Déclaration des Pratiques de Certification AC Qualifié Cachet

Version 1.0 | Diffusion : public | OID : 1.3.6.1.4.1.58553.1.2.2.1/1.3.6.1.4.1.58553.1.2.2.2

Historique du document

Version	Date de version	Rédacteur(s)	Approbateur(s)	Modifications
0.2	10/03/2023	Noureddin SOUAD	Zouhair HAMDAOUI	Création du document
1.0	13/10/2023	Fatimazahrae JALAL	Zouhair Hamdaoui	Mise à jour conformément à la loi 43.20

Sommaire

1 INTRODUCTION

1.1 Présentation générale

Ce document la Déclaration des Pratiques de Certification (DPC) expose les pratiques que la société DAMANESIGN applique dans le cadre de la fourniture de certificats électroniques qualifiés pour le cachet électronique pour des personnes morales et la délivrance des certificats électroniques qualifiés pour l'horodatage en conformité avec la Politique de Certification (PC) de l'AC « Damanesign Qualified Seal CA ».

L'AC Damanesign Qualified Seal CA ne peut être utilisée que pour :

- Produire des certificats électroniques qualifiés pour le cachet électronique ;
- Produire les certificats des unités d'horodatage du service d'horodatage électronique qualifié
- Signer des Listes des Certificats Révoqués (LCR) ;
- Produire des certificats de signature des réponses OCSP de l'AC.

La chaîne de certification est la suivante :

- AC Racine : Damanesign Root CA
- AC Émettrice : Damanesign Qualified Seal CA

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

1.2 Identification du document

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

Le numéro d'OID de la présente D.P.C. est : 1.3.6.1.4.1.58553.1.2.2.1/1.3.6.1.4.1.58553.1.2.2.2

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

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

OID : 1.3.6.1.4.1.58553.1.2.1.2 pour les certificats d'horodatage qualifiés ;

Et les certificats OCSP de l'AC.

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

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

1.3.1 Le Prestataire de services de confiance

Voir 1.3.1 de la PC

1.3.2 Autorité de certification

Voir 1.3.2 de la PC

1.3.3 Autorité d'enregistrement

Voir 1.3.3 de la PC

1.3.4 Porteurs de certificats

Voir 1.3.4 de la PC

1.3.5 Responsables de Certificat de Cachet

Voir 1.3.5 de la PC

1.3.6 Responsables d'unité d'horodatage

Voir 1.3.6 de la PC

1.3.7 Utilisateurs de certificat

Voir 1.3.6 de la PC

1.3.8 Mandataire de certification

Voir 1.3.7 de la PC

1.3.9 Personne autorisée :

Voir 1.3.8 de la PC

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Bi-clés et certificats des porteurs

Voir 1.4.1.1 de la PC

1.4.1.2 Bi-clés et certificats d'A.C.

Voir 1.4.1.2 de la PC

1.4.2 Domaines d'utilisation interdits

Voir 1.4.2 de la PC

1.5 Gestion de la D.P.C.

1.5.1 Entité gérant la D.P.C.

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

1.5.2 Point de contact

Voir 1.5.2 de la PC

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

Voir 1.5.3 de la PC

1.6 Définitions et sigles

1.6.1 Sigles

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

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

1.6.2 Définitions

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

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

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

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

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

- Rédaction des documents de spécifications de l'I.G.C.
- Mise en application de la P.C.
- Gestion des certificats (de leur cycle de vie)
- Choix des dispositifs cryptographiques et gestion des données d'activation
- Publication des certificats valides et des listes de certificats révoqués

- Conseil, information ou formation des acteurs de l'I.G.C.
- Maintenance et évolution de la P.C. et de l'I.G.C.
- Journalisation et archivage des événements et informations relatives au fonctionnement de l'I.G.C., à son niveau ;

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

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

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

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

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

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

Infrastructure à Clés Publiques (**I.G.C.**) **:** désigne un ensemble de moyens organisationnels, techniques (matériels et logiciels), humains, documentaires et contractuels pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques. L'I.G.C. génère, distribue, gère et archive les Certificats. Chacune des composantes de l'I.G.C. est décrite dans la politique de certification définissant le niveau de confiance confié à chacune d'entre elles.

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

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

Politique de certification (P.C.) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une A.C. se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une P.C. peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Prestataire de services de certification électronique (P.S.C.E.) - Un P.S.C.E. se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un P.S.C.E. peut

fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un P.S.C.E. comporte au moins une A.C. mais peut en comporter plusieurs en fonction de son organisation. Les différentes A.C. d'un P.S.C.E. peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (A.C. Racines / A.C. filles). Un P.S.C.E. est identifié dans un certificat dont il a la responsabilité au travers de son A.C. ayant émis ce certificat et qui est elle-même directement identifiée dans le champ issuer du certificat.

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

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

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

2.1 Entités chargées de la mise à disposition des informations

Voir 2.1 de la PC

2.2 Informations devant être publiées

Voir 2.2 de la PC

2.2.1 Publication du certificat d'AC

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

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

2.2.2 Publication de la CRL

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

`http://pki.damanesign.ma/crl/ca_ qseal_2022.crl`

2.2.3 URL d'OCSP

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

http://ocsp.damanesign.ma/ca_qseal

2.3 Délais et fréquences de publication

Voir 2.3 de la PC

2.4 Contrôle d'accès aux informations publiées

Toutes les informations publiées indiquées ci-dessus, sont publiques et ne sont accessibles qu'en lecture. L'accès en modification aux données publiées est restreint aux équipes internes Damanesign en charge de publier les documents sur l'espace de publication. Un contrôle d'accès fort et nominatif est mis en place, respectant la politique de mot de passe Damanesign qui est conforme aux exigences règlementaires en vigueur.
L'accès en modification du système de publication des informations d'état de certificats nécessite un contrôle d'accès fort.

L'accès est autorisé aux personnes habilitées conformément au politique de contrôle d'accès.

Pour en savoir plus, veuillez consulter "*La politique de contrôle d'accès*".

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Voir le 3.1.1 de la PC

3.1.2 Nécessité d'utilisation de noms explicites

3.1.2.1 A.C. Cachet qualifié

Voir 3.1.2.1 de la PC

3.1.2.2 Certificat de cachet

Voir 3.1.2.2 de la PC

3.1.2.3 Certificat d'horodatage

Voir 3.1.2.3 de la PC

3.1.3 Pseudonymisation des porteurs

Sans objet

3.1.4 Règles d'interprétation des différentes formes de nom

Sans objet.

3.1.5 Unicité des noms

Voir 3.1.5 de la PC

3.1.6 Identification, authentification et rôle des marques déposées

Voir le 3.1.6 de la PC

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.

3.1.7 Validation initiale de l'identité

Voir le 3.1.7 de la PC

3.1.8 Méthode pour prouver la possession de la clé privée

Voir le 3.1.8 de la PC

3.1.9 Validation de l'identité d'un organisme

Voir 3.1.10

3.1.10 Validation de l'identité d'un individu

Voir 3.1.10 de la PC

3.1.11 Informations non vérifiées du porteur

Aucune.

3.1.12 Validation de l'autorité du demandeur

Voir PC 3.1.12

3.1.13 Certification croisée d'A.C.

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

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

3.2.1 Identification et validation pour un renouvellement courant

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

3.2.2 Identification et validation pour un renouvellement après révocation

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

3.3 Identification et validation d'une demande de révocation

L'AE authentifie toutes les demandes de révocation.

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

Le RCC du certificat dispose de deux moyens pour révoquer le certificat :

1ère méthode : Révocation en ligne du certificat Damanesign

- Dans votre navigateur accédez à la page : « https://guichet.damanesign.ma » pour effectuer la révocation du certificat en ligne ;
- Accédez au menu "Services" ensuite veuillez choisir "Révocation du Certificat".
- Renseigner l'adresse courriel et le numéro de CIN du RCC de certificat ;
- Cette étape est protégée par un mécanisme CAPTCHA qui permet de réduire les risques associés aux attaques par des automates, cliquer sur « Continuer » ;
- Saisir les réponses aux questions secrètes (se référer à la copie du formulaire des réponses aux questions secrètes) ;
- Si vous avez plusieurs certificats, Cliquer sur le numéro (N°) correspondant au certificat à révoquer, s'assurer bien que les informations affichées correspondent au certificat que vous souhaitez révoquer ;
- Choisir la raison de la révocation et renseigner un commentaire puis cliquer sur le bouton « Révocation du certificat » pour terminer la révocation.

2éme méthode : Révocation du certificat via un appel téléphonique

- Le RCC a la possibilité de contacter le département de Révocation de Damanesign sur le numéro suivant +212 5 37 68 68 01 qui est joignable et disponible les jours ouvrés.
- Dans le cadre d'une démarche sécurité, le RCC va devoir répondre à une série de questions qui seront posées par l'équipe Damanesign afin de l'authentifier et de s'assurer de son identité.

- En dernier lieu, le RCC du certificat va devoir préciser le certificat à révoquer et communiquer la raison de révocation du certificat.

Le représentant légale ou Le mandataire de certification dispose d'un seul moyen pour révoquer le certificat d'un porteur :

Révocation par courrier du certificat Damanesign :

Le représentant légale et le mandataire dispose de la possibilité de révoquer le certificat cachet par courrier **:**

Il est invité à envoyer la demande de révocation de certificat signée et cachetée par courrier à l'adresse suivante :

Damanesign, Service Enregistrement et Relation Clientèle
Direction développement
4 RUE OUED ZIZ 3EME ETAG E APPT 7 AGDAL, Rabat
10080, Rabat.

Le service de Damanesign procède à vérifier les données du demandeur ensuite révoque le certificat.

Un courrier de confirmation est envoyé au demandeur et au RCC notifiant la révocation effective du certificat.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

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

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

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

- Une demande de certificat écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le nom du service de création d'horodatage concerné par cette demande,
- Un mandat, daté de moins de 3 mois, désignant le futur RUH comme étant habilité à être RUH pour le service de création d'horodatage pour lequel le certificat d'horodatage doit être délivré. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RUH,
- Les conditions générales d'utilisation signées par le RUH
- Un document officiel d'identité en cours de validité du RUH comportant une photographie d'identité notamment la carte d'identité nationale, le passeport, qui est présenté à l'AE, qui en conserve une copie.
- Une photocopie d'un justificatif d'identité du représentant légal
- Une pièce valide au moment de l'enregistrement portant le numéro d'identification de l'entreprise
- L'adresse courriel du RUH

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

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

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

Damanesign suit la procédure suivante :

- **Notification Immédiate :** En cas de non-confirmation d'une demande de révocation dans les 24 heures, le personnel de l'autorité de certification (AC) doit être immédiatement informé de la situation.
- **Analyse :** Une analyse de la demande de révocation doit être effectué pour identifier les raisons de la non-confirmation. Cela peut inclure la vérification des systèmes, des journaux d'audit, et des données de la demande de révocation.
- **Communication avec le Demandeur :** Le demandeur de la révocation doit être contacté pour obtenir des informations supplémentaires ou clarifications via l'e-mail et/ou le téléphone.
- **Actions à prendre :** Sur la base de l'analyse, des actions appropriées doivent être mises en œuvre. Cela peut inclure la révocation du certificat concerné et/ou renouvellement selon la procédure décrite dans le présent document.
- **Rapport Post-Action :** Un rapport post-action doit être généré pour documenter toutes les étapes de la procédure de révocation. Ce rapport doit être sauvegarder et archiver avec le dossier de porteur.

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

Les abonnés, les parties faisant confiance, les fournisseurs de logiciels d'application et d'autres tiers peuvent soumettre des rapports de problème de certificat via contact@damanesign.ma.

Damanesign publie des instructions relatives à la révocation de certificat dans un guide dédiée faisant partie de son référentiel public.

Pour tout rapport de problème de certificat, le déclarant est prié d'inclure ses coordonnées, les abus suspectés et le sujet lié (par exemple, FQDN ou IP).

La AE du Damanesign commence l'enquête sur un rapport de problème de certificat dans les 24 heures suivant la réception et décide si la révocation ou d'autres actions appropriées sont nécessaires, basées au moins sur les critères suivants :

- La nature du problème allégué,
  Le nombre de rapports de problème de certificat reçus concernant un certificat particulier ou un sujet,
  L'entité faisant le rapport (par exemple, une notification d'une organisation anti-logiciels malveillants ou d'une agence de maintien de l'ordre a plus de poids qu'une plainte anonyme),
  La législation locale pertinente.

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

4 EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

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

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

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

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

Voir 4.2 de la PC

4.3 Traitement d'une demande de certificat

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

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

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

- Le contrôle du dossier d'enregistrement (dossier complet), à savoir :
  - « Contrat d'abonné – Conditions Particulières »
  - « Conditions Générales d'utilisation »
  - « Autorisation de demande de certificat »
  - « Procuration du représentant légal – Désignation d'un mandataire de certification » dans le cas d'une demande via un M.C....
- La vérification que le futur RCC a pris connaissance des modalités applicables pour l'utilisation du Certificat. Pour cela, l'A.E. vérifie que le Porteur a paraphé et signé le document « Conditions Générales d'utilisation ».
- La vérification avec un soin raisonnable de la vraisemblance des pièces constitutives du Dossier de Souscription (Pièces d'identité, mandats, …) ; et en particulier de l'identité du demandeur futur RCC ou M.C. le cas échéant ;
- Dans le cas d'une demande via un M.C., celui-ci retransmet le dossier à l'A.E. après avoir effectué les opérations ci-dessus.

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

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

La demande de certificat comporte les éléments mentionnés ci-dessus, ainsi que le nom du service à utiliser dans le certificat.

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

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

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

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

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

4.3.2 Acceptation ou rejet de la demande

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

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

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

[OID : 1.3.6.1.4.1.58553.1.2.1.2]
En cas de rejet de la demande, l'AE en informe le RUH, de vive voix ou par courriel, en justifiant le rejet.

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

4.3.3 Durée d'établissement du certificat

Voir 4.3.3 de la PC

4.4 Délivrance du certificat

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

[OID : 1.3.6.1.4.1.58553.1.2.1.1]
Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération et de préparation des différents éléments du RCC : -la bi-clé, ainsi que le certificat associé. À partir de ce moment, le dispositif de cachet Damanesign sera activé.

Le processus de génération du certificat est lié de manière sécurisée au processus de génération de la bi-clé. La clé privée et le certificat sont intégrés dans le support cryptographique du porteur. Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres Mesures de sécurité non techniques et Mesures de sécurité techniques ci-dessous, notamment la séparation des rôles de confiance (cf. chapitre Mesures de sécurité procédurales).

[OID : 1.3.6.1.4.1.58553.1.2.1.2]
Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC produit le certificat et le fournit en main propre au responsable de l'unité d'horodatage.

4.4.2 Notification de la délivrance du certificat au RCC

Voir PC 4.4.2

4.5 Acceptation du certificat

4.5.1 Démarche d'acceptation du certificat

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

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

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

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

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

4.5.2 Publication du certificat

Les certificats ne sont pas publiés par l'A.C.

4.5.3 Notification aux autres entités de la délivrance du certificat

Sans objet.

4.6 Usages de la bi-clé et du certificat

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

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

Cet usage est indiqué explicitement dans les extensions des certificats au sens X509 du terme :

- Key Usage :
  - Digital Signature et Non Repudiation

4.6.2 Utilisation de la clé privée et du certificat par le RUH

Les clés privées des unités d'horodatage ne sont utilisables que pour signer les contremarques qualifiées produites par les unités d'horodatage du service Damanesign.
Il est souligné que le service se limite strictement à l'émission de contremarques de temps qualifiées. La réponse à une demande de contremarque de temps est assurée dans un délai ne dépassant pas quelques secondes, garantissant ainsi le maintien de la réactivité et de l'ergonomie de l'application cliente.

Cet usage est indiqué explicitement dans les extensions des certificats au sens X509 du terme :

- Key Usage :
  - Digital Signature

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

Voir 4.6.2 de la P.C.

4.7 Renouvellement d'un certificat

Voir 4.7 de la P.C.

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

Voir PC 4.8

4.8.1 Origine d'une demande d'un nouveau certificat

La demande d'un nouveau certificat suit le même processus qu'une demande initiale.
Cf section 4.1 « Demande de certificat ».

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

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

4.8.3 Notification au porteur de l'établissement du nouveau certificat

Voir 4.4.2.

4.8.4 Démarche d'acceptation du nouveau certificat

Voir4.5.

4.8.5 Publication du nouveau certificat

Voir 0.

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

Voir 4.3.2.

4.9 Modification du certificat

La modification du certificat n'est pas autorisée.

4.10 Révocation et suspension des certificats

4.10.1 Causes possibles d'une révocation

4.10.1.1 Certificats de cachet

Voir 4.10.1.1 de la PC

- *Certificats d'horodatage*

Voir 4.10.1.2 de la PC

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

Voir 4.10.1.2 de la PC

4.10.2 Origine d'une demande de révocation

4.10.2.1 Certificats de signature

Voir 4.10.2.1 de la PC

4.10.2.2 Certificats d'horodatage

Voir 4.10.2.2 de la PC

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

Voir 4.10.2.3 de la PC

4.10.3 Procédure de traitement d'une demande de révocation

4.10.3.1 Révocation d'un certificat de cachet

Voir 4.10.3.1 de la PC

La procédure de révocation des certificats par l'AC. est décrite dans la documentation interne de l'IGC, elle suit les étapes :

- l'A.E. vérifie le nom de serveur et le numéro du certificat a révoquer ;
- l'A.E. envoi le numéro de certificat et la raison de révocation du certificat cachet ;
- L'AC génère une nouvelle LCR qui contient le numéro du certificat et la date de révocation ;
- L'AC publie le nouveau CRL à la place de l'ancienne.

L'AE envoie une notification de la révocation du certificat cachet au RCC et au MC qui le représente le cas échéant, par mail

4.10.3.2 Révocation d'un certificat d'horodatage

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

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

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

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

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

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

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

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

4.10.4 Délai accordé au porteur pour formuler la demande de révocation

Voir 4.10.4 de la P.C.

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

4.10.5.1 Révocation d'un certificat de cachet

Voir 4.10.5.1 de la P.C.

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

Voir 4.10.5.2 de la P.C.

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

Pour vérifier l'état d'un certificat de cachet, l'A.C. « DAMANESIGN QUALIFIED SEAL » met à disposition des utilisateurs de certificats de cachet la CRL et un service OCSP. Cette adresse de publication L.C.R. est indiquée dans le champ CRLDistributionPoint des certificats de cachet.

Pour vérifier l'état du certificat de l'A.C. « DAMANESIGN QUALIFIED SEAL » DAMANESIGN fournit une adresse de publication de la L.A.R. « https://pki.damanesign.ma/crl/ca_root_2022.crl » cette adresse est indiquée dans le champ CRLDistributionPoint du certificat de l'A.C. « DAMANESIGN QUALIFIED SEAL »

Damanesign a mis aussi en place un service OCSP. L'adresse du système est précisée dans le profil des certificats émis.

Les résultats retournés par l'OCSP et les LCR sont consistants modulo les délais de publication des LCRs.

L'utilisateur d'un certificat de cachet est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. Il pourra utiliser la dernière LCR publiée par l'AC ou son service OCSP afin de vérifier le statut de révocation du certificat de porteur. L'utilisateur doit aussi vérifier le statut de révocation des AC de la chaîne de certification en utilisant pour chacune la dernière LAR émise par l'AC de niveau supérieur.

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

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

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

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

Voir 4.10.6

4.10.9 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.10.10 Exigences spécifiques en cas de compromission de la clé privée

Aucune exigence spécifique en cas de compromission de la clé privée d'un serveur hormis la révocation du certificat (voir 4.10.10 de la P.C.).

La révocation suite à une compromission de la clé privée de l'AC fait l'objet d'une information clairement diffusée au moins sur le site de DAMANESIGN et éventuellement relayée par d'autres moyens (associations, clubs utilisateur, réseaux sociaux, etc.).

En cas de compromission de sa clé privée ou de connaissance de la compromission de la clé privée de l'A.C. ayant émis son certificat, le RCC/RUH s'oblige à interrompre immédiatement et définitivement l'usage du certificat et de la clé privée qui lui est associée.

Dans le cas de compromission d'une clé d'A.C., le certificat correspondant sera immédiatement révoqué. De même, tous les certificats de cachet /horodatage en cours de validité émis par cette AC. En plus DAMANESIGN doit :

- Informer tous les RCCS, RUHS, les Mandataires de Certification et les autres entités en lien avec l'AC
- Indiquer que les certificats et les informations de statut de révocation ayant été délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

4.10.11 Suspension de certificats

Voir 4.10.11 de la PC

4.11 Fonction d'information sur l'état des certificats

4.11.1 Caractéristiques opérationnelles

Voir 4.11.1 de la PC

4.11.2 Disponibilité de la fonction

Voir 4.11.1 de la PC

4.11.3 Séquestre de clé et recouvrement

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

5 Mesures de sécurité non techniques

Voir [PCQSIGN].

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés de l'A.C.

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

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

6.1.1.2 Clés porteurs générées par le RCC

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

Les bi-clés des porteurs sont générées directement dans le dispositif de création de signature destiné au porteur conformément aux exigences des sections 6.1.5 et 6.1.6.

6.1.1.3 Clés générées par le RUH pour l'horodatage

L'AH garantit que les clés cryptographiques des UH sont produites dans des circonstances et dans un environnement contrôlé, au cours d'une cérémonie de clés faisant l'objet d'un procès-verbal.

Ces clés sont générées et protégées au sein d'un HSM et ne sont pas exportées. La longueur des clés de l'AH est d'au moins 3072 bits avec l'algorithme RSA.

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

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet.

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

Sans objet.

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

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

6.1.5 Tailles des clés

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

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

Les clés RSA des certificats de cachet des RCCS ont une taille de [2048/4096] bits et sont associées à la fonction d'empreinte SHA-256.

Les clés RSA des certificats de cachet des RUHS Sont une taille de 3076 bits et sont associées à la fonction d'empreinte SHA-256.

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

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

Voir 6.1.6 de la PC

6.1.7 Objectifs d'usage de la clé

[OID : 1.3.6.1.4.1.58553.1.2.1.1]

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

[OID : 1.3.6.1.4.1.58553.1.2.1.2]

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

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

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'A.C.

L'A.C. s'assure que :

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

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.

6.2.1.2 Dispositifs de création de signature des serveurs

Voir 6.2.1.2 de la PC

6.2.1.3 Dispositifs des unités d'horodatage

Voir 6.2.1.3 de la PC

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

Le contrôle des clés privées de signature des AC est assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets. Il y a 5 porteurs de secrets pour chaque AC, qui se voient remettre ces secrets sur carte à puce lors de la cérémonie des clés. Nous utilisons une méthode N-M avec N=3 et M=5.

Pour plus d'information veuillez consulter le document : "*Damanesign - PV Cérémonie des clés* "

6.2.3 Séquestre de la clé privée

Les clés privées de l'AC ne doivent en aucun cas être séquestrées.

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

6.2.4 Copie de secours de la clé privée

[OID : 1.3.6.1.4.1.58553.1.2.1.1]
Les clés privées des cachets ne font l'objet d'aucune copie de secours par l'A.C.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]
Si les clés privées font l'objet d'une copie, celle-ci se fait :

- Dans un module cryptographique conforme aux exigences de la section exigences de sécurité du module cryptographique de l'AC, ou
- Hors d'un module cryptographique, mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement utilisé offre un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuie sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées ne soient à aucun moment en clair en dehors du module cryptographique.

6.2.5 Archivage de la clé privée

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

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

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

6.2.7 Stockage de la clé privée dans un module cryptographique

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

[OID : 1.3.6.1.4.1.58553.1.2.1.1]
Le stockage des clés privées des certificat cachet est réalisé dans des supports cryptographiques répondant aux exigences de sécurité du module cryptographique des services de cachet.

[OID : 1.3.6.1.4.1.58553.1.2.1.2]
Le stockage des clés privées des unités d'horodatage est réalisé dans un module cryptographique répondant aux exigences de la section exigences de sécurité du module cryptographique de l'AC.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'A.C.

L'activation des clés privées d'A.C. dans un module cryptographique doit être contrôlée via des données d'activation (*cf.*6.2.2) et doit faire intervenir au moins trois personnes dans des rôles de confiance.

6.2.8.2 Clés privées des RCC

Voir 6.2.8.2 de la PC

6.2.8.3 Clés privées des RUH

Voir 6.2.8.3 de la PC

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'A.C.

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

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

6.2.9.2 Clés privées des RCC

Voir 6.2.9.2 de la PC

6.2.9.3 Clés privées des RUH

Voir 6.2.9.3 de la PC

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées d'A.C.

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

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

6.2.10.2 Clés privées des RCC

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

6.2.10.3 Clés privées des RHU

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

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

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.

Les supports cryptographiques utilisés par les RCC sont conformes à EAL5+.

Ces exigences sont précisées au chapitre 10 et 11.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques des A.C. sont archivées dans le cadre de l'archivage des certificats correspondants. Voir 5.5.2

6.3.2 Durées de vie des bi-clés et des certificats

Voir 6.3.2 de la P.C.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

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

La génération et l'installation des données d'activation des modules cryptographiques de l'I.G.C interviennent lors de la cérémonie de l'A.C. dont le procès-verbal détaille l'intégralité des actions effectuées. « DAMANESIGN– Cérémonie des clés ».

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

Les codes PIN des porteurs sont générés par L'A.C. . L'A.C. transmet le code PIN par le biais d'un courrier recommandé à l'utilisateur en invitant le Porteur à récupérer le support chez DAMANESIGN.

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

Ces opérations sont sous la responsabilité du RUH.

6.4.2 Protection des données d'activation

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

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

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

6.4.2.2 Protection des données d'activation correspondant aux clés privées des certificats cachet

Les données d'activation des clés serveurs des RCCS sont protégés sous leur responsabilité par un mot de passe ou des donnes d'activation conformément aux exigences.

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

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique. Ces opérations sont sous la responsabilité du RUH.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

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

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

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

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

6.6 Mesures de sécurité liées au développement des systèmes

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

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

6.7 Mesures de sécurité réseau

Cf. document « DAMANESIGN - Description de l'infrastructure DAMANESIGN ».

6.8 Horodatage / Système de datation

Voir 6.8 de la P.C.

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

7.1 Certificats de l'A.C.

Voir 7.1 de la P.C.

7.2 Certificat de cachet (**1.3.6.1.4.1.58553.1.2.1.1**)

Voir 7.2 de la P.C.

7.3 Certificat d'horodatage (1.3.6.1.4.1.58553.1.2.1.2)

Voir 7.3 de la P.C.

7.4 Liste de Certificats Révoqués

Voir 7.3 de la P.C.

7.5 Certificat OCSP

Voir 7.5 de la P.C.

7.6 Certificats du service OCSP

Voir 7.6 de la P.C.

8 Audits de conformité et évaluations

Voir [PCQSIGN].

9 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

Voir [PCQSIGN].

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

10.1 Exigences sur les objectifs de sécurité

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

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

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

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

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

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

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