Politique de certification et Déclaration des pratiques de certification de l'Autorité de certification « Damanesign Seal2 CA »
-Cachet Simple-

Version 1.1 | Diffusion : public

ids: **1.3.6.1.4.1.58553.1.8.1.1 /1.3.6.1.4.1.58553.1.8.1.2**

Historique du document

Version	Date de version	Rédacteur(s)	Approbateur(s)	Modifications
1.0	20/02/2025	Fatimazahrae Jalal	Zouhair HAMDAOUI	Création du document
1.1	04/03/2025	Fatimazahrae Jalal	Zouhair HAMDAOUI	Nouvelle autorité de cachet

Table des matières

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 le cachet Simple" expose les pratiques que la société DAMANESIGN applique dans le cadre de la fourniture de certificats de cachet.
Dans le cadre de son offre de services de confiance, Damanesign fournit un service de génération et de délivrance des Certificats pour le cachet simple, délivrés par une Autorité de Certification appartenant à l'Infrastructure de Gestion de Clés (IGC) Damanesign.
Cette Autorité de Certification est dénommée « Damanesign Seal2 CA » et sera nommée « AC » dans le reste du document.
L'AC Damanesign Seal2 CA ne peut être utilisée que pour :

- Produire des certificats électroniques pour le cachet électronique simple (à la volée) ;
- Produire des certificats électroniques pour l'horodatage simple ;
- Signer des Listes des Certificats Révoqués (LCR) ;

La chaîne de certification est la suivante :

- AC Racine : Damanesign Root CA
  - AC Émettrice : Damanesign Seal2 CA
    - Certificat d'unité d'horodatage

1.2 Identification du document

La présente P.C. est dénommé Déclaration des pratique et Politique de certification de l'autorité « Damanesign Seal2 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 :

1.3.6.1.4.1.58553.1.8.1.1 /1.3.6.1.4.1.58553.1.8.1.2

Dans cette politique de certification, les types de certificats gérés pour le cachet et l'horodatage sont les suivants :
- **[1.3.6.1.4.1.58553.1.8.1.1]** : Les certificats électroniques pour le cachet électronique simple ;
- **[1.3.6.1.4.1.58553.1.8.1.2]** : Les certificats électroniques pour le service d'horodatage simple.

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'IGC

1.3.1 Autorité de certification

L'autorité de certification Damanesign Seal2 CA a la charge de 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 à clés publiques (IGC).
Les prestations de l'AC 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 bi-clés cachet : Cette fonction génère les bi-clés dans une ressource cryptographique matérielle certifiée et hébergée chez Damanesign.

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

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 RCC 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 des serveurs

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, etc.). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR)

Fonction de journalisation et d'audit : ce service permet de collecter l'ensemble des données utilisées et ou générées dans le cadre de la mise en œuvre des services d'IGC afin d'obtenir des traces d'audit consultables. Ce service est mis en œuvre par l'ensemble des composantes techniques de l'IGC.

La présente PC définit les exigences de sécurité pour tous les services décrits ci-dessus dans la délivrance des certificats par les AC aux porteurs. La Déclaration des Pratiques de Certification (notée DPC) donnera les détails des pratiques de l'IGC dans cette même perspective.

Les composantes de l'IGC mettent en œuvre leurs services conformément à la présente PC et la DPC associée.

Les changements majeurs sont notifiés à la DGSSI.

Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

1.3.2 Porteur de certificat

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]

Responsable du certificat de cachet (RCC) : La personne physique responsable du certificat de cachet, notamment de l'utilisation de ce certificat et de la bi-clé correspondante, pour le compte de l'entité dont dépend le serveur informatique identifié dans le certificat.

Le RCC respecte les conditions qui lui incombent définies dans la présente P.C.
Le RCC est par défaut un responsable légal de l'entité sujette. Il peut alternativement être une personne nommée par un représentant légal de l'entité sujette. Dans ce dernier cas, le RCC peut être hiérarchiquement rattaché à l'entité sujette, ou rattaché à une autre entité avec laquelle un lien contractuel ou réglementaire existe. Le RCC peut être amené à changer en cours de validité du certificat (départ du RCC de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.) sans remettre en cause la validité du certificat.
[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
Les porteurs sont les unités d'horodatage du service Damanesign, représentés par le responsable des unités d'horodatage.

1.3.3 Mandataire de certification (MC)

Le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des RCC.
Le recours à un mandataire de certification (MC) n'est pas obligatoire pour une entité. Une même entité peut s'appuyer sur un ou plusieurs MC. Dans le cas où elle y a recours, le MC doit être formellement désigné par un représentant légal de l'entité concernée. Le MC est en relation directe avec l'AE de l'IGC.
Les engagements du MC à l'égard de l'AC sont précisés dans un contrat avec l'entité responsable du MC.
Ce contrat stipule notamment que le MC doit :

- Effectuer correctement et de façon indépendante les contrôles d'identité et des éventuels attributs des futurs RCC et serveurs informatiques de l'entité pour laquelle il est MC,
- Respecter les parties de la PC et de la DPC de l'AC qui lui incombent.
- L'entité doit signaler à l'AC, si possible préalablement mais au moins sans délai, le départ du MC de ses fonctions et, éventuellement, lui désigner un successeur.

1.3.4 Utilisateur de certificat

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]
L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une valeur de cachet provenant du serveur auquel le certificat est rattaché.
Un utilisateur est une personne physique ou morale ayant accès à un fichier signé, dont le cachet a été générée par la clé privée d'un certificat émis par l'AC couverte par ces CGU. Il est à noter qu'aucun lien direct n'existe entre la société Damanesign et un utilisateur.
Cette PC traite des certificats de cachet, un utilisateur de certificats peut être :

- Un agent (personne physique) destinataire de données signées par un serveur informatique et qui utilise un certificat et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises par le serveur identifié dans le certificat. L'agent respecte la politique et les pratiques de sécurité édictées par le responsable de son entité.
- Un usager destinataire de données provenant d'un serveur informatique et qui utilise un certificat et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises par le serveur identifié dans le certificat.

- Un serveur informatique destinataire de données provenant d'un autre serveur informatique et qui utilise un certificat et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises par le serveur identifié dans le certificat.

[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
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 apposée sur ces données.

1.3.5 Personne autorisée

Il s'agit d'une personne autre que le RCC et le mandataire de certification et 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 RCC (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du RCC ou d'un responsable des ressources humaines.

1.3.6 La Déclaration des Pratiques de Certification (DPC)

Décrit l'organisation opérationnelle de l'IGC et la répartition des rôles entre les différentes composantes en fonction de l'organisation fonctionnelle et de la définition des rôles décrites dans sa PC.
L'organisation et l'ordonnancement des différentes fonctions de l'IGC les unes par rapport aux autres dépendent du modèle adopté par l'AC.
Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, les exigences qui incombent à l'AC en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- Être une entité légale au sens de la loi marocaine
- Être en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats de cachet de cette entité. L'AC peut aussi, le cas échéant, être en relation contractuelle / hiérarchique / réglementaire avec le ou les mandataires de certification choisis par l'entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de ses clientes, aux RCC, aux utilisateurs de certificats, ceux 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.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions obligatoires de la présente PC, notamment en matière de génération des certificats, de remise au RCC, 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 PC, notamment en termes de fiabilité, de qualité et de sécurité. À ce titre, elle possède un système de gestion de la qualité et de la sécurité de l'information adaptés aux services de certification qu'elle assure
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR), Diffuser ses certificats d'AC aux RCC et utilisateurs de certificats.
- Suivre les demandes en capacité et réaliser des projections concernant les futurs besoins en capacité afin de garantir la disponibilité du service, notamment en matière de capacités de traitement et de stockage.

1.3.7 Autorité d'enregistrement.

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]

L'AE est utilisée pour la mise en œuvre des services d'enregistrement de demandes de certificats, de remise de certificats, de remise au RCC, de révocation de certificats et journalisation et d'audit. L'AE est chargée d'authentifier et d'identifier les RCCs, et les personnes autorisées. L'AE est mise en œuvre par Damanesign. Pour cela, l'AE assure les tâches suivantes :

- La prise en compte et la vérification des informations du futur RCC et du serveur informatique, ainsi que de leur entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- Le cas échéant, la prise en compte et la vérification des informations du futur MC et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- L'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC suivant l'organisation de cette dernière et les prestations offertes ;
- La conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du RCC ou, le cas échéant, du MC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles)

L'AE peut s'appuyer sur un MC désigné et placé sous la responsabilité de l'entité cliente pour effectuer tout ou partie des opérations de vérification des informations.
Dans ce cas, l'AE doit s'assurer que les demandes sont complètes et exactes et effectuées par un MC dûment autorisé.
Dans tous les cas, l'archivage des pièces du dossier d'enregistrement (sous forme électronique) est de la responsabilité de l'AE.

[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]

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.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

La présente PC traite des bi-clés et des certificats émis à la demande d'un RCC ou/et au responsable des unités d'horodatage, afin que des entités puissent sceller/horodaté électroniquement des

données, dans le cadre d'échanges dématérialisés avec les catégories d'utilisateurs de certificats identifiées à la section « Entités intervenant dans l'IGC ».

☐ *Bi-clés et Certificat des AC*

Le certificat de l'AC sert à authentifier les certificats cachet serveur. La clé privée associé au certificat d'AC sert pour :

- La signature de certificat cachet serveur ;
- La signature de certificat d'horodatage
- La signature de LCR.

☐ *Bi-clés et Certificat de porteur*

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]

La présente PC traite des bi-clés et des certificats utilisés par le service de cachet électronique Damanesign qu'elle fournit à ses clients dont la fonction est de signer des données au nom de la personne morale du client, afin que les catégories d'utilisateurs de certificats identifiées au chapitre 1.3.4 ci-dessus puissent en vérifier le cachet.

Ceci correspond notamment :

- Apposition d'un cachet sur des données par un serveur informatique et vérification de ce cachet par un usager,
- L'utilisation de la clé privée du serveur et du certificat associé doit rester strictement limitée au cachet de données émises par le serveur informatique identifié dans le certificat.
- L'utilisateur du certificat a ainsi l'assurance que le serveur informatique identifié dans le certificat est bien l'émetteur des données reçues. Le niveau d'assurance dépend, notamment, des moyens mis en œuvre par l'AC tout au long du cycle de vie du certificat, ainsi que des mesures prises pour protéger la clé privée au niveau du serveur.

Il est rappelé que l'utilisation de la clé privée par le RCC et du certificat associé doit rester strictement limitée au service de cachet de document et de validation de cachet de document. Dans le cas contraire, leur responsabilité pourrait être engagée.

[Horodatage Simple : 1.3.6.1.4.1.58553.1.8.1.2]

Les certificats d'horodatage ne sont utilisables que pour signer les contremarques produites par les unités d'horodatage du service Damanesign.

1.4.2 Domaines d'utilisation interdits

Ces certificats ne peuvent pas être utilisés pour un usage à titre personnel, vers des domaines d'usage non explicitement autorisés.

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

Tout domaine d'application n'étant pas prévu dans le chapitre précédent, est interdit. De plus, les usages du certificat doivent être en conformité avec la législation et la réglementation.

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

Damanesign est chargé de la validation et de la gestion de la Politique de Certification (PC/DPC), sous la responsabilité du Responsable de la Certification Électronique (Responsable d'AC).

1.5.2 Point de contact

Les demandes d'informations ou commentaires sur cette Politique de Certification 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 D.P.C.

Damanesign utilise ses propres méthodes pour approuver le présent document et les résultats de la revue de conformité effectuée par les experts qu'elle nomme à cet effet.
La conformité de la DPC/ PC est prononcée par l'A.C. au vu des résultats des audits internes effectués.
Cette approbation suit une procédure bien définie. La DPC/PC est revue régulièrement, au minimum une fois par an, par le comité de pilotage de la gouvernance de l'IGC.

1.6 Définitions et acronymes

1.6.1 Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

AC	Autorité de Certification
ACR	Autorité de Certification Racine
ACS	Autorité de Certification Subordonnée
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
AH	Autorité d'Horodatage
CN	Common Name
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
DSA	Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés.
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
UH	Unité d'Horodatage
O	Organization
OC.	Opérateur de Certification

OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PC	Politique de Certification
PP	Profil de protection
PSCE	Prestataire de Services de Certification Electronique
RCC	Responsable du Certificat de Cachet.
RFC	Request For Comment
RSA	Rivest Shamir Adelman
SP	Servcie de publication
SHA-2	Secure Hash-Algorithm Two
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Universal Ressource Locator
X.509	Format des certificats d'identité recommandé par l'Union Internationale des Télécommunications (UIT).

1.6.2 Définitions

Les termes utilisés dans la présente PC sont les suivants :

Agent : Personne physique agissant pour le compte d'une autorité administrative.
Applicatif de vérification de cachet : Il s'agit de l'application mise en œuvre par l'utilisateur pour vérifier le cachet des données reçues à partir de la clé publique du serveur contenue dans le certificat correspondant.
Applications utilisatrices : Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins de signature de cachet du serveur auquel le certificat est rattaché.
Autorités administratives : Ce terme générique désigne les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.
Autorité d'enregistrement (AE) : voir chapiter 1.3.7
Autorité d'horodatage (AH) : Autorité responsable de la gestion d'un service d'horodatage.
Autorité de certification (AC) : Au sein d'un Prestataire de Service de Certification Électronique (PSCE), une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et le terme d'AC est le seul utilisé.
Authentification : Processus permettant de vérifier l'identité déclarée d'une personne ou de tout autre entité, ou de garantir l'origine de données reçues.
Bi-clé : Une bi-clé est un couple composé d'une clé privée (devant être tenue secrète) et d'une clé publique, nécessaire à la mise en œuvre de techniques cryptologiques basées sur des algorithmes asymétriques (RSA ou DSA par exemple).

Certificat électronique : Fichier électronique attestant qu'une 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'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.
Certificat d'AC : Certificat d'une autorité de certification.
Chaîne de confiance : Ensemble des certificats nécessaires pour valider la généalogie d'un certificat final.
Clé privée : partie secrète d'une bi-clé détenue par son propriétaire. Cette partie de la clé ne doit pas être divulguée.
Clé publique : partie publique d'une bi-clé mise à la disposition des tierces parties pour pouvoir valider l'utilisation d'un certificat.
Common Name (CN) : Identité réelle ou pseudonyme d'un Porteur, d'un Serveur ou d'une AC.
Compromission : Divulgation, modification, substitution ou utilisation sans autorisation de données confidentielles (y compris les clés cryptographiques et d'autres paramètres de sécurité fondamentaux).
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'IGC.
Dispositif de création de cachet : Il s'agit du dispositif matériel et/ou logiciel utilisé par le serveur pour stocker et mettre en œuvre sa clé privée pour la création de cachet.
Distinguished Name (DN) : Nom distinctif X.500 du Porteur, du Serveur ou de l'AC pour lequel le certificat est émis.
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.
Famille de certificats : Ensemble des certificats émis et gérés suivant une Politique de Certification particulière de l'AC.
Fonction de génération des certificats : voir Chapitre 1.3.1
Fonction de génération des éléments secrets du serveur : voir Chapitre 1.3.1
Fonction de gestion des révocations : voir Chapitre 1.3.1
Fonction de publication :voir Chapitre 1.3.1
Fonction d'information sur l'état des certificats :voir Chapitre 1.3.1
Fonction de remise au RCC :voir Chapitre 1.3.1
HSM (Hardware Security Module) : Boîtier cryptographique matériel dans lequel sont stockées les clés publiques et privées des Autorités de Certification.
Infrastructure de Gestion de Clés (IGC) : Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.
Liste des Autorités Révoquées (LAR) : Liste contenant les identifiants des certificats d'autorités subordonnées révoquées ou invalides.

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

OID : Identificateur numérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.

Système d'information : Tout ensemble de moyen destiné à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives elles-mêmes.

Mandataire de certification : voir Chapitre 1.3.3

Personne autorisée : voir chapitre 1.3.5

Politique de certification (PC) : Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles un AC 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 PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs, les responsables de certificats et les utilisateurs de certificats.

Prestataire de services de certification électronique (PSCE) : 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 PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins un AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Subordonnées). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC 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.

Renouvellement d'un Certificat : Opération effectuée à la demande d'un Porteur ou d'un Responsable de Certificat ou en fin de période de validité d'un Certificat et qui consiste à générer un nouveau Certificat.

Révocation d'un Certificat : Opération dont le résultat est la suppression de la caution de l'AC sur un Certificat donné, avant la fin de sa période de validité exclusivement.

La demande peut être la conséquence de différents types d'événements tels que la compromission d'une bi-clé, le changement d'informations contenues dans un certificat, etc.

L'opération de révocation est considérée terminée quand le certificat mis en cause est publié dans la Liste des Certificats Révoqués. Le certificat est alors inutilisable.

Responsable du certificat de cachet : voir Chapitre 1.3.2.

Serveur informatique : Il s'agit d'un service applicatif (disposant d'un certificat fourni par l'AC) rattaché à l'entité, (identifiée dans le certificat) détenant le nom de domaine correspondant au service ou en charge de ce service

Usager : Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives.
Utilisateur de certificat : L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du porteur du certificat.
Validation de certificat : Opération de contrôle du statut d'un Certificat ou d'une chaîne de certification.

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 RCC et utilisateurs de certificats :

- La présente politique de certification ;
- Les certificats de l'Autorité de Certification "Damanesign Seal2 CA" et l'AC Racine ;
- La liste des certificats révoqués (LCR) ;
- La liste des autorités révoquées (LAR).

De plus compte tenu de la complexité de lecture d'une PC pour des personnes non spécialistes du domaine, il est obligatoire que l'AC publie également des conditions générales d'utilisation (CGU).

L'AC a également pour obligation de publier, à destination des RCC, les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.)

Il est recommandé que ces conditions générales reprennent ainsi, à destination des RCC et des utilisateurs de certificats, les informations pertinentes de la PC de l'AC :

- Les conditions d'usages des certificats et leurs limites,
- L'identifiant : OID de la PC applicable,
- Les obligations et responsabilités des différentes parties, notamment les exigences relatives à la vérification du statut de révocation d'un certificat pour les utilisateurs,
- Les garanties et limites de garanties de l'AC,
- Les informations sur comment vérifier un certificat,
- La durée de conservation des dossiers d'enregistrement et des journaux d'évènements,
- Les procédures pour la résolution des réclamations et des litiges,
- Le système légal applicable.

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_seal2_2025.crt

2.2.2 Publication de la CRL

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

http://pki.damanesign.ma/crl/ca_seal2_2025.crl

2.3 Délais et fréquences de publication

Les délais et fréquences de publication sont les suivants :

- La fréquence de publication des PC/DPC Damanesign sont décrites dans chaque PC/DPC.
- La PC/DPC est publiée avant toute émission d'un certificat final contenant l'OID correspondant;
- Les LCR/LAR sont publiées quotidiennement ;
- Les certificats d'AC sont publiés suite à leur émission et avant toute signature d'un certificat final ;
- Les CGU Damanesign sont publiées suite à chaque mise à jour.

Ces informations sont disponibles sept jours sur sept, vingt-quatre heures sur vingt-quatre, avec une disponibilité de 99.7% sur un mois. Le Comité de Direction Technique Damanesign décide des différentes parties (clients, utilisateurs, sous-traitants de la fourniture du service, organismes de contrôle…) à informer lors de la publication effective ou à venir d'une nouvelle PC (version initiale ou modification d'une PC existante) selon la nature des évolutions apportées. En particulier, les clients de Damanesign, les porteurs et les utilisateurs de certificats sont informés des changements à venir dès lors que l'évolution est susceptible d'affecter leur adhésion au service.
Il est à noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une indisponibilité de cette information.

2.4 Contrôle d'accès aux informations publiées

Toutes les informations mentionnées ci-dessus sont publiques et n'ont aucune restriction d'accès. L'accès en modification aux données publiées est limité aux équipes internes de Damanesign, responsables de la publication des documents dans l'espace dédié. Un contrôle d'accès strict et nominatif est en place, respectant les politiques de Damanesign, conformes aux exigences réglementaires en vigueur.

2.5 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

Cachet) 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 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.

- **Certificat de l'AC :**

L'identité de l'AC dans le certificat est donnée dans le chapitre de profiles des certificats et des LCR. Voir chapitre 7

- **Certificat Cachet :**

L'identité du porteur dans le certificat est donnée dans le chapitre de profiles des certificats et des LCR. Voir chapiter 7

- **Certificat Horodatage :**

L'identité de l'unité d'horodatage dans le certificat est donnée dans le chapitre de profiles des certificats et des LCR. Voir chapitre 7

Les certificats de test émis par l'AC Damanesign Seal2 CA sont identifiables immédiatement par l'ajout du préfixe « TEST – » dans la valeur de l'attribut CN.
En dehors de cette spécificité, les certificats de tests émis par l'AC Damanesign Seal2 CA suivent les mêmes processus que les certificats de production nominale.

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les services de création de cachet dans les certificats sont explicites. L'identification de l'entité à laquelle ce service est rattaché est obligatoire.

3.1.3 Anonymisation ou pseudonymisation des services de création de cachet

Les noms utilisés dans un certificat ne peuvent pas comporter de pseudonymes ou des données anonymes.

3.1.4 Règles d'interprétations des différentes formes de noms

Les règles d'interprétation des différentes formes de nom sont explicitées dans la section décrivant le profil des Certificats et des LCR.

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.
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.

3.1.6 Identification, authentification et rôle des marques déposées

L'AE se réserve le droit de suspendre la génération d'un certificat si le CN est susceptible d'être lié ou de porter préjudice à un quelconque titre ou droit de propriété intellectuelle. Si un tel cas arrive, l'AE demandera au RCC les informations et documents démontrant la légitimité de son CN. A défaut, le RCC devra demander la génération d'un nouveau certificat avec une modification du CN permettant d'éviter la reprise et résoudre le litige.

3.2 Validation initiale de l'identité

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]
La procédure d'enregistrement d'un service de création de cachet pour une entité, auquel un certificat doit être délivré, s'effectue par le biais de l'enregistrement du RCC correspondant.
Si le RCC change au cours de la validité du certificat de cachet, tout nouveau RCC doit également être enregistré selon la même procédure.
L'enregistrement d'un RCC et du serveur informatique associé peut être réalisé soit directement auprès de l'Autorité de Certification (AE), soit par l'intermédiaire d'un mandataire de certification de l'entité. Dans ce dernier cas, le mandataire doit être préalablement enregistré par l'AE.
La validation initiale de l'identité d'une entité ou d'une personne physique s'effectue dans les cas suivants :
1. **Enregistrement d'un RCC sans MC pour un certificat de cachet à émettre** : L'AE valide l'identité de l'entité (personne morale) à laquelle le RCC est rattaché, l'identité de la personne physique désignée comme RCC, ainsi que son habilitation à remplir ce rôle pour le service de création de cachet et l'entité concernée.
2. **Enregistrement d'un nouveau RCC sans MC pour un certificat de cachet déjà émis** : L'AE valide l'identité de la personne physique désignée comme nouveau RCC et son habilitation à remplir ce rôle pour le service de création de cachet et l'entité concernée.
3. **Enregistrement d'un MC** : L'AE valide l'identité de l'entité (personne morale) pour laquelle le MC interviendra, l'identité de la personne physique désignée comme MC, ainsi que son lien avec l'entité.
4. **Enregistrement d'un RCC via un MC pour un certificat de cachet à émettre ou d'un nouveau RCC pour un certificat de cachet déjà émis** : Le MC valide l'identité de la personne physique désignée comme RCC, ainsi que son habilitation à remplir ce rôle pour le service de création de cachet et l'entité concernée.

[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
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.

3.2.1 Méthode pour prouver la possession de la clé privée

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]

La bi-clés associée du porteur est générée et stockée d'une manière sécurisée par les servers de Damanesign après l'aboutissement du processus de la validation d'identité du demandeur par l'AE. La génération des clés publique et privée du certificat Cachet serveur se fait dans le serveur de la plateforme Damanesign APP. Dans ce PC/DPC, le cachet serveur sera conservé sur les servers Damanesign. Cependant, le secret du cachet serveur sera sous le contrôle direct du responsable du cachet serveur.

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

[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]

Le responsable de l'unité d'horodatage présente une CSR signée avec la clé privée de l'UH.

3.2.2 Validation de l'identité d'un organisme

Les informations concernant la structure à laquelle le RCC est rattaché font l'objet de vérification lors de l'enregistrement (existence, validité, ...).

3.2.3 Validation de l'identité d'un individu.

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]

Pour l'enregistrement d'une demande de certificat Cachet Serveur simple déposé directement auprès de l'AE, l'AE réalise les opérations suivantes :

- Vérifier l'identité de la personne morale et son représentant légal en demandant obligatoirement dans le dossier d'enregistrement :
- Un extrait officiel du registre de commerce délivré dans une date ne dépassant pas trois mois
- Un justificatif ou une attestation de domiciliation
- Vérifier l'identité du responsable du certificat en demandant obligatoirement une copie d'un document officiel en cours de validité justifiant son identité et comportant son nom, prénom, photo, date et lieu de naissance, sinon. Un document de procuration signé par le reprenant légal désignant nominativement le responsable du certificat pour demander des certificats cachet serveur le compte de la personne morale,
- Si le représentant légal dispose d'un certificat qualifié en son nom, il peut signer électroniquement le document de la procuration,
- Demander obligatoirement au responsable du certificat une adresse mail et son numéro gsm.

En outre, l'AE se réserve le droit de demander d'autre pièces justificatives et\ou recourir à des méthodes supplémentaires pour vérifier l'identité des personnes morales et responsables du certificat Cachet Serveur.

[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
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.

3.2.4 Informations non vérifiées du RCC et/ou du serveur informatique

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

3.2.5 Validation de l'autorité du demandeur

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]
Cette étape est effectuée en même temps que la validation de l'identité du responsable de certificat.
[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
L'AE vérifie dans l'organigramme interne que le demandeur est bien responsable de l'unité d'horodatage.

3.2.6 Certification croisée d'AC

Sans Objet.

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

Pour garantir la sécurité des transactions numériques, il est important de renouveler régulièrement les bi-clés. Lors de ce renouvellement, un nouveau certificat est automatiquement créé et délivré à l'utilisateur. Il est important de noter que la fourniture d'un nouveau certificat de signature cachet au RCC ne peut se faire qu'après le renouvellement de la bi-clé correspondante. Cette mesure de sécurité vise à garantir l'intégrité et la fiabilité des signatures numériques.

3.3.1 Identification et validation pour un renouvellement courant

Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales (se reporter au § 3.2 ci-dessus). Lors du premier renouvellement, l'AC doit au minimum s'assurer que les informations du dossier d'enregistrement initial sont toujours valides et que le certificat à renouveler existe, et est toujours valide. Lors du premier renouvellement, le RCC/RUH signe la demande de certificat et est authentifié par l'AE à l'aide des informations recueillies lors de la première demande.

Lors du renouvellement suivant, l'AE, saisie de la demande, identifiera le RCC/RUH selon la même procédure que pour l'enregistrement initial ou une procédure offrant un niveau de garantie équivalent.

3.3.2 Identification et validation pour un renouvellement après révocation

Lorsqu'un certificat est définitivement révoqué, la procédure pour demander un nouveau certificat est la même que celle de l'enregistrement initial.

3.4 Identification et validation d'une demande de révocation

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]

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

- **Révocation via téléphone** : l'utilisateur pourra contacter Damanesign par téléphone afin de demander la révocation de son certificat. Pour ce faire, Damanesign s'assure de son identité. Une série de 2 questions aléatoires concernant son identité sera posée au RCC. Ces questions seront fondées sur les informations en possession de Damanesign. La validation sera effective, suite à une confirmation obtenue via un autre canal que l'appel téléphonique. Par exemple, nous pouvons lui envoyer un lien de confirmation sur son adresse courrier électronique.
- **Révocation par courriel** : l'utilisateur pourra contacter Damanesign par mail afin de demander la révocation de son certificat. Pour ce faire, Damanesign s'assure de son identité. Une série de 2 questions aléatoires concernant son identité sera posée au porteur. Ces questions seront fondées sur les informations en possession de Damanesign. La validation sera effective, suite à une confirmation obtenue via un autre canal que le mail. Par exemple, nous pouvons : lui envoyer un code sur son numéro de téléphone o effectuer un appel téléphonique pour avoir une confirmation
- **Révocation par courrier** : une demande pourra être faite par courrier, via une lettre recommandée avec accusé de réception. La demande écrite doit être signée par le RCC, ou par un responsable de l'entité de rattachement du RCC.

[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]

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.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]

L'obtention d'un certificat est conditionnée par une demande formulée par le représentant légal de l'entité concernée ou par un mandataire dûment mandaté à cet effet.

Il est impératif que le futur RCC exprime son consentement préalable à la demande de certificat, quelle que soit la personne qui la dépose.

[1.3.6.1.4.1.58553.1.8.1.2]

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

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

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]
La constitution d'un dossier de demande de certificat électronique nécessite l'inclusion des informations suivantes :

- Le nom du service de création de cachet électronique à utiliser.
- Les données personnelles d'identification du Responsable de Certificat cachet (RCC).
- Les données d'identification de l'entité à laquelle appartient le RCC. Ces informations ne sont pas requises si la demande est effectuée par l'intermédiaire d'un Mandataire de certification.

Le dossier de demande peut être établi par le futur RCC à partir des éléments fournis par son entité ou par l'entité elle-même. Dans tous les cas, le dossier doit être signé par le futur RCC.
En l'absence de Mandataire **(MC)** au sein de l'entreprise, le dossier de demande est transmis directement à l'Autorité d'Enregistrement (AE).
Si l'entreprise a désigné un Mandataire, le dossier de demande lui est remis pour qu'il puisse le compléter et le transmettre à l'AE.
L'AE doit s'assurer qu'elle dispose des coordonnées du Mandataire Certifié ou du futur RCC afin de faciliter la communication en cas de besoin.
[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
Les informations suivantes doivent au moins faire partie de la demande de certificat (cf. section validation initiale de l'identité) :

- La CSR comportant le nom complet de l'unité d'horodatage ;
- 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.

4.2 Traitement d'une demande de certificat

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

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]
Conformément au chapitre 3.2, les identités "personne physique" et "personne morale" font l'objet d'une vérification approfondie.
L'AE, ou le MC le cas échéant, doit effectuer les opérations suivantes :

- Valider l'identité du futur RCC ;
- Vérifier la cohérence des justificatifs présentés ;
- S'assurer que le futur RCC a pris connaissance des modalités applicables pour l'utilisation du certificat (voir les conditions générales d'utilisation).

Si la demande est faite par un Mandataire de certification (MC), il vérifie les informations et la transmet à l'Autorité d'Enregistrement (AE). L'AE vérifie que la demande correspond bien au mandat du MC.
Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat et, le cas échéant, de la bi-clé vers la fonction adéquate de l'IGC.
L'AE conserve ensuite une trace des justificatifs présentés :

- Si le dossier est au format papier, sous la forme d'une photocopie signée à la fois par le futur RCC et par l'AE, ou le MC le cas échéant ;

- Si le dossier est au format électronique, les différents justificatifs sous une forme électronique ayant valeur légale.

[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
L'AE vérifie en face à face l'identité du responsable de l'unité d'horodatage et sa fonction dans l'organigramme Damanesign.

4.2.2 Acceptation ou rejet de la demande

En cas d'approbation de la demande, l'AE (service d'enregistrement) transmet la demande à l'AC (service de génération de certificat).
En cas de rejet de la demande, l'AE en informe le RCC/MC/ responsable de l'unité d'horodatage (en fonction de l'origine de la demande) en justifiant le rejet.

4.2.3 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.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]
Une fois l'origine de la demande et son intégrité vérifiées par l'Autorité de Certification (AC) provenant de l'Autorité d'Enregistrement (AE), l'AC lance les processus de génération et de préparation des différents éléments nécessaires à l'utilisation du certificat cachet dans le processus de cachet électronique pour le client.
L'AC génère la paire de clés (bi-clé) du serveur. Le processus de génération du certificat est lié de manière sécurisée à la génération de la bi-clé, garantissant l'ordonnancement des opérations et, en fonction de l'architecture de l'Infrastructure à Clé Publique (PKI), l'intégrité et l'authentification des échanges entre les composants.

[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
À la suite de 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.

4.3.2 Notification par l'AC de la délivrance du certificat au RCC

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]
La notification de génération du certificat est transmise par message électronique à une adresse fournie par le RCC.
[1.3.6.1.4.1.58553.1.8.1.2]
Pas de notification spécifique puisque le responsable de l'unité d'horodatage reçoit le certificat en main propre.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]
Dès que le RCC a récupéré son certificat, l'AC considère le certificat comme accepté.
Si le RCC ne souhaite pas accepter son certificat, alors il dispose d'un délai de 15 jours pour manifester son non-consentement auprès de l'AE. Passé ce délai, le certificat est considéré comme accepté.
[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
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.

4.4.2 Publication du certificat

Les certificats des AC sont publiés par Damanesign.
Le certificat Cachet Serveur est publié dans les documents cachetés par ce certificat.
Le certificat d'horodatage est publié par l'Autorité de certification Damanesign avant son utilisation, conformément aux dispositions prévues dans la Politique d'Horodatage Damanesign.

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

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]
Seuls les responsables du certificat Cachet Serveur sont notifiés.
[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
L'AC notifie le responsable de l'entité de l'horodatage de la génération de certificat.

4.5 Usage de la bi-clé et du certificat

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

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.
[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]
L'utilisation de la clé privée et du certificat associé est strictement limitée au service de cachet de données émises par le serveur. Les RCC doivent s'assurer du respect strict des usages autorisés des bi-clés et des certificats au niveau des serveurs. Dans le cas contraire, leur responsabilité pourrait être engagée.
L'usage autorisé de la bi-clé du serveur et du certificat associé est indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.
Cet usage est indiqué explicitement dans les extensions des certificats au sens X509 du terme :

- Key Usage : **Digital Signature et Non Répudiation**.

[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
Les clés privées des unités d'horodatage ne sont utilisables que pour signer les contremarques produites par les unités d'horodatage du service Damanesign.

4.5.2 Utilisation de la clé publique et du certificat par Le porteur du certificat

Voir chapitre précédent et chapitre 1.4

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats Cachet Serveur. Ils doivent respecter obligatoirement :

- Vérifier que l'extension « KeyUsage » contenue dans le certificat Cachet serveur 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 Cachet Serveur ;
- Vérifier la validité de la chaîne de certification (dates de validité, signature des certificats statut de révocation) en partant du certificat Cachet Serveur et en remontant jusqu'à certificat de l'AC Racine.

[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]

Les certificats des unités d'horodatage sont utilisés pour vérifier la validité des jetons d'horodatage (des dispositions sont prévues dans la Politique d'Horodatage Damanesign).

4.6 Renouvellement d'un certificat

La présente politique de certification (PC) exige que le renouvellement d'un certificat s'accompagne du renouvellement de la paire de clés cryptographiques (bi-clé) correspondante. L'autorité de certification (AC) étant responsable de la génération des bi-clés des serveurs, elle s'assure qu'un certificat lié à une bi-clé existante ne puisse être renouvelé conformément aux directives du RFC 3647.

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

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

4.7.1 Causes possibles de changement d'une Bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des serveurs et les certificats correspondants seront renouvelés au minimum tous les 3 ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du serveur (voir chapitre 4.9, notamment le chapitre 4.9.1 pour les différentes causes possibles de révocation).

4.7.2 Origine d'une demande d'un nouveau certificat

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]

Le déclenchement de la fourniture d'un nouveau certificat de cachet peut être automatique ou bien à l'initiative du RCC

[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]

Les paires de clés et les certificats associés des responsables unité d'horodatage sont renouvelés au moins tous les cinq ans. De plus, un renouvellement anticipé peut avoir lieu si le certificat est révoqué.

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

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre 3.3 ci-dessus. Pour les actions de l'AC, voir chapitre 4.3.1.

4.7.4 Notification de l'établissement du nouveau certificat

Voir chapitre 4.3.2

4.7.5 Démarche d'acceptation du nouveau certificat

Voir chapitre 4.4.1

4.7.6 Publication du nouveau certificat

La publication du nouveau certificat se fera de la même façon qu'à l'enregistrement initial.

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

La notification se fera de la même façon qu'à l'enregistrement initial.

4.8 Modification du certificat

La modification de certificat correspond à une révocation de l'ancien certificat et la génération d'un nouveau.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

- **Certificat Composante IGC**

L'AC précise dans sa DPC les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen l'ensemble des RCC concernés que leurs certificats cachet correspondants ne sont plus valides. Pour cela, l'IGC envoie des récépissés aux AE et aux MC. Ces derniers informent les RCC en leur indiquant explicitement que leurs certificats cachet ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

- **Certificats Porteur**

Un certificat est révoqué quand l'association la clé publique et l'identité qu'il certifie n'est plus considérée comme étant valide. Les motifs qui invalident cette association sont :

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- Le demandeur, RCC ou le MC n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;
- La cessation d'activité du Client ou la fin d'activité du serveur ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;
- La révocation de l'AC qui a émis le certificat ;

- La fin de vie de l'AC qui a émis le certificat ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

Quand l'une de ces occurrences se produit, le certificat en question doit être révoqué.

4.9.2 Origine d'une demande de révocation

❑ **Certificat Composante IGC**

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.
La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

❑ **Certificats de cachet**

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

- Le RCC du certificat de cachet ;
- Un représentant légal de l'entité ;
- L'AC émettrice du certificat ou l'une de ses composantes (AE).

Nota : le RCC doit être informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son certificat.

❑ **Certificats d'horodatage**

- L'AC émettrice du certificat
- Le responsable de l'unité d'horodatage Damanesign.

4.9.3 Procédure de traitement d'une demande de révocation

❑ **Révocation d'un certificat d'une composante de l'IGC**

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

❑ **Révocation d'un certificat de porteur ;**

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre Identification et validation d'une demande de révocation.
La demande de révocation est opérée auprès de l'AE ou de l'AC
Les informations suivantes doivent figurer dans la demande de révocation de certificat :

- Le nom du serveur utilisé dans le certificat ;

- Le nom du demandeur de la révocation ;
- Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série...) ;
- Eventuellement, la cause de révocation.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats.
L'information de révocation est diffusée via une LCR signée par une entité désignée par l'AC.
Le demandeur de la révocation est informé du bon déroulement de l'opération et de la révocation effective du certificat.

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]
De plus, si le RCC n'est pas le demandeur, il est également informé de la révocation effective de ce certificat. L'entité, directement ou via son MC le cas échéant (au choix de l'entité), est informée de la révocation de tout certificat de cachet qui lui sont rattachés.
L'opération est enregistrée dans les journaux d'évènements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

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

4.9.5 Délai de traitement par l'AC d'une demande de révocation

- **Révocation d'un certificat d'une composante de l'IGC**

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 qui a émis le certificat, et que cette liste est accessible au téléchargement. La révocation d'un certificat de signature de l'AC (signature de certificats et de LCR / LAR) sera effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

- **Révocation d'un certificat porteur ;**

Par nature une demande de révocation est traitée en urgence.
La fonction de gestion des révocations est disponible 24/24.
Cette fonction a une durée maximale d'indisponibilité par interruption de service d'une heure et une durée maximale totale d'indisponibilité par mois de 4h.

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]
Toute demande de révocation d'un certificat de cachet est traitée dans un délai inférieur à 24h, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

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

L'utilisateur d'un certificat porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. Il pourra utiliser la dernière LCR publiée.

4.9.7 Fréquence d'établissement des LCR

La fréquence de publication des LCR est la suivante :

- Configuration des LCR :
  - Période de publication : 1 jours ;
  - Overlap (marge) : 0 minutes ;
  - Durée de validité : 1 jours ;

4.9.8 Délai maximum de publication d'une LCR

Lorsque l'information sur l'état de la révocation d'un certificat est assurée au travers de la mise en place d'un service de publication de LCR et, le cas échéant, de Delta LCR, celles-ci doivent être publiées et disponibles pour le téléchargement au maximum dans les 10 minutes suivant leur génération.

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

Sans objet

4.9.10 Exigences de vérification en ligne de la révocation des certificats par les applications utilisatrices de certificats

Voir 4.9.6

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1, Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
Pour les certificats de cachet et les certificats d'horodatage, 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.
Quant au RCC., l'A.C. impose par voie contractuelle qu'en cas de compromission de sa clé privée du R.C. ou de connaissance de la compromission de la clé privée de l'A.C. ayant émis son certificat, le R.C. s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.
Pour les certificats d'AC, outre les exigences du chapitre Révocation et suspension des certificats ci-dessus, la révocation suite à une compromission de la clé privée fera l'objet d'une information diffusée clairement sur le site Internet www.damanesign.ma / www.pki.damanesign.ma. De plus, en cas de compromission de la clé privée de l'AC, l'AC s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

4.9.13 Causes possibles d'une suspension

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

4.9.14 Origine d'une demande de suspension

Sans objet

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

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

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24h, 7j/7j. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4h et un taux de disponibilité annuel de 99,9%.

4.10.3 Dispositifs optionnels

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

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

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

4.12 Séquestre de clé et recouvrement

Le séquestre des clés privées des serveurs est interdit par la présente PC.
Les clés privées d'AC ne doivent pas non plus être séquestrées.
Les clés privées des unités d'horodatage n'est pas séquestrée.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

4.12.2 Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

5 MESURE DE SÉCURITÉ NON TECHNIQUES

5.1 Mesures de sécurité physique

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

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

5.1.1 Accès physique

L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.
L'accès aux machines (serveurs, boîtiers cryptographiques, poste d'administration de l'AC, éléments actifs du réseau) est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines (contrôle d'accès par biométrie, droits associés).

5.1.2 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.
Elles permettent également de respecter les exigences des PC et les engagements de l'AC en matière de disponibilité de ses fonctions, notamment la fonction d'information sur l'état des certificats.

5.1.3 Vulnérabilité aux dégâts des eaux

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

5.1.4 Prévention et protection incendie

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

5.1.5 Conservation des supports

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

5.1.6 Mise hors service des supports

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

5.1.7 Sauvegardes hors site

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

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

L'A.C. distingue au moins les cinq rôles fonctionnels de confiance suivants :
Responsable de sécurité : Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est responsable des opérations de génération des certificats.
Responsable d'application : Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'I.G.C. au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
Ingénieur système : Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
Opérateur : Un opérateur au sein d'une composante de l'I.G.C. réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
Contrôleur : Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'I.G.C. et aux politiques de sécurité de la composante.
Un même rôle fonctionnel peut être tenu par différentes personnes.
De manière générale, des procédures doivent être établies et appliquées pour tous les rôles administratifs et les rôles de confiance ayant trait à la fourniture de services de certification. Ces rôles doivent être décrits et définis dans la description des postes propre à chaque entité opérant

une des composantes de l'I.G.C. sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles doivent déterminer la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilisation des employés.
Lorsqu'appropriées, ces descriptions doivent différencier entre les fonctions générales et les fonctions spécifiques à l'A.C. L'A.C. doit implémenter techniquement ce principe de moindre privilège via les mécanismes de contrôle d'accès qu'elle met en œuvre. Ces descriptions figurent dans la documentation interne de l'A.C.

5.2.2 Nombre de personnes requises par tâches

Le nombre de personnes requises par tâches selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, est précisé dans la documentation interne de l'A.C.

5.2.3 Identification et authentification pour chaque rôle

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

- Son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- Son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- Le cas échéant et en fonction du rôle, un compte soit ouvert à son nom dans ces systèmes

5.2.4 Rôles exigeant une séparation des attributions

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. Néanmoins il y a une séparation obligatoire de ces rôles : 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

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

- Qualifications, compétences et habilitations requises
- Procédures de vérification des antécédents
- Exigences en matière de formation initiale
- Exigences et fréquence en matière de formation continue
- Fréquence et séquence de rotation entre différentes attributions

- Sanctions en cas d'actions non autorisées
- Exigences vis-à-vis du personnel des prestataires externes
- Documentation fournie au personnel

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

Damanesign s'assure de l'honnêteté de son personnel amené à travailler au sein de la composante en mettant en œuvre des moyens respectant le cadre légal et les réglementations en vigueur. Ces personnes ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions. Elles devront remettre à Damanesign une copie de leur casier judiciaire.
Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches. Ces vérifications seront menées préalablement à l'affectation à un rôle de confiance.
Ces vérifications sont effectuées préalablement à l'affectation à un rôle de confiance et revues au minimum tous les 3 ans.

5.3.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.

5.3.4 Exigences en matière de formation continue et fréquences des formations

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte le mode de travail de ces intervenants.
Les intervenants sont formés à la gestion des incidents et sont au fait de l'organisation de remontée d'incidents.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

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

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

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

5.3.8 Documentation fournie au personnel

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

5.4 Procédures de constitution des données d'audit

5.4.1 Type d'événement à enregistrer

Les événements suivants sont enregistrés :

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

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

5.4.2 Fréquence de traitement des journaux d'événements

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

5.4.3 Période de conservation des journaux d'événements

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

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

5.4.4 Protection des journaux d'événements

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

5.4.5 Procédure de sauvegarde des journaux d'événements

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

5.4.6 Système de collecte des journaux d'événements

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

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

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

5.4.8 Évaluation des vulnérabilités

Le contrôle des journaux d'événement système et technique est continu et quotidien afin d permettre une anticipation des vulnérabilités, et des remontées d'alerte en cas de vulnérabilités.
Le contrôle des journaux des événements fonctionnels est réalisé à la demande en cas de litige, ou pour analyse de comportement de l'Autorité de Certification.

5.5 Archivage des données

5.5.1 Types de données à archiver

Des dispositions en matière d'archivage sont prises par l'A.C. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'I.G.C.
Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.
Les données à archiver sont les suivantes :

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

5.5.2 Période de conservation des archives

☐ *Dossiers de demande de certificat*

Tout dossier de demande de certificat accepté doit être archivé aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi marocaine.
En ce qui concerne les certificats de l'AC, les dossiers d'enregistrement (demandes de certificats) sont archivés pendant sept ans après l'expiration du certificat associé.
Les certificats des porteurs et d'A.C., ainsi que les L.C.R. produites, doivent être archivés pendant au moins sept ans après leur expiration.
La durée de conservation des dossiers d'enregistrement doit être portée à la connaissance du signataire.
Au cours de cette durée d'opposabilité des documents, le dossier d'enregistrement doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées.
Ce dossier doit permettre de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

☐ *Journaux d'événements et autres*

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

5.5.3 Certificats, LAR et LCR émis par l'AC

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

5.5.4 Protection des archives

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

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

La documentation interne de l'A.C. décrit les moyens mis en œuvre pour archiver les pièces en toute sécurité.
Dans le cadre d'un transfert ou d'une cessation d'activité, l'ensemble des archives peuvent être confiées à un tiers chargé d'en assurer, pour la durée initialement prévue, la disponibilité et la protection dans les termes décrits dans ce paragraphe.

5.5.5 Procédure de sauvegarde des archives

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

5.5.6 Exigences d'horodatage des données

Chaque évènement contient la date et l'heure précise de réalisation.
Les composants sont synchronisés quotidiennement avec une source de temps UTC.

5.5.7 Système de collecte des archives

L'archivage est réalisé soit de manière automatique, soit de manière manuelle par du personnel autorisé.
La documentation interne de l'A.C. décrit le système de collecte des archives, interne ou externe, qui doit respecter les exigences de protection des archives concernées.

5.6 Procédures de récupération et de vérification des archives

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

5.7 Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela, la période de validité de ce certificat de l'AC doit être supérieure à celle des certificats qu'elle signe. Au regard de la date de fin de validité de ce certificat, son renouvellement sera demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.
Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée sera utilisée pour signer des certificats.
Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.8 Reprise suite à compromission et sinistre

Chaque entité opérant une composante de l'IGC doit met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements.
Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'A.C., l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'A.C. Le cas de l'incident majeur est impérativement traité dès détection ; la publication de l'information de révocation du certificat est réalisée dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé…).
L'A.C. prévient directement et sans délai le point de contact identifié au sein de la D.G.S.S.I.
Si l'un des algorithmes, ou des paramètres associés, utilisés par l'A.C. ou ses signataires devient insuffisant pour son utilisation prévue restante, alors l'A.C. s'engage à :

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

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

Chaque entité opérant une composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents. Les équipes d'exploitation mettent en œuvre des

procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels.
Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. L'AC prévient également directement et sans délai l'organe de contrôle (DGSSI), et la CNDP, en cas d'événement concernant des données personnelles.

5.8.2 Procédures de reprise en cas de sinistre

Chaque composante dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions. La sauvegarde des composants l'IGC permet d'assurer une reprise d'activité en cas de sinistre sous 24 heures.
Ces plans sont testés au minimum une fois par an.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité de la composante (Procédures de reprise en cas de sinistre).
Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué.
En outre, l'AC respecte les engagements suivants :

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

5.8.4 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences du présent document (cf. § 5.8.2 > Procédures de reprise en cas de sinistre).

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

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

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 :

- Le transfert de ses obligations à d'autres parties ;
- Elle assure la continuité du service d'archivage
- Elle assure la continuité du service de publication, et d'information sur l'état de certificat

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 signataires 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
- Révoque tous les Certificats qu'elle a signés et qui seraient encore en cours de validité ;
- Publie une dernière LCR ayant une date de validité positionnée au 31 décembre 9999, 23h59m59s ;

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.
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 SECURITE TECHNIQUES

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

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]
La génération des clés des serveurs est effectuée dans un environnement sécurisé (voir Chapitre 5).

Les paires de clés des serveurs sont générées dans un module cryptographique conforme aux exigences de sécurité pour la création de cachets et d'horodatages, puis transférées de manière sécurisée au porteur sans que l'AC n'en conserve de copie.
Pour la génération d'un certificat d'AC, une bi-clé est générée lors d'une cérémonie de clé à l'aide d'une ressource matérielle conforme.
[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
Les clés privées des unités d'horodatage est généré par leur responsable d'application respectif, à l'intérieur du matériel cryptographique de l'infrastructure IGC. Ce matériel est un HSM qualifié.

6.1.2 Transmission de la clé privée à son propriétaire

La clé privée n'est pas transmise au serveur.

6.1.3 Transmission de la clé publique à l'AC

Sans objet.

6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

La clé publique des AC est enveloppée dans un certificat signé par l'AC racine. Sa diffusion s'accompagne de l'empreinte numérique du certificat ainsi que d'une déclaration qu'il s'agit bien d'une clé publique de l'AC. La clé publique de l'AC, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) pourront aisément être récupérées par les utilisateurs de certificats, via l'interface publique (voir chapitre Entités chargées de la mise à disposition des informations).

6.1.5 Tailles des clés

Les clés d'AC auront ces caractéristiques :

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

Les clés des cachets simple devront avoir ces caractéristiques :

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

Les clés d'Horodatage devront avoir 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

L'utilisation d'une clé privée d'Autorité de Certification (AC) et du certificat associé est strictement limitée à la signature de certificats et de Listes de Certificats Révoqués (LCRs). De même, l'utilisation

de la clé privée des porteurs et du certificat associé est strictement limitée à la création de cachets/Horodatage.

L'utilisation de l'extension « Key Usage » dans les certificats porteur (et aussi de l'extension « Extended Key Usage » lorsqu'elle est présente) ainsi que dans les certificats des AC, est décrite dans les profils de certificats et indique l'objectif d'usage de la clé.

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

Les modules cryptographiques, utilisés par l'AC et les serveurs, pour la génération et la mise en œuvre de leurs clés de signature, sont des modules cryptographiques répondant aux exigences du chapitre Annexe 1 Exigences de sécurité du module cryptographique de l'AC ci-dessous.
Damanesign utilise des HSM certifiés et s'assure de leur sécurité, physique et logicielle.
Damanesign héberge ce matériel dans des zones d'accès contrôlées et protégées contre les pannes électriques, les inondations ainsi que les incendies.
Damanesign s'assure de la sécurité des HSM lors de leur mise en place, lors de la cérémonie des clés, lors de leur utilisation, et ce jusqu'à leur fin de vie.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Nous utilisons une méthode N-M.
Le contrôle de la clé privée du RCC est sous son contrôle exclusif. Damanesign ne dispose pas des éléments permettant d'accéder et d'utiliser la clé privée d'un serveur durant le processus de signature. Le processus technique garantit que seule la clé privée générée pour le serveur durant le processus de cachet est utilisée.
[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1, Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
Le contrôle de la clé privée du porteur est sous son contrôle exclusif.
Le contrôle de la clé privée du responsable de l'unité d'horodatage est sous son contrôle exclusif.

6.2.3 Séquestre de la clé privée

Sans objet.

6.2.4 Copie de secours de clé privée

Les clés privées des cachets ne font l'objet d'aucune copie de secours par l'AC.
Les clés privées d'horodatage ne font l'objet d'aucune copie de secours par l'AC.
La bi-clé de l'AC est sauvegardée sous le contrôle de plusieurs personnes à des fins de reprise d'activité. Les sauvegardes des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles. Les sauvegardes sont rapidement transférées sur site sécurisé de sauvegarde délocalisé afin de fournir et maintenir la capacité de reprise d'activité de l'AC. Les sauvegardes de clés privées d'AC sont stockées dans des ressources cryptographiques matérielles ou sous forme chiffrée.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC ne sont pas archivées.
Les clés privées de l'horodatage ne sont pas archivées par l'AC.
Les clés privées des cachets ne sont pas archivées ni par l'AC ni par aucune des composantes de l'IGC.

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

La génération des clés privées d'AC et des porteurs se fait dans le module cryptographique. Le transfert vers / depuis le module cryptographique ne se fait que pour la génération des copies de sauvegardes. Ceci se fait sous forme chiffrée, conformément aux exigences du chapitre Copie de secours de la clé privée.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC stockées dans des ressources cryptographique matérielles sont protégées avec le même niveau de sécurité que celui dans lequel elles ont été générées.
Le stockage des clés privées des porteurs 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

L'activation des clés privées d'AC se fera dans un module cryptographique et sera contrôlée via des données d'activation (voir chapitre Données d'activation). Pour l'AC, les porteurs de secrets devront être présents afin de réaliser l'activation.
L'activation de la clé privée de porteur est liée au processus de cachet réalisé par le RCC.
L'activation de la clé privée de l'horodatage est liée au processus de horodatage réalisé par l'unité d'horodatage.
L'activation de la clé privée du porteur doit au minimum être contrôlée via des données d'activation (voir chapitre 6.4) et doit permettre de répondre aux exigences définies pour le niveau de sécurité considéré.

6.2.9 Méthode de désactivation de la clé privée

La désactivation des clés privées d'AC dans le module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.
Ces conditions de désactivation doivent permettre de répondre aux exigences définies dans le chapitre **Annexe 1 Exigences de sécurité du module cryptographique** de l'AC pour le niveau de sécurité considéré.

6.2.10 Méthode de destruction des clés privées

En fin de vie d'une clé privée d'AC ou de porteur, normale ou anticipée (révocation), cette clé sera systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.
La destruction d'une clé privée implique la destruction des copies de sauvegarde et des données d'activation de manière qu'aucune information ne puisse être utilisée pour la retrouver.
[Cachet Simple : 1.3.6.1.4.1.58553.1.8.1.1]

Pour les certificats à la volé les clés privées des RCCs sont automatiquement détruites à la fin du processus de cachet. Une fois détruites, les clés privées ne sont de fait plus utilisables.
[Horodatage simple : 1.3.6.1.4.1.58553.1.8.1.2]
La destruction des clés privées en fin de vie est de la responsabilité du responsable de l'horodatage concernée.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs de création de cachet

Se rapporter au 6.1.6
Les modules cryptographiques utilisés par l'A.C. et les unités d'horodatage 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.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

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

6.3.2 Durée 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.
La durée de vie des certificats de l'AC est de 30 ans.
Les bi-clés et les certificats de cachet doivent avoir une durée de vie au maximum de 3 ans.
Les bi-clés et les certificats d'horodatage doivent avoir une durée de vie au maximum de 5 ans.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

☐ *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.

☐ *Génération et installation des données d'activation correspondant à la clé privée d'un Certificat de cachet*

Les données d'activation sont générées par :

- L'URL lui permettant d'accéder au processus de cachet ;
- Des codes d'accès ;
- Une clé unique associée au certificat cachet

☐ *Génération et installation des données d'activation correspondant à la clé privée d'un Certificat d'horodatage*

Ces opérations sont sous la responsabilité du Responsable d'unité d'horodatage (RUH).

6.4.2 Protection des données d'activation

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

Le porteur de secret a la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des données d'activation.

☐ *Protection des données d'activation correspondant aux clés privées du cachet*

Le RCC est le seul à connaître ses codes d'accès et de la clé unique associée au cachet.

☐ *Protection des données d'activation correspondant aux clés privées d'horodatage*

Ces opérations sont sous la responsabilité du Responsable d'unité d'horodatage (RUH).

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

L'IGC met en place une série de mesures et de moyens garantissant un haut niveau de sécurité :

- Authentification forte des utilisateurs du système avec gestion des rôles par utilisateur.
- Gestion des sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur).
- Mise en place d'antivirus et d'antimalware pour protéger contre les virus informatiques et les logiciels malveillants, avec des mises à jour régulières.
- Identification et authentification forte des utilisateurs pour l'accès au système, incluant l'authentification à deux facteurs (physique ou logique).
- Gestion des comptes utilisateurs, avec modification et suppression rapide des droits d'accès.
- Protection du réseau contre toute intrusion non autorisée pour assurer la confidentialité et l'intégrité des données.
- Mise en place de fonctions d'audit pour garantir la non-répudiation et documenter les actions effectuées.
- Gestion des reprises sur erreur.
- Identification et authentification forte des rôles de confiance (accès physique et logique).
- Gestion des droits d'accès basée sur des profils respectant le principe du moindre privilège.
- Interdiction de la réutilisation d'objets.
- Exigence de l'utilisation de la cryptographie pour les communications.
- Assure la séparation rigoureuse des tâches.
- Fournit une autoprotection du système d'exploitation.

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Les mesures de sécurité relatives à l'IGC découlent d'une analyse de risque.

Les modules cryptographiques mise en œuvre on fait l'objet d'une évaluation selon la norme FIPS 140-2 Level 3 et CC EAL 4+.

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

Toute évolution significative d'un système d'une composante de l'IGC doit être testée et validée avant déploiement. Ces opérations sont réalisées par du personnel de confiance.

6.6.2 Mesures liées à la gestion de la sécurité

La configuration du système d'AC, ainsi que toute modification ou évolution, est documentée et contrôlée par l'AC.
Il existe un mécanisme permettant de détecter toute modification non autorisée du logiciel ou de la configuration de l'AC. Une méthode formelle de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système d'IGC.
Lors de son premier chargement, une vérification est faite que le logiciel de l'IGC correspond à celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé, et qu'il correspond bien à la version voulue.

6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

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

Il n'y a pas d'horodatage utilisé par l'AC mais une datation sûre. Tous les composants de l'AC sont régulièrement synchronisés avec un serveur de temps tel qu'une horloge atomique ou un serveur Network Time Protocol (NTP). Le temps fourni par ce serveur de temps est utilisé pour établir l'heure :

- Du début de validité d'un Certificat ;
- De la révocation d'un Certificat ;
- De l'affichage de mises à jour de LCR.

Des procédures automatiques peuvent être utilisées pour maintenir l'heure du système.

7 PROFILS DES CERTIFICATS ET CRLS

Les certificats émis par l'AC sont des certificats au format X.509 v3 (populate version field with integer "2").
Les champs des certificats « cachet serveur » et des AC sont définis par le RFC 5280.

7.1 Profil Certificat AC

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	sha256WithRSAEncryption
Issuer	cn=Damanesign Root CA ou=154609 o=Damanesign c=MA
Validity	29 ans
Subject	cn=Damanesign Seal2 CA ou=154609 oi=NTRMA-154609 o=Damanesign c=MA
Subject Public Key Info	RSA 4096 bits

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

7.2 Profil Certificats Cachet [1.3.6.1.4.1.58553.1.8.1.1]

- **PROFIL DE CERTIFICAT CACHE GENERER A LA VOLEE**

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 Seal2 CA ou=154609 oi=NTRMA-154609 o=Damanesign c=MA
Validity	1 heure

Subject	cn= nom du service de création de cachet oi= Identifiant de l'organisation (ICE, RC, TVA, …) o= Nom de l'organisation propriétaire du cachet c=MA
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	Digital Signature, Non répudiation
Basic Constraints	O	CA : FALSE
Certificate Policies	N	OID: 1.3.6.1.4.1.58553.1.8.1.1 CPS: https://pki.damanesign.ma/cps.html
Issuer Alternative Name	N	Non utilisé
CRL Distribution Points		`http://pki.damanesign.ma/crl/ca_seal2_2025.crl`
Authority Information Access	N	`CA:` http://pki.damanesign.ma/cert/ca_seal2_2025.crt

7.3 Profil Certificats d'horodatage [1.3.6.1.4.1.58553.1.8.1.2]

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	cn=Damanesign Seal2 CA ou=154609 oi=NTRMA-154609 o=Damanesign c=MA
Validity	5 ans
Subject	cn= Nom commun de l'unité d'horodatage Damanesign oi= Identifiant de l'organisation (ICE, RC, TVA, …) o= Nom déposé de l'organisation tel qu'enregistré au registre du commerce serialNumber= Numéro aléatoire c=MA
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	Digital Signature
Extended Key Usage	O	id-kp-timeStamping
Basic Constraints	O	CA : FALSE
Certificate Policies	N	OID: 1.3.6.1.4.1.58553.1.8.1.2 CPS: https://pki.damanesign.ma/cps.html
Issuer Alternative Name	N	Non utilisé
CRL Distribution Points		`http://pki.damanesign.ma/crl/ca_seal2_2025.crl`
Authority Information Access	N	CA:http://pki.damanesign.ma/cert/ca_seal2_2025.crt

7.4 Liste de Certificats Révoqués

Champ	Contenu
Version	2, indiquant qu'il s'agit d'un certificat version 3.
Signature	Sha256WithRSAEncryption
Issuer	CN = Damanesign Seal2 CA OU = 154609 OI=NTRMA-154609 O = Damanesign C = MA
thisUpdate	Date et heure UTC
nextUpdate	Date et heure UTC (1 j de validité)
RevokedCertificates	Liste des numéros de série des certificats révoqués (Couples UserCertificate-RevocationDate)
Numéro de LCR	Entier
AuthorityKeyIdentifier	Identifiant de la clé de l'A.C.

8 AUDITS DE CONFORMITE ET EVALUATIONS

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

8.1 Fréquences et circonstances des évaluations

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

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

8.2 Identités / qualifications des évaluateurs

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

8.3 Relations entre évaluateurs et entités évaluées

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

8.4 Sujets couverts par les évaluations

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

8.5 Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend au PSCo, un avis parmi les suivants : « réussite », « échec », « à confirmer ». Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'A.C. qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, etc. Le choix de la mesure à appliquer est effectué par l'A.C. et doit respecter ses politiques de sécurité internes.
- En cas de résultat « à confirmer », l'A.C. remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'A.C. confirme à la composante contrôlée la conformité aux exigences de la P.C.

8.6 Communication des résultats

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

9 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

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

9.1.2 Tarifs pour accéder aux certificats

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

Les certificats de la chaîne de confiance sont accessibles par les utilisateurs de certificats gratuitement.

9.1.3 Tarifs pour accéder aux informations d'état de révocation

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

9.1.4 Tarifs pour d'autres services

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

9.1.5 Politique de remboursement

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

9.2 Responsabilité financière

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

9.3 Confidentialité des données

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :

- La documentation interne de l'A.C.,

- Les clés privées de l'A.C., des composantes et des serveurs et RCCs,
- Les données d'activation associées aux clés privées d'A.C. et des signataires,
- 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,

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, 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 signataires à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations au signataire.

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 1.6.2.

9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- Le dossier d'enregistrement du RCC.
- Le dossier d'enregistrement du responsable d'unité d'horodatage.

9.4.3 Informations à caractère non personnel

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

9.4.4 Responsabilité en termes de protection des données personnelles

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

9.4.5 Notification et consentement d'utilisation des données personnelles

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

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

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

9.4.7 Autres circonstances de divulgation d'informations personnelles

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

9.5 Droits sur la propriété intellectuelle et industrielle

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

9.6 Interprétations contractuelles et garanties

Sans objet.

9.7 Limite de garantie

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

9.8 Limite de responsabilité

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

9.9 Indemnités

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

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

9.10.1 Durée de validité

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

9.10.2 Fin anticipée de validité

Sans objet

9.10.3 Effets de la fin de validité et clauses restant applicables

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

9.11 Notifications individuelles et communications entre les participants

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

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

9.12 Amendements à la P.C.

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

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

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

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

9.13 Dispositions concernant la résolution de conflits

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

9.14 Juridictions compétentes

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

9.15 Conformité aux législations et réglementations

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

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'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR / LAR), ainsi que, pour la génération des bi-clés des signataires, répond aux exigences de sécurité suivantes :

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

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