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

3.2.1 Identification et validation pour un renouvellement courant

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

3.2.2 Identification et validation pour un renouvellement après révocation

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

3.3 Identification et validation d'une demande de révocation

L'AE authentifie toutes les demandes de révocation.

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

Le Référentiel de Certification (RCC) a deux méthodes pour révoquer un certificat Damanesign :

- **Révocation en ligne** : Accédez à la page "https://guichet.damanesign.ma" dans votre navigateur, suivez les étapes indiquées sous "Services" et "Révocation du Certificat", en renseignant les détails requis et en choisissant la raison de la révocation.
- **Révocation par appel téléphonique** : Le RCC peut contacter le service de révocation de Damanesign au +212 5 37 68 68 01 pendant les jours ouvrés, répondre à des questions pour l'authentification, préciser le certificat à révoquer et la raison de la révocation.

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

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

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

Le responsable de l'autorité d'horodatage s'adresse en personne à l'AE, qui l'authentifie sur la base de l'annuaire interne de Damanesign.

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

Dans le cas où une demande de révocation ne peut être confirmée dans les 24 heures, Damanesign suit la procédure suivante :

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

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

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

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

- La législation locale pertinente.

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

4 EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

La demande de certificat provient du RCC nommé par le responsable légal de l'entité.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

La demande de certificat provient du responsable de l'autorité d'horodatage.

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

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

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

- Le nom du service de création de cachet à utiliser dans le certificat ;
- Les données personnelles d'identification du RCC ;
- Les données d'identification de l'entité.

Le dossier d'enregistrement est établi soit directement par le futur RCC à partir des éléments fournis par son entité, soit par une personne autorisée. Le dossier doit être déposé directement auprès de l'Autorité d'Enregistrement (AE) chez Damanesign.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

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

- Une pièce d'identité valide au nom du porteur.

Le dossier d'enregistrement est établi directement par le futur porteur. Le dossier est transmis à l'AE. Le certificat généré par l'AC sera remis en main propre au responsable de l'unité d'horodatage.

Les conditions générales d'utilisation, signées par le demandeur, doivent faire partie de 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

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

L'A.E. s'engage à effectuer les tâches suivantes :

Le contrôle du dossier d'enregistrement (dossier complet), à savoir :
« Contrat d'abonné – Conditions Particulières »
« Conditions Générales d'utilisation »
« Autorisation de demande de certificat »
« Procuration du représentant légal – Désignation d'un mandataire de certification » dans le cas d'une demande via un M.C....

La vérification que le futur RCC a pris connaissance des modalités applicables pour l'utilisation du Certificat. Pour cela, l'A.E. vérifie que le Porteur a paraphé et signé le document « Conditions Générales d'utilisation ».

La vérification avec un soin raisonnable de la vraisemblance des pièces constitutives du Dossier de Souscription (Pièces d'identité, mandats, …) ; et en particulier de l'identité du demandeur futur RCC ou M.C. le cas échéant ;

Dans le cas d'une demande via un M.C., celui-ci retransmet le dossier à l'A.E. après avoir effectué les opérations ci-dessus.
L'A.E. effectue ensuite l'archivage du dossier d'enregistrement conformément à « Politique de sauvegarde et d'archivage ».
[OID : 1.3.6.1.4.1.58553.1.2.1.2]
La demande de certificat comporte les éléments mentionnés ci-dessus, ainsi que le nom du service à utiliser dans le certificat.

Le dossier de demande est établi directement par le RUH à partir des éléments fournis par son entité.

L'A.E. vérifie ensuite l'identité du RUH conformément aux exigences précédemment décrites.

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

- Si le dossier est au format papier, sous la forme d'une photocopie signée à la fois par le RUH et par l'A.E., ces signatures étant précédées de la mention « copie certifiée conforme à l'original » ;
- Si le dossier est au format électronique, les différents justificatifs sous une forme électronique ayant valeur légale.

L'A.E. effectue ensuite l'archivage du dossier d'enregistrement conformément à « Politique de sauvegarde et d'archivage ».

4.3.2 Acceptation ou rejet de la demande

[OID : 1.3.6.1.4.1.58553.1.2.1.1]
En cas de problème remonté sur un dossier d'enregistrement, l'A.E. en informe le RCC ou le M.C. par tout moyen mis à sa disposition. Le dossier est mis en attente jusqu'à régularisation.

En cas de rejet de la demande, l'A.E. en informe le RCC ou, le M.C. le cas échéant, par courrier en justifiant le rejet.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

En cas de rejet de la demande, l'AE en informe le RUH, de vive voix ou par courriel, en justifiant le rejet.

En cas d'acceptation de la demande, l'A.E. présente au RUH le DN du futur certificat pour acceptation. Le RUH notifie son acceptation sous la forme d'un accord signé au format papier, conservé par l'A.E.

4.3.3 Durée d'établissement du certificat

L'AC doit s'efforcer de traiter la demande de certificat dans un délai raisonnable. Néanmoins, il n'y a aucune restriction concernant la durée maximale ou minimale de traitement.

4.4 Délivrance du certificat

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

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'A.E., l'A.C. déclenche la génération du certificat.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC produit le certificat et le fournit en main propre au responsable de l'unité d'horodatage.

4.4.2 Notification de la délivrance du certificat au porteur

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

Le RCC est notifié immédiatement par courriel de la génération de son certificat.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

Pas de notification spécifique puisque le responsable de l'unité d'horodatage reçoit le certificat en main propre.

4.5 Acceptation du certificat

4.5.1 Démarche d'acceptation du certificat

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

A la réception de son certificat, Le RCC ou le mandataire doit vérifier que les informations qui sont inscrites sur le certificat sont conformes à ses données suite à cela il signe l'attestation d'acceptation du certificat pour prendre possession du support cryptographique.

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

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

L'acceptation du certificat est réalisée par le responsable de l'unité d'horodatage qui reçoit et vérifie immédiatement le certificat. En cas de refus, le responsable de l'unité d'horodatage demande la révocation du certificat.

4.5.2 Publication du certificat

Les certificats des RCC/RHU ne sont pas publiés par l'AC. Ils peuvent toutefois l'être par le RCC / RHU ou son entité.

4.5.3 Notification aux autres entités de la délivrance du certificat

Sans objet.

4.6 Usages de la bi-clé et du certificat

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

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

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

- À la signature des certificats
- À la signature des CRL.

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

Cet usage est indiqué explicitement dans les extensions des certificats.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

Les clés privées des unités d'horodatage ne sont utilisables que pour signer les contremarques de temps qualifiées produites par les unités d'horodatage du service Damanesign.

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

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

4.7 Renouvellement d'un certificat

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

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

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques.

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

Ainsi les bi-clés des RCC, et les certificats correspondants, seront renouvelés au minimum tous les 2 ans.

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

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

Ainsi les bi-clés des RUH, et les certificats correspondants, seront renouvelés au minimum tous les 5 ans.

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

4.8.1 Origine d'une demande d'un nouveau certificat

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

L'entité peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un RCC / RUH qui lui est rattaché.

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

Voir 4.3 ; toutefois, la vérification d'identité du RCC/RUH est réalisée par l'A.E. conformément au 3.2.

4.8.3 Notification au RCC de l'établissement du nouveau certificat

Voir 4.4.2.

4.8.4 Démarche d'acceptation du nouveau certificat

Voir4.5.

4.8.5 Publication du nouveau certificat

Voir 4.5.2.

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

Voir 4.5.3.

4.9 Modification du certificat

La modification du certificat n'est pas admise.

4.10 Révocation et suspension des certificats

4.10.1 Causes possibles d'une révocation

4.10.1.1 Certificats de cachet

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

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

4.10.1.2 Certificats d'horodatage

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

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

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

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

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

4.10.2 Origine d'une demande de révocation

4.10.2.1 Certificats de cachet

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

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

4.10.2.2 Certificats d'horodatage

Les personnes pouvant demander une révocation de certificat d'horodatage sont :

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

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

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

4.10.3 Procédure de traitement d'une demande de révocation

4.10.3.1 Révocation d'un certificat de cachet

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

La demande de révocation doit comporter au minimum :

- Le prénom et nom du demandeur de la révocation
- Le nom du serveur utilisé dans le certificat
- Le DN du serveur ou toute autre information (par exemple : le numéro de série du certificat) permettant d'identifier de façon certaine le certificat devant être révoqué
- La cause de révocation

Damanesign met à disposition des RCC et des représentants légaux d'entreprises un guichet électronique leur permettant de révoquer leur certificat à tout moment.

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

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

4.10.3.2 Révocation d'un certificat d'horodatage

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

- Les informations du RUH figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat
- Le RUH n'a pas respecté les modalités applicables d'utilisation du certificat
- La clé privée du RUH est suspectée de compromission, est compromise, est perdue ou est volée

- Le RUH ou une entité autorisée (représentant légal de l'entité) demande la révocation du certificat
- Le décès du RUH ou la cessation d'activité de l'entité du RUH
- Rupture technologique, nécessitant de procéder à la génération de nouveaux bi-clés (longueurs des clés trop faibles, algorithmes de hachage compromis)

4.10.3.3 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 l'autorité national (D.G.S.SI) sera immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification.

4.10.4 Délai accordé au porteur pour formuler la demande de révocation

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

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

4.10.5.1 Révocation d'un certificat de cachet

Par nature, une demande de révocation doit être traitée en urgence.

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

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

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

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

La révocation d'un certificat d'une composante de l'IGC doit être effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC (LAR) qui a émis le certificat, et que cette liste est accessible au téléchargement.

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

Le point de contact identifié au sein de l'autorité national (D.G.S.S.I.) doit être immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification.

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

L'utilisateur d'un certificat est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. Il pourra utiliser la dernière LCR publiée par l'AC ou son service OCSP afin de vérifier le statut de révocation du certificat de porteur.

L'utilisateur doit aussi vérifier le statut de révocation des AC de la chaîne de certification en utilisant pour chacune la dernière LAR émise par l'AC de niveau supérieur.

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

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

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 30 minutes et une durée maximale totale d'indisponibilité par mois inférieure à 2 heures.

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

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

4.10.9 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.10.10 Exigences spécifiques en cas de compromission de la clé privée

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

4.10.11 Suspension de certificats

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

4.11 Fonction d'information sur l'état des certificats

4.11.1 Caractéristiques opérationnelles

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

Les LCR / LAR sont publiées à l'adresse spécifiée dans le chapitre 2.2, et à l'adresse contenue dans les certificats émis.

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

4.11.2 Disponibilité de la fonction

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

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) inférieure à 1 heures et une durée maximale totale d'indisponibilité par mois de 4 heures.

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

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

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

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

4.11.3 Séquestre de clé et recouvrement

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

5 Mesures de sécurité non techniques

[PCQSIGN]

6 Mesures de sécurité techniques

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

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés de l'A.C.

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

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

6.1.1.2 Clés porteurs générées par l'A.C.

Sans objet.

6.1.1.3 Clés ocsp générées par l'A.C.

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

6.1.1.4 Clés porteurs générées par le RCC

La bi-clé est obligatoirement dans un environnement sécurisé par L'AC.

6.1.1.5 Clés générées par le RUH pour les unités d'horodatage

La bi-clé est obligatoirement dans un environnement sécurisé par L'AC.

Les unités d'horodatage doivent avoir une seule clé d'horodatage active à la fois.

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet.

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

Sans objet.

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

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

6.1.5 Tailles des clés

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

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

Les clés RSA des certificats de cachet ont une taille de [2048/4096] bits.

Les clés RSA des certificats d'horodatage ont une taille de 3072 bits.

Les clés des certificats OCSP ont ces caractéristiques :

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

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

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

Les bi-clés des serveurs sont générées conformément aux exigences de l'autorité national la D.G.S.S.I.

6.1.7 Objectifs d'usage de la clé

(Voir 1.4.1)

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

L'utilisation de la clé privée des serveurs et du certificat associé est strictement limitée à la création de cachets (voir 1.4.1).

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

L'utilisation de la clé privée et du certificat associé est strictement limitée à la création de contremarques de temps (voir 1.4.1).

Les unités d'horodatage doivent avoir une seule clé d'horodatage active à la fois.

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'A.C.

L'A.C. s'assure que :

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

6.2.1.2 Dispositifs de création de cachet des porteurs

Les dispositifs de création de cachet, pour la mise en œuvre de leurs clés privées, respectent les exigences du chapitre 11 ci-dessous. Le RCC s'engage contractuellement à utiliser un dispositif conforme à ces exigences.

6.2.1.3 Modules cryptographiques pour les unités d'horodatage

Les unités d'horodatage, pour la mise en œuvre de leurs clés privées, respectent les exigences du chapitre 11 ci-dessous. Le RUH s'engage contractuellement à utiliser les modules cryptographiques conforme à ces exigences.

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

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

6.2.3 Séquestre de la clé privée

Sans objet.

6.2.4 Copie de secours de la clé privée

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

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

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

Les clés privées des UH peuvent faire l'objet d'une copie de secours (sauvegarde) ; dans ce cas, cette copie ne peut être restaurée que par le personnel de confiance (porteurs de secrets d'IGC). La sécurité de la sauvegarde est assurée par les mécanismes de sécurité intrinsèques au HSM.

6.2.5 Archivage de la clé privée

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

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

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

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

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

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

6.2.7 Stockage de la clé privée dans un module cryptographique

Le stockage des clés privées d'AC est réalisé dans un module cryptographique répondant aux exigences de la section exigences de sécurité du module cryptographique de l'AC (Annexe 1). Dans le cas des copies de secours, le stockage peut être effectué en dehors d'un module cryptographique moyennant le respect des exigences de la section copie de la clé privée.

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

Le stockage des clés privées des certificat cachet est réalisé dans des supports cryptographiques répondant aux exigences de sécurité du module cryptographique des services de cachet.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

Le stockage des clés privées des unités d'horodatage est réalisé dans un module cryptographique répondant aux exigences de la section exigences de sécurité du module cryptographique de l'AC.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'A.C.

L'activation des clés privées d'A.C. dans un module cryptographique doit être contrôlée via des données d'activation (*cf.* 6.2.8) et doit faire intervenir au moins deux personnes dans des rôles de confiance.

6.2.8.2 Clés privées des RCC

L'activation de la clé privée du RCC est contrôlée via des données d'activation sous la responsabilité du porteur (code PIN).

6.2.8.3 *Clés privées des RUH*

L'activation des clés privées des unités d'horodatage se fera dans un module cryptographique et sera contrôlée via des données d'activation sous la responsabilité du RUH.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 *Clés privées d'A.C.*

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

6.2.9.2 *Clés privées des RCC*

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

6.2.9.3 *Clés privées des RUH*

La désactivation de la clé privée d'une unité d'horodatage est sous le contrôle exclusif du RUH. Ce dernier s'engage à assurer la sécurité des conditions de désactivation de la clé privée dont il est responsable.

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 11. En fin de vie d'une clé privée d'A.C., normale ou anticipée (révocation), cette clé doit être systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.10.2 *Clés privées des RCC*

La destruction de la clé privée d'un serveur est sous le contrôle exclusif du RCC. Ce dernier s'engage à assurer la sécurité des conditions de destruction de la clé privée de scellement dont il est responsable.

6.2.10.3 *Clés privées des RHU*

La destruction de la clé privée d'une unité d'horodatage est sous le contrôle exclusif du RUH. Ce dernier s'engage à assurer la sécurité des conditions de destruction de la clé privée dont il est responsable.

6.2.10.4 *Niveau de qualification du module cryptographique et des dispositifs de création de signature*

Ces exigences sont précisées au chapitre 10.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

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

6.3.2 Durées de vie des bi-clés et des certificats

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

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

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

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

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

Ces opérations sont sous la responsabilité du RCC.

6.4.1.3 Génération et installation des données d'activation correspondant à la clé privée d'un certificat d'horodatage

Ces opérations sont sous la responsabilité du RUH.

6.4.2 Protection des données d'activation

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

6.5 Mesures de sécurité des systèmes informatiques

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

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

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

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

6.6 Mesures de sécurité liées au développement des systèmes

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

6.7 Mesures de sécurité réseau

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

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

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

6.8 Horodatage / Système de datation

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

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

7.1 Certificats de l'A.C.

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	`sha256WithRSAEncryption`

Issuer	`CN = Damanesign Root CA`
	`OU = Damanesign trust services`
	`OU = 154609`
	`O = Damanesign`
	`C = MA`

Validity	30 ans

Subject	`C=MA`
	`O=Damanesign`
	`OI=NTRMA-154609`
	`OU=154609`
	`OU=Damanesign trust services`
	`CN=Damanesign Qualified Seal CA`

Subject Public Key Info	RSA 4096 bits

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

7.2 Certificat de cachet (1.3.6.1.4.1.58553.1.2.1.1)

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	2 ans
Subject	Voir 3.1.2.2
Subject Public Key Info	RSA 2048 bits

Champ	Criticité	Général
Authority Key Identifier	N	Contient l'identifiant de clé de la clé publique de l'AC émettrice (champ *Subject Key Identifier* du certificat de l'AC émettrice). Méthode 1 définie dans la RFC 5280, § 4.2.1.2.

Champ	Criticité	Général
Subject Key Identifier	N	Identifiant de la clé du sujet (AC) Méthode 1 définie dans la RFC 5280, § 4.2.1.2.
Key Usage	O	DigitalSignature , nonRepudiation
Basic Constraints	O	CA: FALSE
Certificate Policies	N	OID: `1.3.6.1.4.1.58553.1.2.1.1` CPS: https://pki.damanesign.ma/cps.html
Subject Alternative Name ***Issuer Alternative Name***	N	Non utilisée
CRL Distribution Points	N	`http://pki.damanesign.ma/crl/ca_qseal_2024.crl`
Authority Information Access	N	`CA:http://pki.damanesign.ma/cert/ca_qseal_2024.crt` `OCSP: http://ocsp.damanesign.ma/ca_qseal`

Champ	Criticité	Général
Qc Compliance	O	`id-etsi-qcs 1`
QcSSCD	O	`id-etsi-qcs 4`
QcType	O	`id-etsi-qct-eseal`

7.3 Certificat d'horodatage (1.3.6.1.4.1.58553.1.2.1.2)

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	5 ans
Subject	Voir 3.1.2.2
Subject Public Key Info	RSA 3072 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	`digitalSignature`
Extended Key Usage	O	`id-kp-timeStamping`
Basic Constraints	O	`CA:FALSE`
Certificate Policies	N	`OID: 1.3.6.1.4.1.58553.1.2.1.2` `CPS: https://pki.damanesign.ma/cps.html`
Subject Alternative Name ***Issuer Alternative Name***	N	Non utilisée
CRL Distribution Points	N	`http://pki.damanesign.ma/crl/ca_qseal_2022.crl`
Authority Information Access	N	`CA: http://pki.damanesign.ma/cert/ca_qseal_2024.crt` `OCSP : http://ocsp.damanesign.ma/ca_qseal`

7.4 Liste de Certificats Révoqués

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Signature	`sha256WithRSAEncryption`

Champ	Contenu
Issuer	C=MA O=Damanesign OI=NTRMA-154609 OU=154609 OU=Damanesign trust services CN=Damanesign Qualified Seal CA
thisUpdate	Date et heure UTC
nextUpdate	Date et heure UTC (1 an de validité)
RevokedCertificates	Liste des numéros de série des certificats révoqués (Couples *UserCertificate-RevocationDate*)
Numéro de LCR	Entier
ExpiredCertsOnCRL	*La 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.*
AuthorityKeyIdentifier	Identifiant de la clé de l'A.C.

7.5 Certificat OCSP

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Signature	Sha256WithRSAEncryption
Issuer	C=MA O=Damanesign OI=NTRMA-154609 OU=154609 OU=Damanesign trust services CN=Damanesign Qualified Seal CA
thisUpdate	Date et heure UTC
nextUpdate	Date et heure UTC (2 ans de validité)
Numéro de série	Défini par l'outil et comprenant une part aléatoire
Longueur des clés	2048 bits
Key Usage	Digital Signature
Extended Key Usage	id-kp-OCSPSigning
Basic Constraints	"CA:false"

7.6 Répondeur OCSP

7.6.1 Requêtes OCSP

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

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

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

7.6.2 Réponses OCSP

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

Champ	Commentaires	Valeur attendue
Version	Version de la requête	0 (version 1)
responderID	Nom du répondeur	Hash de la clé publique du répondeur
producedAt	Heure de production de la réponse	Heure de production à la seconde près
responses – **certID** – **certStatus** – **revocationDate** – **ThisUpdate** – **Next Update** – **ArchiveCutOff**	Statut des certificats identifiés dans la requête	Le statut du certificat est le statut actuel du certificat (thisUpdate est la date courante). La date de révocation est fournie le cas échéant, mais pas la raison de révocation, Date de début de validité du certificat de l'AC (Autorité de Certification)

8 Audits de conformité et évaluations

Voir [PCQSIGN].

9 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

Voir [PCQSIGN].

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

10.1 Exigences sur les objectifs de sécurité

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

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

11 Annexe 2 : Exigences de sécurité du module cryptographique des services de cachet

Le dispositif de protection des éléments secrets utilisé par le service de cachet pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- Si la bi-clé du service applicatif est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée
- Assurer la correspondance entre la clé privée et la clé publique
- Générer un cachet ou une authentification qui ne peut être falsifiée sans la connaissance de la clé privée

Par ailleurs, des mesures de sécurité organisationnelles, procédurales ou techniques doivent être mises en place afin de :

- Détecter les défauts lors des phases d'initialisation, et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de régénération de la clé privée
- Garantir la confidentialité et l'intégrité de la clé privée
- Assurer pour le serveur légitime uniquement la fonction de génération des cachets électroniques et protéger la clé privée contre toute utilisation par des tiers
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif