POSTE MAROC

BARID ESIGN	
Type de document	**POLITIQUE DE CERTIFICATION**
Titre :	**POLITIQUES DE CERTIFICATION SUPPORTANT LA SIGNATURE ELECTRONIQUE POUR L'AC CLASSE 3 PLACEE SOUS L'AC RACINE BARIDESIGN E-GOV**

SOMMAIRE

1. INTRODUCTION

La présente Politique de Certification (PC) est un recueil d'engagements et d'exigences portant sur un ensemble de services de confiance et de produits de sécurité qui participent à la sécurisation des échanges dématérialisés entre les différents partenaires (publics, entreprises et usagers).

L'objectif de ce document est de définir les engagements minimums que Poste Maroc s'engage à respecter dans l'émission, la délivrance et la gestion de certificats de signature électronique sécurisée tout au long de leur cycle de vie. Il a également pour objet de renseigner les promoteurs d'applications acceptant ces mêmes certificats.

Ce document concerne l'ensemble des Politiques de Certification supportant des certificats supportant la signature électronique et délivrés par l'AC Classe 3 placée sous l'AC Racine BarideSign e-gov. Il s'agit de certificats supportant exclusivement la signature électronique (service de non-répudiation). Les certificats concernés par ce document peuvent être fournis, soit à des particuliers, soit à des professionnels.

Les autres familles de certificats et les Politiques de Certification correspondantes concernées par l'AC Classe 3 placée sous l'AC Racine BarideSign e-gov ne sont pas traitées par le présent document.

Les certificats et les clés privées associées sont fournis sur des supports cryptographiques, tels que des cartes à microcircuit avec contacts ou des clés cryptographiques équipées d'un connecteur USB.

Les supports cryptographiques sont remis lors d'un face à face lors duquel le futur porteur doit justifier de son identité.

Les codes PINs permettant l'usage des clés privées résidant sur les supports cryptographiques sont fournis par courrier postal envoyé au futur porteur en Recommandé avec Accusé Réception.

1.1. Présentation générale

La gestion d'un certificat comprend notamment l'ensemble des phases du cycle de vie d'un certificat, de la demande d'attribution d'un certificat, jusqu'à la fin de vie de ce certificat (fin de validité ou révocation). Les politiques de certification sont définies indépendamment des détails de l'environnement utilisé pour la mise en œuvre de l'infrastructure de gestion de la confiance à laquelle elle s'applique.

L'objectif de ce document est de définir les engagements minimums que la Poste Maroc, en tant que prestataire de services de certification électronique (PSCE), s'engage à respecter dans l'émission, la délivrance et la gestion de certificats supportant la signature électronique et délivrés par l'AC Classe 3 tout au long de leur cycle de vie.

La définition de ces PCs fait intervenir des exigences temporelles requises pour le niveau de sécurité escompté. La section 9.2 ci-après permet de quantifier ces valeurs.

Afin de faciliter la lecture de ce document, sa structure suit celle définie dans le [RFC 3647].

1.2. Acronymes et Terminologie

1.2.1. Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

AA	Autorité Administrative
AC	Autorité de Certification
ANRT	Agence Nationale de Réglementation des Télécommunications
AE	Autorité d'Enregistrement
ASN 1	Abstract Syntax Notation One
CRL	Certificate Revocation List
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards Publications
IETF	Internet Engineering Task Force
IGC	Infrastructure de Gestion de Clés.
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
OCSP	On-line Certificate Status protocol
OID	Object Identifier (identifiant d'objet)
PC	Politique de Certification
PP	Profil de Protection
PIN	Personal Identification Number (code numérique à 6 chiffres)
PSCE	Prestataire de Services de Certification Electronique
RSA	Rivest Shamir Adelman
SP	Service de Publication
RFC	Request For Comments
SHA	Secure Hash Algorithm

1.2.2. Terminologie

- **Authentification** – Action de s'assurer de l'identité ou de l'identifiant présumé d'une entité donnée ou de l'origine d'une communication ou d'un fichier.
- **Autorité Administrative** – Autorité responsable d'une IGC et possédant un pouvoir décisionnaire au sein de celle-ci.
- **Autorité d'Enregistrement (AE)** - Au sein d'un PSCE, une entité a en charge, au nom et sous la responsabilité de ce PSCE, la prise en compte des demandes de certificats et éventuellement des demandes de révocation des certificats.
- **Autorité de Certification (AC)** – Au sein d'un PSCE, une entité 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.
- **Autorité de Certification Racine** – Une Autorité de Certification située au sommet d'une hiérarchie d'ACs.
- **Applications utilisatrices** - Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur d'un certificat.
- **Certificat (numérique)** - Fichier 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 un certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre un identifiant de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une période donnée précisée dans celui-ci.
- **Code PIN** (Personal identification Number) – Code numérique personnel de 6 chiffres permettant d'activer une clé privée protégée dans un support cryptographique.
- **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. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.
- **Confidentialité** – fonction ou service permettant d'assurer la protection de la sémantique de données stockées ou échangées.
- **Déclaration des pratiques de certification (DPC)** - Ensemble des pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique 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.
- **Intégrité** – concerne la détection de modifications de données stockées ou échangées.

- **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'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 Certificats Révoqués (LCR)** – Liste des numéros de certificats émis par une AC qui doivent être considérées comme non valides bien de n'ayant pas encore atteint leur fin de validité. La liste ne contient pas les numéros de certificats révoqués au-delà de la fin de leur période de validité.
- **Mandataire de Certification (MC)** : Un mandataire de certification peut être désigné par l'entité cliente et placé sous sa responsabilité. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des porteurs de cette entité (il assure notamment le face-à-face pour l'identification des porteurs) lorsque celui-ci est requis).
- **Politique de certification (PC)** - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une 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 et les utilisateurs de certificats.
- **Porteur** : personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat.
- **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. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de l'AC ayant émis ce certificat et qui est 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 cryptographique** – Support physique, qui peut être soit une carte à microcircuit avec contacts, soit une clé cryptographique équipée d'un connecteur USB, contenant au moins un certificat et la clé privée associée.

1.3. Niveau de sécurité

Conformément au décret n°2-08-518 pris pour l'application des articles 13, 14, 15 et 21 et 23 de la loi n°53-05 relative à l'échange électronique des données juridiques, le tableau suivant décrit le niveau sécurisé du point de vue enjeux considérés:

Domaine	**Niveau sécurisé**
Contextes type d'utilisation	Risques **très forts** de tentative d'usurpation d'identité pour pouvoir signer indûment des données (intérêt pour les usurpateurs, effets de la signature, etc.).

1.4. PSCE et niveau de sécurité

Au niveau sécurisé décrit ci-dessus, correspondent des processus organisationnels, techniques et sécuritaires adaptés détaillés dans le tableau ci-dessous :

Domaine	**Niveau sécurisé**
Validation initiale de l'identité du porteur	Contrôle de l'identité en face-à-face ou suivant une méthode équivalente.
Remise / acceptation d'un certificat	Remise en face-à-face si l'authentification du porteur se fait en face-à-face et que celle-ci n'a pas eu lieu à l'enregistrement. Vérification que le certificat est bien associé à la clé privée correspondante. Acceptation explicite du certificat par le porteur.
Révocation d'un certificat	Authentification formelle de la demande via un mécanisme fort (ex : série de 4/5 questions / réponses, utilisation d'un certificat et d'un outil sécurisé,...) Service accessible 24h/24 et 7j/7,
Service d'état des certificats	Publication de LCRs ainsi qu'un service en ligne informant de l'état révoqué / non révoqué d'un certificat (service OCSP). Service accessible 24h/24 et 7j/7.

Protection des clés de l'AC (privées / publiques)	Génération et mise en œuvre des clés et des certificats de l'AC dans un module cryptographique répondant aux exigences de la PC Type, certifié à un niveau équivalent à EAL4+ des critères communs. Cérémonies des clés sous le contrôle d'au moins deux personnes (rôles de confiance) et au moins deux témoins externes (dont un officier public recommandé). Contrôle des clés privées de l'AC par au moins deux personnes dans des rôles de confiance (porteurs de parts de secrets). Activation des clés privées de l'AC par au moins deux personnes dans des rôles de confiance.

1.5. Signature électronique sécurisée et certificat sécurisé

La mise en œuvre d'un procédé de signature électronique respectant les exigences définies pour le niveau sécurisé permet de bénéficier de la présomption de fiabilité du procédé de signature tels que définies dans l'article 417-3 du dahir formant Code des obligations et des contrats.

En effet, les exigences formulées dans la présente PC à l'égard des prestataires de services de certification électronique et des dispositifs de création de signature électronique sécurisée répondent aux exigences de l'Article 6 de la Loi 53-05 relative à l'échange électronique des documents juridiques.

1.6. Identification des PCs

L'arc OID des PCs est indiqué ci-dessous :

- niveau Baridesign: 1.2.504.1.1.1.1,
- niveau PC : 1,
- niveau ACs externes: 1,
- niveau environnement de production : 1,
- niveau usage du certificat :
  - 25 (Baridesign AC Classe 3 – signature sécurisée – pro),
  - 26 (Baridesign AC Classe 3 – signature sécurisée – particulier),
- niveau version majeure de document : 1 (version 1), 2 (version 2), ...

Nota :

Les rubriques spécifiques aux professionnels sont marquées : [PROFESSIONNELS]

Les rubriques spécifiques aux particuliers ont marquées : [PARTICULIERS]

1.7. Fonctionnalités minimales couvertes

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

- **Autorité d'enregistrement (AE)** - Cette fonction vérifie les informations d'identification des demandeurs de certificats avant de transmettre les demandes à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. Il s'agit d'une part des demandeurs de certificats (porteurs) et d'autre part de certificats pour les administrateurs de l'AC. L'AE a également en charge, lorsque cela est nécessaire, la re-vérification des informations des demandeurs lors du renouvellement d'un certificat d'AC.
- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement (AE) et de la clé publique associée.
- **Fonction de génération des éléments secrets des porteurs** - Cette fonction génère les éléments secrets à destination des porteurs, et les prépare en vue de leur remise (par exemple, personnalisation de la carte à puce, courrier sécurisé avec le code d'activation, etc.).
- **Fonction de remise du certificat** - Cette fonction remet à un porteur ou à un administrateur au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif du porteur, codes d'activation,…).

- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats.
- **Fonction de gestion des révocations** - Cette fonction traite les demandes de révocation des certificats (notamment identification et authentification des demandeurs) et détermine les actions à mener.
- **Fonction d'information sur l'état des certificats -** Cette fonction fournit aux utilisateurs de certificats d'AC des informations sur l'état (révoqué, non révoqué) des certificats. Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR).

1.8. Interactions avec l'IGC

Un certain nombre d'entités et personnes interagissent avec l'IGC ou au sein de l'IGC. Il s'agit notamment de :

- **Autorité de certification (AC)** - Au sein d'un PSCE, l'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.
- **Autorité d'Enregistrement (AE)** - A pour rôle la prise en compte et la vérification des informations du demandeur du certificat et la constitution du dossier d'enregistrement correspondant.
- **Porteur** - La personne physique identifiée dans le certificat (en l'occurrence un demandeur de certificat ou un administrateur de l'AC) et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat.
- **Utilisateur de certificat** - L'entité (e.g. serveur informatique) ou la personne physique qui se fie à un certificat émis par cette AC.

1.9. Responsabilités

1.9.1. De L'AC du PSCE

Quelle que soit l'organisation opérationnelle mise en œuvre par le PSCE, celui-ci, en tant que personne morale, reste in fine responsable vis-à-vis de toute partie externe à l'IGC (utilisateurs, autorités publiques, etc.) des prestations fournies et garantit le respect des engagements pris dans sa PC et sa DPC, relatifs à son activité de certification.

Dans le cadre de ses fonctions opérationnelles, le PSCE assume directement ou sous-traite à des entités externes, les exigences suivantes :

- L'AC est en relation par voie contractuelle / hiérarchique / réglementaire avec les porteurs pour la gestion de leurs certificats ;
- L'AC rend accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux porteurs, aux utilisateurs de certificats, … qui mettent en œuvre ses certificats ;
- L'AC s'assure que les exigences de la famille de certificats concernés cette 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 ;
- L'AC conduit une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre ; et élabore sa DPC en fonction de cette analyse ;
- L'AC met en œuvre les différentes fonctions identifiées dans sa PC, notamment en matière de génération des certificats, de remise aux porteurs, de gestion des révocations et d'information sur l'état des certificats ;
- L'AC met 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 ;
- L'AC génère et renouvelle lorsque nécessaire, ses bi-clés et assurer la gestion des certificats et des LCRs avec les nouvelles bi-clés ;
- L'AC met en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état de ses certificats :
    - Publication de sa politique de certification, couvrant l'ensemble des rubriques du [RFC 3647];
    - Publication de la liste des certificats révoqués;
    - Publication des certificats auto-signés de l'AC Racine de rattachement, en cours de validité;
    - Publication, à destination des porteurs de certificats, des différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.). Les délais et les fréquences de publication dépendent des informations concernées :
        - Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), l'information est publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.
        - Pour les certificats d'AC, ils sont diffusés sous délai T_DIFF_AC.
    - Information sur l'état de ses certificats au moyen d'un répondeur OCSP.

- Les exigences de disponibilité des systèmes publiant ces informations dépendent des informations concernées :
    - Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), les systèmes ont une disponibilité de T_INF_DISP avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de T_INF_INDISP et une durée totale maximale d'indisponibilité par mois de T_INF_MAX, ceci hors cas de force majeure.
    - Pour les certificats d'AC, les systèmes ont une disponibilité de T_AC_DISP avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de T_AC_INDISP et une durée totale maximale d'indisponibilité par mois de T_AC_MAX, ceci hors cas de force majeure.
    - Pour les informations d'état des certificats (cf. section 3.10).

A 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 non disponibilité de cette information et que les exigences ci-dessus s'appliquent également à la disponibilité des informations publiées sur ces systèmes.

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture depuis l'Internet. L'accès à l'information sur l'état des certificats au moyen d'un répondeur OCSP est libre d'accès depuis l'Internet.

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).

1.9.2. De l'AE du PSCE

Les responsabilités de l'AE du PSCE sont les suivantes :

- 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,
- L'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage),
- La conservation et la protection en confidentialité et en intégrité des données personnelles des demandeurs de certificats, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

1.9.3. Du porteur des certificats

Dans le cadre des présentes PC, un porteur de certificat ne peut être qu'une personne physique. Cette personne utilise sa clé privée et le certificat correspondant pour son propre compte ou dans le cadre de ses activités en relation avec l'entité identifiée dans le certificat et avec laquelle il a un lien contractuel / hiérarchique / réglementaire.

1.9.4. Du MC

Les engagements du MC à l'égard du PSCE sont précisés dans un contrat écrit avec l'entité responsable du MC. Ce contrat stipule notamment que le MC doit :

- effectuer correctement et de façon indépendante les contrôles d'identité des futurs porteurs de l'entité pour laquelle il est MC ;
- respecter les parties de la PC et de la DPC qui lui incombent.

1.10. Usage des certificats

1.10.1. Domaines d'utilisation applicables

1.10.1.1 Bi-clés et certificats des porteurs

Le présent document traite des bi-clés et des certificats à destination de différentes catégories de porteurs afin que ces derniers puissent signer électroniquement des données (documents ou messages) dans le cadre d'échanges électroniques. L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de signature électronique.

Dans le cadre d'une application d'échanges dématérialisés de niveau sécurisé, les certificats de signature électronique objets du présent document sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité afin de pouvoir signer indûment des données sont très forts (intérêt pour les usurpateurs, effets de la signature, etc.).

De telles signatures électroniques apportent, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données. L'utilisateur du certificat a ainsi l'assurance que le porteur identifié dans le certificat a manifesté son consentement quant au contenu des données signées électroniquement à l'aide de la clé privée correspondante.

La présente PC traite:

- o des bi-clés et des certificats à usage de signature sécurisée pour les professionnels,
- o des bi-clés et des certificats à usage de signature sécurisée pour les particuliers.

Nota : Certaines applications d'échanges dématérialisés peuvent nécessiter des certificats à des fins de validation ou de recette. Les certificats à des fins de validation ou de recette sont identiques aux certificats "de production" fournis et gérés par l'AC du PSCE, à ceci près qu'ils sont gérés par une AC différente et que cette AC utilise des clés différentes.

Le champ CN du DN de cette AC de test est : TEST Baridesign AC Classe 3

L'arc OID des PCs de test est indiqué ci-dessous :

- niveau Baridesign: 1.2.504.1.1.1.1,
- niveau PC : 1,
- niveau ACs externes: 1,
- niveau environnement de test : 2,
- niveau usage du certificat :
  - 25 (Baridesign AC Classe 3 – signature sécurisée – pro),
  - 26 (Baridesign AC Classe 3 – signature sécurisée – particulier),
- niveau version majeure de document : 1 (version 1), 2 (version 2), ...

1.10.1.2 Bi-clés et certificats d'AC et de composantes

Ce document comporte également des exigences, lorsque nécessaire, concernant les bi-clés et certificats de l'AC (signature des certificats des porteurs, des LCRs et des réponses OCSP ainsi que des clés, bi-clés et certificats des composantes de l'IGC (sécurisation des échanges entre composantes, authentification des opérateurs, etc.).

L'AC gère différents types d'objets : des certificats, des LCRs et des réponses OCSP.

Pour signer les certificats des porteurs, des administrateurs, des serveurs OCSP ainsi que les LCRs, l'AC dispose d'une bi-clé.

Pour signer les réponses OCSP, l'AC utilise des serveurs OCSP qui disposent d'autres bi-clés. Les certificats correspondant à ces bi-clés sont générés par l'AC.

L'ensemble des clés privées ci-dessus ne sont utilisés que pour la signature de certificats, de LCRs et/ou de réponses OCSP.

1.11. Gestion de la PC

1.11.1. Entité gérant la PC

Poste Maroc est responsable de la validation et de la gestion de la PC répondant aux exigences de la présente PC.

1.11.2. Point de contact

Toute demande d'information peut se faire auprès du :

Préciser la fonction de la personne (par exemple : RSSI de XXX), une adresse postale et une adresse e-mail (boite de service).

1.11.3. Entité déterminant la conformité d'une DPC avec cette PC

Le document [DPC] est approuvé par l'Autorité Administrative de l'AC (AA).

1.11.4. Procédures d'approbation de la conformité de la DPC

L'Autorité Administrative de l'AC nomme les personnes (ou l'entité) qui déterminent la conformité de la DPC avec la présente PC.

2. IDENTIFICATION ET AUTHENTIFICATION

2.1. Nommage

2.1.1. Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500. Dans chaque certificat X509 V3 de l'IUT-T (voir [X.509]), l'AC émettrice (issuer) et le porteur (subject) sont identifiés par un "Distinguished Name" DN de type X.501 dont le format exact est :

Pour le champ issuer :

CN= Baridesign AC Classe 3

OU= Baridesign

OU= 50413 (numéro d'immatriculation de Poste Maroc au Registre Central du Commerce tenu par l'Office Marocaine de la Propriété Industrielle et Commerciale (OMPIC))

O= Barid Al Maghrib

C= MA (Maroc)

Pour le champ subject :

- [PROFESSIONNELS] pour un certificat destiné à un professionnel:

SN= numéro de série attribué par l'AC pour différencier des homonymes (mêmes nom et prénoms)

CN= *NOM Prénom*

userid= nom pouvant être utilisé en tant qu'identifiant unique pour s'authentifier à un système informatique (computer system login name). Cet attribut est décrit dans le RFC 1274 à la section 9.3.1. Son OID est le suivant : { itu-t(0) data(9) pss(2342) ucl(19200300) pilot(100) pilotAttributeType(1) userid(1) }. Cet attribut est optionnel.

OU= nom de l'unité d'organisation à laquelle le professionnel appartient

OU= numéro d'immatriculation de l'organisation au Registre Central du Commerce tenu par l'Office Marocaine de la Propriété Industrielle et Commerciale (OMPIC)

O= nom de l'organisation à laquelle le professionnel appartient.

C= MA (Maroc)

- [PARTICULIERS] pour un certificat destiné à un particulier:

  SN= numéro de série attribué par l'AC pour différencier des homonymes (mêmes nom et prénoms)

  CN= *NOM Prénom*

  userid= nom pouvant être utilisé en tant qu'identifiant unique pour s'authentifier à un système informatique (computer system login name). Cet attribut est décrit dans le RFC 1274 à la section 9.3.1. Son OID est le suivant : { itu-t(0) data(9) pss(2342) ucl(19200300) pilot(100) pilotAttributeType(1) userid(1) }. Cet attribut est optionnel.

  C= MA (Maroc)

2.1.2. Nécessité d'utilisation de noms explicites

Le DN du porteur est construit à partir des nom et prénom, de son état civil tels que portés sur les documents d'identité présentés lors de son enregistrement auprès de l'AE ou, le cas échéant, du MC.

[PROFESSIONNELS] Pour un professionnel, sont ajoutés :

- le nom du pays dans lequel les autres attributs doivent être compris,
- le nom de l'organisation à laquelle le professionnel appartient,
- le numéro d'immatriculation de l'organisation au Registre Central du Commerce tenu par l'Office Marocaine de la Propriété Industrielle et Commerciale (OMPIC),
- le nom de l'unité d'organisation à laquelle le professionnel appartient.

[PARTICULIERS] Pour un particulier, sont ajoutés :

- le nom du pays dans lequel les autres attributs doivent être compris.

2.1.3. Unicité des noms

Afin d'assurer une continuité d'une identification unique du porteur au sein du domaine de l'AC dans ses certificats successifs (renouvellement) et pour éviter toute ambiguïté, le DN du champ "subject" de chaque certificat de porteur permet d'identifier de façon unique le porteur correspondant au sein du domaine de l'AC.

Durant toute la durée de vie de l'AC, un DN attribué à un porteur de certificats ne sera jamais attribué à un autre porteur. En effet, l'attribut « numéro de série » inclus dans le DN pour différencier des homonymes est un numéro unique attribué par l'AC.

A noter que le numéro de série du certificat est propre au certificat et non pas au porteur et donc ne peut pas être utilisé pour assurer une continuité de l'identification des certificats successifs d'un porteur donné.

2.1.4. Identification, authentification et rôle des marques déposées

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

2.2. Validation initiale de l'identité du demandeur de certificat

L'enregistrement d'un porteur peut se faire soit directement auprès de l'AE, soit via un mandataire de certification. Dans ce dernier cas, le MC doit être préalablement enregistré par l'AE.

2.2.1. Méthode pour prouver la possession de la clé privée

Les clés des porteurs sont générées directement dans un support cryptographique.

Que ce soit pour une première demande de certificat ou pour un renouvellement de certificat, le support cryptographique est systématiquement fourni par le PSCE. Le support est remis au porteur lors d'un face à face.

2.2.2. Enregistrement d'une demande

Le dossier d'enregistrement d'un porteur, déposé auprès de l'AE, doit comprendre :

[PARTICULIERS] : Si le futur porteur est un particulier, ce dernier doit en outre communiquer

- Formulaire signé de la demande de certificat électronique et daté de moins de trois mois, le formulaire doit contenir l'adresse professionnelle, l'adresse e-mail professionnelle du futur porteur, l'agence ABB ou il souhaite récupérer son certificat ainsi que les conditions générales qui doivent être signées par le porteur et légalisée auprès des autorités compétentes.
- Deux copies égalisées de la CIN / passeport du futur porteur (Carte de séjour pour les étrangers résidents).
- une enveloppe spécifique contenant les questions secrètes

  Note - Un jeu de questions/réponses sera utilisé comme éléments d'authentification lors d'une demande de révocation. En outre, lors d'un appel téléphonique, le porteur est informé que les informations personnelles d'identité pourront être utilisées comme éléments complémentaires d'authentification lors d'une demande de révocation.

- Une adresse postale personnelle où il peut être joint,
- Une adresse courriel (email) où il peut être joint.

[PROFESSIONNELS] : Si le futur porteur est un professionnel, ce dernier doit en outre communiquer

Les pièces administratives suivantes :

Pour une personne morale :

- Un exemplaire de la ou les pièces mentionnées au tableau ci dessous suivant la nature de la personne morale constatant qu'elle est régulièrement constituée et qu'elle a satisfait aux conditions de publicité prévues par la loi;
- Si nécessaire, Procuration légalisée conférant mandat à une personne physique pour la gestion des certificats de la personne morale, le mandataire ainsi désigné est préalablement enregistré pour l'obtention d'un certificat.
- Formulaire de demande de certificat électronique co-signé par le mandataire et le porteur et daté de moins de trois mois, le formulaire doit contenir l'adresse professionnelle, le numéro de téléphone, l'adresse e-mail professionnelle du futur porteur, l'agence ABB ou il souhaite récupérer son certificat (optionnelle). S'il s'agit d'un certificat de classe 2 ou 3, le formulaire doit être légalisé.
- Les conditions générales qui doivent être co-signées par le mandataire et le porteur avec mention d'approbation du mandataire et légalisées auprès des autorités compétentes.
- Deux copies légalisées de la CIN / passeport du futur porteur (Carte de séjour pour les étrangers résidents).
- Une enveloppe spécifique contenant les questions secrètes

Nature de la personne morale	Pièces Justificatives
Société SA	▪ Statuts revêtus de la signature légalisée du président ▪ Procès verbal de l'assemblée générale constitutive légalisé ▪ Procès verbal du conseil d'Administration légalisé ▪ Copie certifiée de la déclaration d'immatriculation au registre de commerce
Autre forme juridique de société	▪ Statuts revêtus de la signature légalisée du personnel ▪ Procès verbal de l'assemblée générale constitutive légalisé ▪ Copie certifiée de la déclaration d'immatriculation au registre de commerce
Association	▪ Statuts revêtus de la signature légalisée du président ▪ Procès verbal de l'assemblée générale constitutive légalisé ▪ Liste des membres du bureau timbrée et légalisée ▪ Copies certifiées des récépissés de dépôt (Wilaya et tribunal
Pour les entreprises individuelles et les fonctions réglementées (commerçant, professions libérales...)	▪ copie de l'identifiant fiscal et/ou copie de registre de commerce.

Pour les entreprises individuelles et les fonctions réglementées (commerçant, professions libérales...):

- Procuration légalisée conférant mandat à une personne physique pour la gestion des certificats, le mandataire ainsi désigné est préalablement enregistré pour l'obtention d'un certificat.
- Formulaire de la demande de certificat électronique co-signé par le mandataire et le porteur et daté de moins de trois mois, le formulaire doit contenir l'adresse professionnelle, le numéro de téléphone, l'adresse e-mail professionnelle du futur porteur, l'agence ABB ou il souhaite récupérer son certificat (optionnelle). s'il s'agit d'un certificat de classe 2 ou 3, le formulaire doit être légalisé auprès des autorités compétentes.
- Les conditions générales qui doivent être co-signées par le mandataire et le porteur avec mention d'approbation du mandataire et légalisées auprès des autorités compétentes.
- copie de l'identifiant fiscal et/ou copie de registre de commerce.
- Deux copies légalisées de la CIN / passeport du futur porteur (Carte de séjour pour les étrangers résidents).
- une enveloppe spécifique contenant les questions secrètes

Le dossier d'enregistrement peut être déposé par le futur porteur lui-même ou par un mandataire de certification.

2.2.3. Informations non vérifiées du porteur

L'adresse personnelle où le porteur peut être joint, si celle-ci est différente de celle indiquée sur le document attestant l'identité du futur porteur, n'est pas vérifiée lors de l'enregistrement. Toutefois, le porteur ne pourra pas entrer en possession de son PIN et de son support cryptographique si cette adresse est inexacte.

2.2.4. Validation de l'autorité du demandeur

Cette étape est réalisée lors de l'enregistrement via l'AE ou le MC le cas échéant.

2.2.5. Critères d'interopérabilité

Le cas échéant, l'AC documente les accords de reconnaissance avec des AC extérieures au domaine AC Racine BarideSign e-gov auquel l'AC appartient.

2.3. .Identification et validation d'une demande de renouvellement des clés

Le renouvellement de la bi-clé d'un certificat entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne peut pas être fourni à un porteur sans renouvellement de la bi-clé correspondante.

2.3.1. Identification et validation pour un renouvellement courant

L'identification et la validation d'un porteur est identique à une demande initiale, à ceci près que le jeu de questions/réponses utilisé comme éléments d'authentification lors d'une demande de révocation n'est pas demandé. Pour les certificats des administrateurs de l'AC, la procédure est simplifiée et différente.

2.3.2. Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial, à ceci près que le jeu de questions/réponses utilisé comme éléments d'authentification lors d'une demande de révocation n'est pas demandé.

2.3.3. Identification et validation d'une demande de révocation

Les demandes de révocation des certificats des porteurs peuvent effectuées, soit via un service en ligne (serveur web), soit via un service téléphonique.

Lorsque la demande est effectuée via un service en ligne, le porteur doit s'identifier au moyen de l'adresse courriel (email) qu'il a renseignée dans le formulaire d'enregistrement, puis s'authentifier au moyen de 5 questions / réponses sur des informations propres au demandeur choisies au moment de l'enregistrement.

Lorsque la demande est effectuée via un service téléphonique auprès d'un guichet d'assistance, les demandes de révocation peuvent effectuées, soit par le porteur, soitpar son mandataire.

3. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

3.1. Demande de certificat

3.1.1. Origine d'une demande de certificat

Un certificat ne peut être demandé, que par le futur porteur, ou par un MC dûment mandaté par l'organisation à laquelle le professionnel appartient, avec dans tous les cas consentement préalable du futur porteur.

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

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

- les nom et prénoms du porteur à utiliser dans le certificat ;
- une adresse courriel où le porteur peut être joint ;
- un jeu de questions/réponses qui sera utilisé comme éléments d'authentification lors d'une demande de révocation ;

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

3.2. Traitement d'une demande de certificat

3.2.1. Exécution des processus d'identification et de validation de la demande

Les identités des personnes physiques sont vérifiées conformément aux exigences décrites dans les chapitres précédents.

L'AE, ou le MC le cas échéant, effectue les opérations suivantes :

- valider l'identité du futur porteur ou du responsable de la composante OCSP;
- vérifier la cohérence des justificatifs présentés ;
- s'assurer que le futur porteur ou le responsable de la composante OCSP a pris connaissance des modalités applicables pour l'utilisation du certificat.

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

3.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le ou les demandeurs en justifiant le rejet.

3.2.3. Durée d'établissement du certificat

Pour des certificats des porteurs, la durée de validité est comprise entre T_PORT_MIN et T_PORT_MAX.

3.3. Délivrance d'un certificat

3.3.1. Actions de l'AC concernant la délivrance d'un certificat

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. Pour un certificat de porteur: la bi-clé du porteur, le support cryptographique et le code d'activation.

L'ordonnancement des opérations est assuré ainsi que l'intégrité et l'authentification des échanges entres les composantes en fonction de l'architecture de l'IGC.

Les conditions de génération des certificats et la génération des bi-clés, ainsi que les mesures de sécurité à respecter sont précisés aux chapitres ci-dessous.

3.3.2. Notification par l'AC de la délivrance du certificat à un porteur

Selon le cas, le porteur reçoit à son domicile personnel courrier contenant le code d'activation (PIN) qui l'invite à retirer son support cryptographique auprès d'un bureau postal sur présentation d'une pièce d'identité comportant une photographie.

Le support cryptographique contenant le certificat est remis en mains propres au porteur ou au mandataire lors d'un face-à-face au niveau du bureau de distribution sur présentation d'une pièce d'identité. Le porteur ou le mandataire doit signer une attestation d'acceptation du certificat pour prendre possession du support cryptographique.

3.4. Acceptation du certificat

3.4.1. Démarche d'acceptation du certificat

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

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

Le procès verbal de cérémonie des clés signé par le responsable de la composante OCSP constitue une acceptation explicite du certificat par le responsable de la composante OCSP.

3.4.2. Publication des certificats

Les certificats des porteurs ne sont pas publiés.

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

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

3.5. Usages de la bi-clé et du certificat

3.5.1. Utilisation de la clé privée et du certificat d'un porteur par le porteur

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée pour générer des signatures numériques visant à signaler que le signataire s'engage à accepter les conditions énoncées dans le texte qu'il signe. Le type précis d'engagement du signataire – "examiné et approuvé" ou "avec l'intention d'être lié", par exemple – peut être indiqué par le contenu qui est signé – le document signé proprement dit ou des informations signées complémentaires, par exemple.

Les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé et du certificat associé est indiqué dans le certificat lui-même via l'extension critique « keyUsage ». Seul le bit 1 est positionné. Ce bit signifie « non répudiation » selon le RFC 5280 et «*acceptation du contenu*» (contentCommitment) » selon la recommandation [X.509].

3.5.2. Utilisation des clés publiques et des certificats par les utilisateurs de certificats

L'utilisation de la clé publique contenue dans un certificat de porteur est strictement limitée à la vérification de signatures numériques visant à signaler que le signataire s'engage à accepter les conditions énoncées dans le texte qu'il signe. L'usage autorisé de la bi-clé et du certificat associé est indiqué dans le certificat lui-même via l'extension critique « keyUsage ». Seul le bit 1 est positionné. Ce bit signifie « non répudiation » selon le RFC 5280 et «*acceptation du contenu*» (contentCommitment) » selon la recommandation [X.509].

Les utilisateurs de certificats doivent respecter strictement l'usage autorisé. Dans le cas contraire, leur responsabilité pourrait être engagée.

3.6. Renouvellement d'un certificat

Pour un certificat de porteur, le renouvellement d'un certificat implique la génération de nouvelles bi-clés et donc la génération d'un nouveau certificat.

T_REN_CERT avant la date d'expiration du certificat, le porteur est sollicité à renouveler son certificat. Pour ce faire, il reçoit un courriel l'invitant à effectuer cette opération de renouvellement.

3.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé

Note - Conformément au [RFC 3647], ce chapitre traite de la délivrance d'un nouveau certificat liée à la génération d'une nouvelle bi-clé.

3.7.1. Causes possibles de changement d'une bi-clé

Les bi-clés sont périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat. Ainsi les bi-clés des porteurs, et les certificats correspondants, auront une durée maximum de T_PORT_MAX.

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

3.7.2. Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat est à l'initiative du demandeur. Le demandeur est invité à faire une demande de renouvellement T_REN_CERT avant la date d'expiration du certificat.

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

3.7.3. Procédure de traitement d'une demande d'un nouveau certificat

Voir chapitres précédents.

3.7.4. Notification au porteur de l'établissement du nouveau certificat

Voir chapitres précédents.

3.7.5. Démarche d'acceptation du nouveau certificat

Voir chapitres précédents.

3.7.6. Publication du nouveau certificat

Voir chapitres précédents.

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

Voir chapitres précédents.

3.8. Modification du certificat

La modification de certificat n'est pas autorisée dans la présente PC.

3.9. Révocation et suspension des certificats

3.9.1. Causes possibles d'une révocation

3.9.1.1 Certificats de porteurs

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

- les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat ;
- le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- la clé privée du porteur est suspectée de compromission, est compromise, est perdue ou est volée ;
- le porteur ou une entité autorisée (représentant légal de l'entité) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du porteur et/ou de son support) ;
- le décès du porteur ou la cessation d'activité de l'entité du porteur.

3.9.1.2 Certificats d'une composante de l'IGC

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

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

3.9.2. Origine d'une demande de révocation

3.9.2.1 Certificats de porteurs

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

- le porteur au nom duquel le certificat a été émis ;
- le MC,
- un représentant légal de l'AA de l'AC.

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

3.9.2.2 Certificats d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC 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'AA sans délai.

3.9.3. Procédure de traitement d'une demande de révocation

3.9.3.1 Révocation d'un certificat de porteur

Un porteur peut révoquer lui-même un certificat, 24 h / 24 et 7 j / 7, en se connectant sur l'Internet. Ce processus est le seul moyen de révoquer lorsque l'incident se produit en dehors des heures ouvrées.

Le porteur se connecte aux services en ligne, sur la page correspondant à la fonction de révocation de l'AC Baridesign Classe 3. Il doit saisir une série de caractères affichés à l'écran d'une manière déformée (cette étape permet de réduire les risques associés aux attaques par des automates).

Il s'identifie en communicant son adresse de courriel, et répond aux questions secrètes afin de s'authentifier.

Le porteur est alors invité à communiquer les informations permettant de retrouver rapidement et sans erreur le certificat à révoquer ainsi que la raison de la révocation.

Une fois l'opération de révocation effectuée, un courriel de confirmation lui est envoyé.

La révocation peut aussi être effectuée durant les heures ouvrées en appelant par téléphone un guichet d'assistance.

Le demandeur peut être:

1) le porteur,

le mandataire de certificationSi le demandeur est un porteur, il est d'abord identifié :

1. il donne son prénom usuel et son nom,
2. il donne son adresse de courriel,

Le porteur est ensuite authentifié :

- il répond aux questions secrètes.

Si le demandeur est le mandataire de certification, ce dernier dispose de 2 modalités de révocation :

- **Envoyer la demande de révocation de(s) certificat(s) par courriel sécurisé à l'opérateur du guichet d'assistance :**

  Le mandataire reçoit un accusé de lecture relatif au courriel de révocation qu'il a envoyé.

  Suite à cela, il reçoit, dans un délai de 12 h, une notification de la révocation de son certificat.

  Le Mandataire est amené à appeler le guichet d'assistance si sa demande de révocation par courriel sécurisée n'a pas donné lieu à un accusé de réception dans un délai de 4 heures.

- **révoquer le(s) certificat(s) via le guichet d'assistance par courrier et fax :**

  Le mandataire envoie le formulaire de révocation signée par courrier et le faxe au guichet d'assistance.

  L'Opérateur du guichet d'assistance devra rappeler le mandataire sur le n° de téléphone de révocation renseigné sur le formulaire d'enregistrement afin de l'authentifier.

Selon la demande, l'opérateur du guichet d'assistance est amené à révoquer :

- Tous les certificats d'un porteur situés sur un même support cryptographique,
- Un certificat particulier.

Une fois l'opération de révocation effectuée, un courriel de confirmation est envoyé au porteur.

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

3.9.3.2 Révocation d'un certificat d'une composante de l'IGC

Les demandes de révocation d'un certificat d'une composante de l'IGC sont faites en face-à-face sur présentation d'une demande signée par un administrateur de l'AC ou par l'autorité compétente (l'AA de l'AC).

Les informations suivantes doivent au moins figurer dans la demande de révocation de certificat :

- le nom du demandeur de la révocation ;
- le DN de la composante de l'IGC dont le certificat est à révoquer ;
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer ;
- la cause de révocation.

Une fois la demande authentifiée et contrôlée par l'AA de l'AC, s'il s'agit d'un certificat nécessaire au fonctionnement interne de l'AC, celui-ci est supprimé de la liste des certificats utilisés par l'IGC.

Le demandeur de la révocation est informé du bon déroulement de l'opération et de la révocation effective du certificat.

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.

3.9.4. Délai accordé pour formuler la demande de révocation

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

3.9.5. Délai de traitement par l'AC d'une demande de révocation

3.9.5.1 Révocation d'un certificat

Par nature une demande de révocation est traitée en urgence. La fonction de gestion des révocations est disponible conformément à T_REV_DISP. Cette fonction est réputée avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme à T_REV_INDIS et une durée maximale totale d'indisponibilité par mois conforme à T_REV_MAX.

Toute demande de révocation d'un certificat est traitée dans un délai inférieur à T_REV_TRAIT, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise hors d'usage de ce certificat.

3.9.5.2 Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat à usage interne de l'IGC est effective lorsque le certificat est supprimé des certificats utilisés par l'IGC.

3.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble d'un chemin de certification se terminant à un certificat racine de confiance.

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

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

L'utilisateur de certificat doit s'assurer qu'aucun certificat du chemin de certification n'est révoqué.

S'agissant d'un certificat de signature électronique, la vérification de la validité du chemin de certification peut se faire, soit pour le temps présent, soit pour une date passée.

3.9.7. Fréquence d'établissement des LCR

La fréquence de publication des LCR est conforme à F_PUB_LCR.

3.9.8. Délai maximum de publication d'une LCR

Une LCR est publiée dans un délai maximum conforme à T_PUB_LCR suivant sa génération.

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

Un service OCSP est aussi disponible. L'adresse du serveur OCSP à contacter est indiquée dans chaque certificat. L'utilisateur de certificats doit vérifier que la réponse du serveur OCSP est effectivement signée par le serveur OCSP indiqué dans le certificat et qu'elle a été fournie au moment opportun (en temps réel ou à une date passée). L'utilisateur de certificats doit aussi vérifier que le certificat du serveur OCSP n'est pas révoqué, soit pour le temps présent, soit pour une date passée.

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

Voir chapitre 3.9.6 ci-dessus.

3.9.11. Autres moyens disponibles d'information sur les révocations

Les utilisateurs de certificats ne disposent pas d'autres moyens d'information sur les révocations. Les administrateurs de l'AC disposent de moyens complémentaires et notamment des archives des différentes LCRs qui ont été émises.

3.9.12. Exigences spécifiques en cas de compromission d'une clé privée

Pour les certificats de porteur, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour le certificat de l'AC, l'AA s'adresse dans les meilleurs délais à contacter l'AC du niveau immédiatement supérieur pour demander la révocation de son certificat. Cet évènement exceptionnel

fait aussi l'objet d'une information clairement diffusée au moins sur le site Internet du PSCE et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

3.9.13. Causes possibles d'une suspension

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

3.9.14. Origine d'une demande de suspension

Non applicable.

3.9.15. Procédure de traitement d'une demande de suspension

Non applicable.

3.9.16. Limites de la période de suspension d'un certificat

Non applicable.

3.10. Fonction d'information sur l'état des certificats

3.10.1. Caractéristiques opérationnelles

L'AC 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.

Les fonctions d'information sur l'état des certificats consistent à mettre à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCRs et un service fournissant en temps réel l'état révoqué / non révoqué des certificats (service OCSP).

Les numéros des certificats révoqués des porteurs sont publiés au moyen du mécanisme de LCR.

Ces LCR sont des LCR au format V2, publiées au moins dans un annuaire accessible en protocole LDAP V3. Le profil des LCRs est indiqué à la section 6.2 de ce document.

Les serveurs OCSP sont accessibles au moyen du protocole OCSP défini dans le RFC 2560. Le profil du protocole est indiqué à la section 6.3 de ce document.

L'état révoqué / non révoqué des certificats des porteurs peut être obtenu au moyen du service OCSP.

3.10.2. Disponibilité de la fonction

Les fonctions d'information sur l'état des certificats sont disponibles conformément à T_ETAT_DISP.

Ces fonctions sont réputées avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme à T_ETAT_INDIS et une durée maximale totale d'indisponibilité par mois conforme à T_ETAT_MAX.

3.10.3. Dispositifs optionnels

Les administrateurs de l'AC disposent de moyens complémentaires et notamment des archives des différentes LCRs qui ont été émises. Ces moyens ne sont pas directement accessibles aux utilisateurs de certificats.

3.11. Fin de la relation entre le porteur et l'AC

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre le PSCE et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier est révoqué.

3.12. Séquestre de clé et recouvrement

Ce document traite des aspects de signature électronique et interdit le séquestre des clés privées.

3.12.1. Politique et pratiques de recouvrement par séquestre des clés

Non applicable.

3.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Non applicable.

4. MESURES DE SECURITE NON TECHNIQUES

Les exigences définies dans la suite du présent chapitre sont constituées des exigences minimales que toute AC doit respecter, complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC et des résultats d'une analyse de risque.

Le PSCE élabore sa DPC en fonction d'une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre.

4.1. Mesures de sécurité physique

4.1.1. Situation géographique et construction des sites

La situation géographique des sites ne fait pas l'objet d'une publicité particulière. Leur construction respecte les règlements et normes en vigueur et tient compte des résultats d'une analyse des risques et des exigences spécifiques face à des risques accidentels.

4.1.2. Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services du PSCE, les accès aux locaux des différentes composantes de l'IGC sont contrôlés. L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée.

Pour les fonctions de génération des certificats et de gestion des révocations, de génération des éléments secrets du porteur, l'accès est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, un périmètre de sécurité physique où sont installées les machines des composantes de l'IGC concernées a été défini. La mise en œuvre de ce périmètre permet de respecter la séparation des rôles de confiance telle que prévue dans cette PC.

Note - On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisés pour la mise en œuvre de ces fonctions.

4.1.3. Alimentation électrique et climatisation

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

Elles permettent également de respecter les exigences de la présente PC, ainsi que les engagements pris par l'AC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

4.1.4. Vulnérabilité aux dégâts des eaux

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

4.1.5. Prévention et protection incendie

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

4.1.6. Conservation des supports

Dans le cadre de l'analyse de risque, les différentes informations intervenant dans les activités de l'IGC ont été identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations sont traités et conservés dans une enceinte sécurisée accessibles aux seules personnes autorisées.

Parmi les supports, on distingue :

- les cartes d'installation, contenant une partie du secret d'accès aux clés de l'AC qui sont conservées dans des coffres forts;
- les cartes d'activation des clés du boîtier cryptographique qui sont dupliquées et qui sont stockées dans des coffres forts,
- les archives et leur copie de secours qui sont conservées dans des coffres forts différents sur le site de production.

4.1.7. Mise hors service des supports

En fin de vie, les supports papier et magnétiques sont systématiquement détruits par des moyens appropriés, permettant d'éviter toute perte de confidentialité. Les dossiers d'enregistrement sont conservés au moins pendant la période de validité des certificats (en cas de renouvellement, la durée est prolongée).

Les supports de stockage (disque dur) de l'AC ne sont pas être réutilisés à d'autres fins avant destruction complète des informations liées à l'AC qu'ils sont susceptibles de contenir.

4.1.8. Sauvegardes hors site

En complément de sauvegardes sur sites, les composantes de l'IGC mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes sont organisées

de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conforme aux exigences de la présente PC et aux engagements de l'AC en matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des certificats.

Les informations sauvegardées hors site respectent les exigences de la présente PC en matière de protection en confidentialité et en intégrité de ces informations.

Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, au moins, mettent en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.).

4.2. Mesures de sécurité procédurales

4.2.1. Rôles de confiance

Afin de veiller à la séparation des tâches critiques, on distingue les six rôles suivants au sein de l'AC :

- **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'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.
- **Responsable d'application** - Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC 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'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
- **Contrôleur** - Personne 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'IGC et aux politiques de sécurité de la composante.
- **Responsable qualité** : Personne chargée d'assurer la cohérence des actions des différents rôles décrits précédemment et de la qualité des services rendus aux utilisateurs.

En plus de ces rôles de confiance au sein de chaque composante de l'IGC, et en fonction de l'organisation de l'IGC et des outils mis en œuvre, le PSCE peut être amené à distinguer également en tant que rôle de confiance, les rôles de porteur de parts de secrets d'IGC. Ces porteurs de parts de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiés.

Les rôles de confiance spécifiques aux Cérémonies des Clés sont décrits dans le document de Cérémonie des Clés. Ce document n'est pas public.

4.2.2. Nombre de personnes requises par tâches

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

Pour des raisons de sécurité, les fonctions sensibles sont réparties sur plusieurs personnes. La présente PC définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'AC.

La DPC de l'AC précise, en fonction des résultats de son analyse de risque, quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.).

4.2.3. Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'AC fait vérifier l'identité et les autorisations de tout membre du personnel ou de tout prestataire amené à travailler au sein d'une composante de l'AC avant de lui attribuer un rôle et les droits correspondants, notamment :

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

Ces contrôles sont décrits dans la DPC de l'AC et sont conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'AC est notifiée par écrit. Le responsable de Sécurité est informé de chaque nomination.

4.2.4. Rôles exigeant une séparation des attributions

Les attributions associées à chaque rôle sont décrites dans la DPC de l'AC et être conformes à la politique de sécurité de la composante concernée.

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. Pour les rôles de confiance, il est néanmoins requis que les exigences de non cumul ci-dessous soient respectées.

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur ;
- contrôleur et tout autre rôle ;
- ingénieur système et opérateur.

4.3. Mesures de sécurité vis-à-vis du personnel

4.3.1. Qualifications, compétences et habilitations requises

Tous les agents d'autorités administratives sont soumis à un devoir de réserve.

Chaque entité opérant une composante de l'AC s'assure que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'AC.

L'AA de l'AC informe toute personne intervenant dans des rôles de confiance de l'AC par une lettre de mission signée:

- de ses responsabilités relatives aux services de l'AC;
- des procédures liées à la sécurité du système et au contrôle du personnel.

4.3.2. Procédures de vérification des antécédents

Chaque entité opérant une composante de l'AC met en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions. Ils devront remettre à leur employeur 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 sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans). Le service du personnel est en charge de la conservation des dossiers.

4.3.3. Exigences en matière de formation initiale

Le personnel est préalablement 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.

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

4.3.4. Exigences et fréquence en matière de formation continue

Le personnel est préalablement 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.

Le personnel doit avoir la connaissance et comprendre les implications des opérations dont il a la responsabilité.

4.3.5. Fréquence et séquence de rotation entre différentes attributions

Cette information figure dans la DPC.

4.3.6. Sanctions en cas d'actions non autorisées

L'Autorité Administrative de l'AC décide des sanctions à appliquer lorsqu'un personnel abuse de ses droits ou bien effectue une opération non conforme à ses attributions.

4.3.7. Exigences vis-à-vis du personnel des prestataires externes

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC doit également respecter les exigences du présent chapitre. Ceci est traduit en clauses adéquates dans les contrats avec ces prestataires.

4.3.8. Documentation fournie au personnel

Le personnel dispose de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille.

La documentation adéquate, dont doit disposer le personnel en fonction de son besoin d'en connaître pour l'exécution de sa mission, est composée des documents suivants :

- la PC,
- la DPC,
- les procédures internes,
- les manuels d'exploitation,
- les documents techniques relatifs aux matériels et logiciels utilisés.

4.4. Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique. Les fichiers résultants, sous forme papier ou électronique, permettent la traçabilité et l'imputabilité des opérations effectuées.

4.4.1. Type d'évènements à enregistrer

Chaque entité opérant une composante de l'AC journalise au minimum les évènements suivants, automatiquement dès le démarrage d'un système et sous forme électronique, concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de l'AC:

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

D'autres évènements doivent aussi être recueillis par le Responsable sécurité de l'AC, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques ;
- les actions de maintenance et de changements de la configuration des systèmes ;
- les changements apportés au personnel ;
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,...).

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC doivent également être journalisés, notamment :

- réception d'une demande de certificat (initiale et renouvellement) ;
- validation / rejet d'une demande de certificat ;
- évènements liés aux clés de signature et aux certificats d'AC (cérémonie des clés) ;
- sauvegarde / récupération, révocation, renouvellement, destruction,... ;
- le cas échéant, génération des éléments secrets du porteur (bi-clé, codes d'activation,…) ;
- génération des certificats des porteurs ;
- transmission des certificats aux porteurs et, selon les cas, acceptations / rejets explicites par les porteurs ;
- le cas échéant, remise de son dispositif de création de signature au porteur ;
- publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- réception d'une demande de révocation ;

- validation / rejet d'une demande de révocation ;
- génération puis publication des LCR.

Sont également consignés ainsi dans le registre de cérémonies de l'AC, les événements suivants :

- création de bi-clés AC ;
- vérification des supports de parts de secrets ;
- délivrance de certificats :
  - génération de certificat d'un porteur (nouveau certificat, renouvellement) ;
  - génération de certificats d'administrateurs ;
- révocation ;
- fin de vie de l'IGC.

Sont aussi consignés dans le registre de cérémonies de l'AC les événements physiques dont la trace n'est pas fournie automatiquement par le système, comme :

- accès physiques aux plates-formes de cérémonie et cryptographiques de l'AC ;
- déménagement du matériel ;
- sortie pour maintenance ;
- changement de configuration du système ;
- modifications de droits d'accès ;
- changements de mots de passe ;
- destruction de secrets.

Chaque enregistrement d'un évènement dans un journal contient au minimum les champs suivants :

- type de l'évènement ;
- nom de l'exécutant ou référence du système déclenchant l'évènement ;
- date et heure de l'évènement ;
- résultat de l'évènement (échec ou réussite).

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

De plus, en fonction du type de l'évènement, chaque enregistrement contient également les champs suivants :

- destinataire de l'opération ;
- nom du demandeur de l'opération ou bien référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'évènement ;

- toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Les opérations de journalisation sont effectuées au cours du processus. En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement.

Tous les secrets des composantes de l'AC à savoir :

- secrets des HSM,
- secrets pour l'accès aux machines hébergeant l'AC,
- secrets d'administration de l'AC,
- sauvegarde des clés des HSM.

sont stockés dans des coffres-forts. Tout accès à un de ces éléments est tracé manuellement par un PV le même jour ouvré que l'événement.

4.4.2. Fréquence de traitement des journaux d'évènements

L'analyse du contenu des journaux d'événements est effectuée de manière régulière par l'AC. Le traitement pour les alertes est décrit dans la DPC.

4.4.3. Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant au moins le délai T_JOUR_SITE. Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous le délai T_JOUR_SITE (recouvrement possible entre la période de conservation sur site et la période d'archivage).

4.4.4. Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. La DPC et la documentation système précise les moyens de protection employés.

4.4.5. Procédure de sauvegarde des journaux d'évènements

Chaque entité opérant une composante de l'AC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC et en fonction des résultats de l'analyse de risque.

La DPC précise la procédure de sauvegarde des journaux d'évènements.

4.4.6. Système de collecte des journaux d'évènements

La collecte des journaux d'évènements est de la responsabilité de chaque composante de l'IGC pour les journaux qui la concerne.

4.4.7. Notification de l'enregistrement d'un évènement au responsable de l'évènement

Sans objet.

4.4.8. Evaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements sont contrôlés suivant la fréquence F_JOUR_ECH, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité au moins à une fréquence F_JOUR_ANA. Cette analyse doit donner lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) est effectué à une fréquence au moins égale à F_JOUR_RAP, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

4.5. Archivage des données

4.5.1. Types de données à archiver

L'archivage permet d'assurer :

- la pérennité des journaux constitués par les différents systèmes informatique des composantes l'AC,
- la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

L'archivage permet en outre d'assurer leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- la PC ;
- la DPC ;
- les accords contractuels avec d'autres PSCE (en particulier, l'AC de niveau supérieur) ;

- les dossiers de demande de certificat ;
- les certificats et LCR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les justificatifs d'identité des porteurs et leur entité de rattachement ;
- les journaux d'évènements des différentes entités de l'IGC.

4.5.2. Période de conservation des archives

- Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé pendant au moins T_ARCH_DOS. Le dossier de demande de certificat peut être présenté par l'AC lors d'une sollicitation par les autorités habilitées.

Ce dossier, complété par les mentions consignées par l'AE, permet de retrouver l'identité réelle des personnes physiques ayant demandé tout certificat, de porteur, d'administrateur ou de serveur OCSP émis par l'AC.

- Certificats et LCR émis par l'AC

Les certificats des porteurs et des administrateurs, ainsi que les LCR mises à disposition, sont archivés pendant au moins T_ARCH_CER_LCR après l'expiration de ces certificats et de ces LCRs.

- Journaux d'évènements

Les journaux d'évènements sont archivés pendant T_ARCH_EV après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage sont du même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements est assurée tout au long de leur cycle de vie.

- Autres journaux

Pour l'archivage des journaux, autres que les journaux d'évènements, les moyens mis en œuvre pour archiver ces journaux sont indiqués dans la DPC.

4.5.3. Protection des archives

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

- sont protégées en intégrité ;
- sont accessibles aux personnes autorisées ;
- peuvent être relues et exploitées.

Les moyens mis en œuvre pour archiver les pièces en toute sécurité sont indiqués dans la DPC.

4.5.4. Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes est au moins équivalent au niveau de protection des archives. La procédure est indiquée dans la DPC.

4.5.5. Exigences d'horodatage des données

Cf. § 4.4.4 pour la datation des journaux d'évènements.

Cf.§ 5.8 pour les exigences en matière de datation / horodatage.

4.5.6. Système de collecte des archives

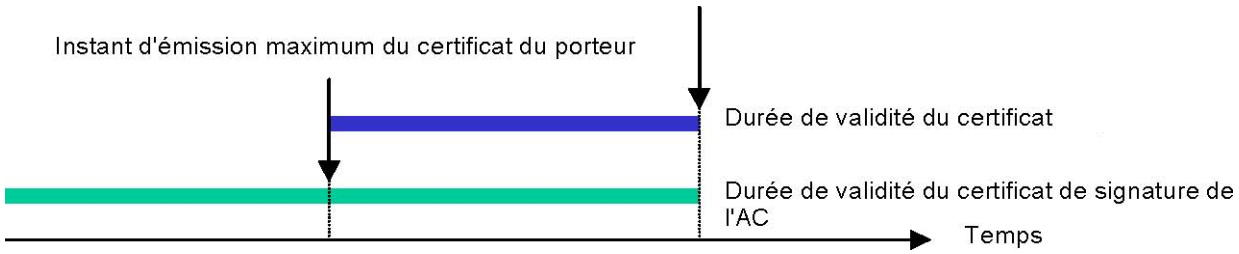
Le système de collecte des archives, qu'il soit interne ou externe, respecte les exigences de protection des archives concernées.

4.5.7. Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) sont récupérables dans un délai inférieur à T_REC_ARCH, sous la responsabilité de l'AC. Le processus de récupération fait l'objet d'une procédure interne de fonctionnement décrite dans la DPC de l'AC.

4.6. Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin de validité serait postérieure à la date d'expiration de la bi-clé de l'AC. Pour cela, la période de validité du certificat de l'AC est supérieure à celle des certificats qu'elle signe.



Au regard de la date de fin de validité de ce certificat, son renouvellement est 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, la nouvelle clé privée est utilisée pour signer:

- les nouveaux certificats des porteurs, des administrateurs et des serveurs OCSP;
- les LCRs relatives à ces nouveaux certificats.

L'ancienne bi-clé servira à signer :

- les LCRs relatives aux certificats émis sous l'ancienne clé.

Le certificat d'AC précédent reste utilisable pour valider les certificats émis sous cette clé ainsi que les LCRs et les réponses des serveurs OCSP et ce au moins jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

Une clé d'AC peut être renouvelée par anticipation si :

- la taille d'une clé de l'AC se révèle être insuffisante pour résister aux progrès réalisés pour « casser » les clés,
- l'algorithme de hachage utilisé pour générer les certificats ou des LCRs se révèle être d'une résistance insuffisante pour résister aux collisions.

4.7. Reprise suite à compromission et sinistre

4.7.1. Procédures de remontée et de traitement des incidents et des compromissions

L'AC 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 du personnel 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'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AA de l'AC du niveau supérieur.

Le cas de l'incident majeur est impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, est faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, …). L'AC prévient également directement et sans délai le point de contact identifié au sein de l'ANRT.

4.7.2. Procédures de reprise en cas de corruption des ressources informatiques

L'AC dispose d'un plan de continuité d'activité (PCA) permettant de répondre aux exigences de disponibilité des différentes fonctions découlant de la présente PC, des engagements de l'AC dans cette PC et des résultats de l'analyse de risque, notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

Ce plan est testé au minimum suivant la fréquence F_TEST_PLAN.

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

Dans le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante, le certificat correspondant est immédiatement supprimé et remplacé.

4.7.4. Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'AC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC. La DPC précise les capacités de continuité d'activité.

4.8. Fin de vie de l'AC

La fin de vie de l'AC concerne soit un transfert partiel d'activité à une autre entité, soit une cessation totale de l'activité.

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

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

4.8.1. Transfert d'activité

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC s'engage à :

1) mettre en place des procédures dont l'objectif est d'assurer un service constant, en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats).
2) assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC. A défaut, les utilisateurs de certificats refuseront les certificats émis par des AC dont les LCR en cours de validité ne seraient plus accessibles, même si le certificat du porteur est encore valide.
3) communiquer au point de contact identifié au sein de l'ANRT 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.
4) tenir informée l'ANRT de tout obstacle ou délai non prévu rencontrés dans le déroulement du processus.

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des porteurs ou des utilisateurs de certificats, l'AC devra en aviser aussitôt que nécessaire les utilisateurs de certificats et, au moins, sous le délai T_CESS.

4.8.2. Cessation totale d'activité

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité :

1) s'interdirait de transmettre à quiconque les clés privées lui ayant permis d'émettre des certificats ou des LCRs ;

2) détruirait dans le ou les modules cryptographiques les clés privées lui ayant permis d'émettre des certificats ou des LCRs,

3) détruirait toutes les copies de sauvegarde des clés privées lui ayant permis d'émettre des certificats ou des LCRs,

4) publierait cette information sur son site web, si cela est possible.

L'AC devrait en aviser aussitôt que nécessaire les utilisateurs de certificats et, au moins, sous le délai T_CESS.

5. MESURES DE SECURITE TECHNIQUES

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC s'engage à respecter. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC et des résultats d'une analyse de risque.

L'AC élabore la DPC en fonction d'une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre.

5.1. Génération et installation de bi-clés

5.1.1. Génération des bi-clés

5.1.1.1 Clés de l'AC

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

Les clés de signature de l'AC sont générées et mises en œuvre dans des modules cryptographiques conformes aux exigences du niveau de sécurité considéré.

La génération des clés de signature de l'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance, dans le cadre de "cérémonies de clés". Ces cérémonies se déroulent en suivant des scripts préalablement définis.

Selon le cas, l'initialisation du module cryptographique et/ou la génération des clés de signature de l'AC s'accompagne de la génération de parts de secrets. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de.

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

Les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de témoins dont au moins deux sont externes à l'AC et sont impartiaux. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

Les manipulations de codes PIN et de codes d'authentification sont effectuées dans un environnement protégé contre les risques de fuites d'information par observation visuelle[1].

[1] Les caméras de surveillance sont positionnées de manière à empêcher de telles fuites d'information.

5.1.1.2 Clés porteurs générées par l'AC

Les clés des porteurs n'étant pas générées par l'AC, cette section est sans objet.

5.1.1.3 Clés porteurs générées par le porteur

Les bi-clés des porteurs sont générées directement dans le dispositif de création de signature destiné aux porteurs conforme aux exigences du niveau de sécurité considéré.

5.1.2. Transmission de la clé publique à l'AC

La clé publique du porteur, une fois générée par le dispositif de création de signature, est protégée en intégrité et son origine est authentifiée lors de sa transmission vers une composante de l'AC.

5.1.3. Transmission de la clé publique de l'AC et des serveurs OCSP aux utilisateurs de certificats

Les clés publiques de l'AC sont diffusées au moyen de certificats signés par l'autorité du niveau supérieur. Le chemin de certification doit commencer par un certificat auto-signé de l'AC Racine BarideSign e-gov.

Un certificat racine auto-signé ne permet pas de garantir par lui-même que la clé publique correspondante appartient bien à l'AC considérée. Sa diffusion s'accompagne de la diffusion, via des sources de confiance, de l'empreinte numérique du certificat ainsi que d'une déclaration qu'il s'agit bien d'une clé publique de l'AC Racine BarideSign e-gov.

La clé publique de l'AC Racine BarideSign e-gov, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) est mise à disposition des utilisateurs sur un site de confiance (interne ou externe) selon les usages.

Les clés publiques des serveurs OCSP sont contenues dans les certificats de serveurs OCSP. Chaque réponse OCSP comporte le certificat du serveur OCSP qui a émis la réponse.

5.1.4. Tailles des clés

Les clés de l'AC, des porteurs respectent les exigences de caractéristiques (tailles, algorithmes, etc.) définis respectivement dans les paragraphes 9.5, 9.6 et 9.7.

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

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé (cf. chapitre 9.3).

5.1.6. Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats et de LCR.

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de signature électronique.

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

5.2.1. Standards et mesures de sécurité pour les modules cryptographiques

5.2.1.1 Modules cryptographiques de l'AC

L'AC dispose de modules cryptographiques qui assurent la protection des clés avec un niveau de sécurité jugé acceptable au regard des menaces pesant sur l'intégrité, la disponibilité et la confidentialité des bi-clés. Les générateurs d'aléas utilisés sont conformes à l'état de l'art.

5.2.1.2 Dispositifs de création de signature des porteurs

Les dispositifs de création de signature des porteurs respectent les exigences du niveau de sécurité considéré.

5.2.2. Contrôle des clés privées par plusieurs personnes

L'initialisation d'un boîtier cryptographique est contrôlée via un processus mettant en œuvre le partage des secrets où n exploitants doivent s'authentifier, avec n égal à 2. Le système cryptographique utilisé garantit que la perte ou le vol d'un élément ne permet pas de compromettre la confidentialité de la clé.

L'exportation dans un module cryptographique des clés privées est assuré par du personnel de confiance et via un outil mettant en œuvre le partage des secrets où m exploitants doivent s'authentifier, avec m égal à 2 au minimum. Le système cryptographique utilisé garantit que si tous les éléments sont perdus ou volés à l'exception d'un seul, il n'est pas possible de compromettre la confidentialité de la clé.

5.2.3. Séquestre des clés privées

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

5.2.4. Copie de secours des clés privées

Les clés privées d'AC peuvent faire l'objet de copies de secours, soit dans un module cryptographique, soit hors d'un module cryptographique, mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant offre un niveau de sécurité équivalent 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 sont à aucun moment en clair en dehors du module cryptographique.

La longueur des clés symétriques de chiffrement utilisées est au moins égale à 100 bits. Le mode opératoire utilisé permet de protéger la clé privée de l'AC en confidentialité mais aussi en intégrité.

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

5.2.5. Archivage des clés privées

Les clés privées de l'AC ne sont en aucun cas être archivées. Les clés privées des porteurs ne sont en aucun cas archivées, ni par l'AC ni par aucune des composantes de l'IGC.

5.2.6. Transfert des clés privées vers / depuis le module cryptographique

Tout transfert d'une clé privée de l'AC vers / depuis le module cryptographique à des fins de restauration ou de sauvegarde se fait sous forme chiffrée.

5.2.7. Stockage des clés privées dans un module cryptographique

Les clés privées de l'AC sont stockées dans des modules cryptographiques répondant au minimum aux exigences du niveau de sécurité considéré. Cependant, le stockage est aussi effectué en dehors d'un module cryptographique moyennant les exigences décrites ci-dessus.

5.2.8. Méthode d'activation des clés privées

5.2.8.1 Clés privées d'AC

L'activation des clés privées d'AC dans un module cryptographique est contrôlée via des données d'activation et fait intervenir initialement au moins deux personnes dans des rôles de confiance (par exemple, responsable sécurité et opérateur). La procédure d'activation est détaillée dans la DPC.

5.2.8.2 Clés privées des porteurs

L'activation de la clé privée d'un porteur dans le dispositif de création de signature est contrôlée via une donnée d'activation (PIN) et permet de répondre aux exigences du niveau de sécurité considéré.

5.2.9. Méthode de désactivation de la clé privée

5.2.9.1 Clés privées d'AC

La désactivation des clés privées d'AC dans un module cryptographique est automatique dès que l'environnement du module évolue : en particulier, arrêt du module, déconnexion du module, déconnexion par l'opérateur. Ces conditions de désactivation permettent de répondre aux exigences du niveau de sécurité considéré.

5.2.9.2 Clés privées des porteurs

La clé privée d'un porteur est automatiquement désactivée par la mise hors tension de son dispositif de création de signature. Les conditions de désactivation de la clé privée d'un porteur permettent de répondre aux exigences de sécurité considérées.

5.2.10. Méthode de destruction des clés privées

5.2.10.1 Clés privées d'AC

En fin de vie d'une clé privée de l'AC, normale ou anticipée, cette clé est détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

5.2.10.2 Clés privées des porteurs

En fin de vie de la clé privée d'un porteur, le porteur est invité à remettre son ancien support à un guichet postal dans le cas d'un renouvellement de certificat. Le support sera ensuite détruit par Poste Maroc. Pour les autres cas, le porteur s'engage à détruire physiquement son support cryptographique.

5.2.11. Niveau d'évaluation sécurité du module cryptographique

Les modules cryptographiques sont évalués au niveau correspondant à l'usage visé.

5.3. Autres aspects de la gestion des bi-clés

5.3.1. Archivage des clés publiques

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

5.3.2. Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des porteurs ont une durée de vie, au moins égale à T_PORT_MIN, et au maximum à T_PORT_MAX.

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

La durée de vie des clés d'AC et des certificats correspondants est égale à T_VAL_AC.

5.4. Données d'activation

5.4.1. Génération et installation des données d'activation

5.4.1.1 Génération des données d'activation correspondant à la clé privée de l'AC

La génération des données d'activation permettant d'initialiser un module cryptographique se fait lors de la phase d'initialisation et de personnalisation de ce module. Les données d'activation sont choisies et saisies par les responsables de ces données eux-mêmes. Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués et qui sont détaillés dans la DPC.

5.4.1.2 Génération et communication des données d'activation correspondant à la clé privée d'un porteur

Les données d'activation des dispositifs de création de signature des porteurs sont générées par l'AC. Elles sont communiquées au porteur au moyen d'un courrier envoyé en recommandé avec accusé réception.

5.4.2. Protection des données d'activation

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

Les porteurs de secrets de l'AC ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des données d'activation. Ils sont informés de cette obligation.

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

Les porteurs ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des codes d'activation (code PIN). Ils sont informés de cette obligation.

5.4.3. Autres aspects liés aux données d'activation

Si un porteur suspecte que son code d'activation a été espionné, il est tenu de changer ce code. Il dispose à cet effet d'un logiciel spécifique.

Si un porteur a bloqué son dispositif de création de signature, il peut le débloquer en se connectant à un serveur en ligne. Le porteur doit s'identifier au moyen de l'adresse courriel (email) qu'il a renseignée dans le formulaire d'enregistrement, puis s'authentifier au moyen d'au moins 4 ou 5 questions / réponses sur des informations propres au demandeur choisies au moment de l'enregistrement.

5.5. Mesures de sécurité des systèmes informatiques

5.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Le niveau minimal d'assurance de la sécurité offerte sur l'infrastructure informatique de chacune des composantes de l'AC est défini dans la DPC de l'AC. Il répond au moins aux objectifs de sécurité suivants :

- Identification et authentification forte des administrateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/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 des droits d'accès ;
- Protection du réseau contre les intrusions ;
- Fonctions d'audits ;
- Eventuellement, gestion des reprises sur erreur.

Des dispositifs de surveillance et des procédures d'audit des paramétrages du système sont mis en place.

5.5.2. Niveau d'évaluation sécurité des systèmes informatiques

Les mesures de sécurité relatives à l'IGC découlent d'une analyse de risques.
Le module cryptographique mis en œuvre a fait l'objet d'une évaluation selon la norme [FIPS 140-2] au niveau 3.

5.6. Mesures de sécurité liées au développement des systèmes

L'implémentation du système permettant de mettre en œuvre les composantes de l'AC est documentée et respecte une méthodologie de développement et de prise en compte des anomalies remontées. La configuration du système des composantes de l'AC ainsi que toute modification et toute mise à niveau sont documentées et contrôlées.

5.7. Mesures de sécurité réseau

Une analyse de risque relative à l'interconnexion a été menée afin d'établir les objectifs et les solutions de sécurité adaptées.

5.8. Horodatage / système de datation des évènements

L'usage d'une date et d'une heure UTC (Universal Time Coordinated) pour générer les certificats et d'une heure locale pour dater les évènements liés aux activités de l'AC est nécessaire. Une synchronisation fine par rapport au temps UTC n'est pas requise. Le système est toutefois en mesure de pouvoir ordonner les évènements avec une précision suffisante. Pour dater ces évènements, les différentes composantes de l'AC ont recours à une heure système.

6. PROFIL DES CERTIFICATS, DES LCR ET DES REPONSES OCSP

6.1. Profil des certificats

6.1.1. Profil d'un certificat de signature électronique

Le gabarit du certificat contient au moins les informations suivantes :

Champs de base : champs de «TBSCertificate»

Champ	Valeur	Détail valeur	Commentaire
Version	V3	2	Certificat x509 v3
Numéro de série	Nombre entier		Nombre entier pour indiquer le numéro de série du certificat
Algorithme de signature du certificat	La valeur doit correspondre à l'OID de l'algorithme défini pour l'attribut « signatureAlgorithm »	sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11	Identifiant de l'algorithme de signature
Emetteur	DN (Distinguished Name)	CN= Baridesign AC Classe 3 OU= Baridesign OU= 50413 O= Barid Al Maghrib C= MA	Identifiant de l'AC racine. Ce champ est conforme aux exigences des chapitres 3.1.1 du [RFC 3739] et 5.2.4 de [ETSI_CERT]
Période de validité	T0 et T0 + X ans	T0 = date d'émission du certificat X maximum = T_PORT_MAX	Date de début et de fin de validité
Sujet	DN (Distinguished Name)	Pour un certificat destiné à un professionnel: SN= numéro de série attribué par l'AC pour différencier des homonymes (mêmes nom et prénoms) CN= *NOM Prénom* userid= nom pouvant être utilisé en tant qu'identifiant unique pour s'authentifier à un système informatique (computer system login name). Cet attribut est décrit dans le RFC 1274 à la section 9.3.1.	Identifiant du porteur. Ce champ est conforme aux exigences des chapitres 3.1.1 du [RFC 3739] et 5.2.4 de [ETSI_CERT]

		Son OID est le suivant : { itu-t(0) data(9) pss(2342) ucl(19200300) pilot(100) pilotAttributeType(1) userid(1) }. Cet attribut est optionnel. OU= nom de l'unité d'organisation à laquelle le professionnel appartient OU= numéro d'immatriculation de l'organisation au Registre Central du Commerce tenu par l'Office Marocaine de la Propriété Industrielle et Commerciale (OMPIC) O= nom de l'organisation à laquelle le professionnel appartient. C= MA (Maroc) Pour un certificat destiné à un particulier: SN= numéro de série attribué par l'AC pour différencier des homonymes (mêmes nom et prénoms) CN= *NOM Prénom* userid= nom pouvant être utilisé en tant qu'identifiant unique pour s'authentifier à un système informatique (computer system login name). Cet attribut est décrit dans le RFC 1274 à la section 9.3.1. Son OID est le suivant : { itu-t(0) data(9) pss(2342) ucl(19200300) pilot(100) pilotAttributeType(1) userid(1) }. Cet attribut est optionnel. C= MA (Maroc)	
Algorithme et valeur de la clé publique de l'AC	RSA encryption OID=1.2.840.113549.1.1.1	Valeur sur 2048 bits	Identifiant de l'algorithme

Extensions

Champ	Valeur	Criticité	Commentaires
basic constraints	Booléen valeur : faux	Extension critique	Indique qu'il ne s'agit pas d'un certificat d'AC
keyUsage	Seul le bit 1 du champ « key usage » est positionné, les autres bits à "0". (c.f. section 9.4 de la PC Type).	Extension critique	Utilisation de la clé : - « non répudiation » selon le RFC 5280, ou - «*acceptation du contenu*» (contentCommitment) » selon la recommandation [X.509].
cRL DistributionPoints	Adresse LDAP et/ou HTTP	Extension non critique	Point de distribution de la LCR
authorityInfo Access	Pour chaque instance présente : accessMethod = id-ad-ocsp accessLocation = uniformResourceIdentifier	Extension non critique	Adresse de serveur OCSP
certification Policy	OID (identifiant d'objet) 1.2.504.1.1.1.1.1.1.X.Y X = 25 (Baridesign AC Classe 3 – signature sécurisée – pro), X = 26 (Baridesign AC Classe 3 – signature sécurisée – particulier), Y = niveau version majeure de document : 1 (version 1), 2 (version 2), ...	Extension non critique	Identifiant de la politique de certification
qCStatements	id-qcs 2 (c.f. [RFC 3739] et [ETSI_QC]) Contient l'identifiant d'objet id-etsi-qcs-QcCompliance ainsi que l'identifiant d'objet id-etsi-qcs-QcSSCD.	Extension non critique	Indique : a) que le certificat est délivré à titre de certificat électronique sécurisé, et b) qu'un dispositif de création de signature électronique, attesté par un certificat de conformité est mis en œuvre, selon la loi n° 53-05 relative à l'échange électronique de données juridiques.
authorityKey Identifier	AKI ID de la clé = XXXX	Extension non critique	Identifiant de la clé publique de l'AC à utiliser pour vérifier la signature du certificat

Pour plus d'informations, consulter le [RFC 5280], le [RFC 3739] et le document [ETSI_QC].

6.2. Profil des LCRs

Le gabarit des LCRs est le suivant :

Champs de base : champs de « TBSCertList »

Champ	Valeur	Commentaires
version	1	Version de la LCR utilisée (V2)
signature	sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11	OID de l'algorithme de signature
issuer	CN=Baridesign AC Classe 3 OU=Baridesign OU=50413 O=Barid Al Maghrib C=MA	DN de l'AC qui a signé la LCR
thisUpdate	Date et heure UTC	Date de génération de la LCR
nextUpdate	Date et heure UTC	Date au plus tard de la mise à jour de la LCR
RevokedCertificates	Liste de tuples: • UserCertificate (numéro de série) • RevocationDate (date de révovation)	Liste des numéros de série des certificats révoqués ainsi que leur date de révocation

Extensions

Champ	Valeur	Criticité	Commentaires
Numéro de LCR	Nombre entier	Extension non critique	Numéro croissant
authorityKeyIdentifier	AKI ID de la clé = XXXX	Extension non critique	Identifiant de la clé publique de l'AC à utiliser pour vérifier la signature de la LCR.

Pour plus d'informations, consulter le [RFC 5280].

6.3. Profil du protocole OCSP

Le profil est conforme au [RFC 2560] de l'IETF.

6.3.1. Profil d'une requête OCSP

Des précisions pour certains champs sont apportées ci-dessous :

Champ	Commentaires
optionalSignature	Si le champ **optionalSignature** est présent, son contenu est ignoré.
requestExtensions	Si le champ **requestExtensions** est présent, son contenu est ignoré.
hashAlgorithm	Les algorithmes acceptés pour **hashAlgorithm** sont SHA-1 et SHA-256.

Un maximum de 20 éléments « **Request** » est accepté.
Au-delà une erreur « malformedRequest » est retournée.

6.3.2. Profil d'une réponse OCSP

Des précisions pour certains champs sont apportées ci-dessous :

Champ	Commentaires
certs	Le champ **certs** contient le certificat du serveur OCSP.
ResponderID	Le choix **byName** du champ **ResponderID** est supporté. Ce champ contient le DN du certificat du serveur OCSP
nextUpdate	Le champ **nextUpdate** est supporté.
revocationReason	Le champ **revocationReason** n'est pas supporté.

Afin de contacter un serveur OCSP habilité à répondre pour le compte de l'AC, un utilisateur de certificats doit, en particulier :

- examiner l'extension **authorityInfoAccess** du certificat dont l'état de révocation est à vérifier, et utiliser successivement les URLs contenues dans chaque champ **accessLocation** associé à un champ **accessMethod** contenant l'identifiant d'objet id-ad-ocsp.
- adresser sa requête OCSP successivement à ces URLs, jusqu'à obtenir une réponse.

Lorsqu'une réponse est obtenue, un utilisateur de certificats doit s'assurer que la réponse OCSP provient d'un serveur OCSP effectivement habilité à répondre pour le compte de l'AC. Pour cela, un utilisateur de certificats doit, en particulier :

- examiner le champ **`certs`** de la réponse est s'assurer qu'il contient un certificat émis par l'AC qui a émis le certificat objet de la requête et qu'il est bien un certificat de serveur OCSP, c'est à dire qu'il contient une extension **`extendedkeyUsage`** avec un identifiant d'objet égal à id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9.),
- s'assurer que le DN contenu dans ce certificat est identique au champ **`byName`** de l'élément **`ResponderID`**,
- vérifier que ce certificat est effectivement signé par l'AC à l'aide de l'une des clés de l'AC valide à l'instant considéré, et que l'instant considéré est encadré par la période de validité de ce certificat,
- vérifier que ce certificat n'est pas révoqué en utilisant une CRL dont l'adresse est mentionnée dans l'extension CRLDistributionPoints contenue dans ce certificat,
- utiliser la clé contenue dans ce certificat pour vérifier la signature de la réponse OCSP.

S'agissant de la vérification de l'état révoqué/ non révoqué d'un certificat de signature électronique, la vérification de la validité de la réponse OCSP peut se faire à un instant considéré, c'est-à-dire soit pour le temps présent, soit pour une date passée. A cet effet, le champ **thisUpdate** de la réponse OCSP doit être utilisé.

Pour plus d'informations, consulter le [RFC 2560] et le [RFC 3279].

7. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits sont réalisés afin de s'assurer que l'ensemble de l'IGC de l'AC est bien conforme à la réglementation en vigueur et notamment aux engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

7.1. Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC a procédé à un contrôle de conformité de cette composante.

L'AC s'engage également à réaliser régulièrement un contrôle de conformité de l'ensemble de son IGC, suivant la fréquence F_CONFORM et conformément à la réglementation en vigueur.

7.2. Identité des auditeurs

Le contrôle d'une composante est réalisé par l'ANRT ou par des experts accrédités par elle, compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

7.3. Relations entre auditeur et entités évaluées

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

7.4. Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect de la réglementation en vigueur et notamment des engagements et pratiques définies dans la PC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

7.5. Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend, 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 au PSCE qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par le PSCE et doit respecter ses politiques de sécurité internes en concertation avec l'ANRT ;

- En cas de résultat "A confirmer", le PSCE remet à la composante un avis précisant sous quel délai les non-conformités sont réparées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, le PSCE confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

7.6. Communication des résultats

Les résultats des audits sont tenus à la disposition de l'ANRT et du PSCE.

8. AUTRES PROBLEMATIQUES METIERS ET LEGALES

8.1. Durée et fin anticipée de validité de la PC

8.1.1. Durée de validité

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

8.1.2. Fin anticipée de validité

La publication d'une nouvelle version de la présente PC peut entraîner, en fonction des évolutions apportées, la nécessité faire évoluer la PC correspondante. En fonction de la nature et de l'importance des évolutions apportées à la PC, le délai de mise en conformité sera arrêté par l'ANRT.

De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

8.2. Tarification et responsabilité financière

8.2.1. Tarifs

8.2.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

8.2.1.2 Tarifs pour accéder aux certificats

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

8.2.1.4 Tarifs pour d'autres services

8.2.1.5 Politique de remboursement

8.2.2. Responsabilité financière :

8.2.2.1 Couverture par les assurances

L'assureur garantit Barid Al Maghrib contre les conséquences pécuniaires de la responsabilité civile pouvant lui incomber en raison des dommages directs corporels, matériels et immatériels consécutifs causés aux tiers, à la suite d'une faute professionnelle commise par Barid Al Maghrib, ou les personnes dont il est civilement responsable, lorsqu'ils sont dans l'exercice des missions relevant des activités assurées.

Pour plus d'information, veuillez consulter la copie de la police d'assurance ci-jointe.

8.2.2.2 Autres ressources

8.2.2.3 Couverture et garantie concernant les entités utilisatrices

9. ANNEXES

9.1. Exigences de sécurité

9.1.1. Exigences sur les objectifs de sécurité des modules cryptographiques

Les modules cryptographiques, utilisés par l'IGC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR et des réponses OCSP), répondent aux exigences de sécurité suivantes :

- assurer la confidentialité et l'intégrité des clés privées de signature durant tout leur cycle 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 des certificats ou des réponses OCSP, qui ne révèlent pas les clés privées de signature et qui ne peuvent pas être falsifiés sans la connaissance de ces clés privées ;
- créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- lors des opérations de sauvegarde et de restauration des clés privées, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

Les modules cryptographiques détectent les tentatives d'altérations physiques et entrent dans un état sûr quand une tentative d'altération est détectée.

9.1.2. Exigences sur les objectifs de sécurité du dispositif de création de signature

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

- garantir que la bi-clé générée par le dispositif de création de signature répond aux exigences de robustesse cryptographique de la bi-clé générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une signature numérique qui ne peut être falsifiée sans la connaissance de la clé privée ;

- assurer la fonction d'authentification pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ;
- permettre de garantir l'authenticité de la clé publique lors de son export hors du dispositif.

9.2. Variables de temps

La définition de cette PC fait intervenir des exigences temporelles. Les tableaux suivants quantifient ces variables pour le niveau de sécurisé.

9.2.1. Variables de temps figurant dans la PC Type

Variable	Description	Valeur
F_CONFORM	Fréquence de contrôle de conformité de l'ensemble de l'IGC.	1 fois par an
F_JOUR_ANA	Fréquence d'analyse complète des journaux d'évènements.	1 fois par jour ouvré et dès la détection d'une anomalie
F_JOUR_ECH	Fréquence de contrôle des journaux d'évènements pour identification des tentatives en échec d'accès ou d'opération	1 fois par 24 h
F_JOUR_RAP	Fréquence de rapprochement des journaux d'évènements.	1 fois par semaine
F_PUB_LCR	Fréquence de publication des LCR	24 h
F_TEST_PLAN	Fréquence de test du plan de continuité.	1 fois par an
T_AC_DISP	Disponibilité des systèmes publiant les certificats d'AC.	24 h / 24 7 j /7
T_AC_INDISP	Durée maximale d'indisponibilité par interruption (panne ou maintenance) des systèmes publiant les certificats d'AC.	1 h
T_AC_MAX	Durée maximale totale d'indisponibilité par mois des systèmes publiant les certificats d'AC.	4 h
T_CESS	Délai minimum d'information en cas de cessation d'activité programmée	1 mois
T_DIFF_AC	Délai de diffusion préalable des certificats d'AC	24 h
T_ETAT_DISP	Disponibilité de la fonction d'information sur l'état des certificats	24 h / 24 7 j / 7

T_ETAT_INDIS	Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des certificats	1 h
T_ETAT_MAX	Durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats	4 h
T_INF_DISP	Disponibilité de la fonction de publication des informations (hors informations d'état des certificats).	Jours ouvrés
T_INF_INDISP	Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de publication	8 h (jours ouvrées)
T_INF_MAX	Durée maximale totale d'indisponibilité par mois de la fonction de publication	32 h (jours ouvrés)
T_JOUR_SITE	Délai de conservation des journaux d'évènements sur site et de mise en archive	1 mois
T_PORT_MAX	Durée de vie maximale d'une bi-clé et d'un certificat porteur	3 ans
T_PORT_MIN	Durée de vie minimale - hors révocation - d'une bi-clé et d'un certificat porteur	1 an
T_PUB_LCR	Délai maximum de publication d'une LCR suite à sa génération	30 min
T_REC_ARCH	Délai maximum de récupération des archives	2 jours ouvrés
T_REV_DISP	Disponibilité de la fonction de gestion des révocations	24 h / 24 7 j /7
T_REV_INDIS	Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations	30 min
T_REV_MAX	Durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations	2 h
T_REV_TRAIT	Délai maximum de traitement d'une demande de révocation	24 h

9.2.2. Variables de temps complémentaires à celles figurant dans la PC Type

Variable	Description	Valeur
T_VAL_AC	Durée de validité du certificat de l'AC	10 ans
T_REN_CERT	Durée avant la date d'expiration du certificat, qui déclenche une sollicitation de renouvellement du certificat d'un porteur	3 mois
T_ARCHIV	Durée d'archivage postérieure à l'expiration des certificats	5 ans
T_VAL_ADM	Durée de validité d'un certificat d'administrateur	3 ans
T_ARCH_DOS	Durée minimum d'archivage d'un dossier de demande de certificat de porteur	5 ans
T_ARCH_CER_LCR	Durée d'archivage des certificats et des LCRs après l'expiration de ces certificats et de ces LCRs.	5 ans
T_ARCH_EV	Durée d'archivage des journaux d'évènements après leur génération	5 ans

9.3. Sécurité applicable à l'application IGC

L'application IGC a besoin de disposer de certificats pour assurer la sécurité d'une part entre ses divers composants et d'autre part des applets signés.

La sécurité entre ses divers composants est assurée au moyen de certificats à usage interne gérés selon le mode « listes blanches », générés par l'application IGC elle-même.

La sécurité des applets signés est assurée selon le navigateur utilisé avec :

- des certificats de signature de codes Active X, et
- des certificats de signature de codes d'applets Java.

Ces certificats sont émis sous une Politique de Certification (PC) mise en œuvre par l'Autorité de Certification du fournisseur du logiciel, en la circonstance la société Bull. Le nom de l'AC est : BullSign.

L'identifiant d'objet de cette PC, dans sa version 1, est : 1.3.6.1.4.1.107.211.2.1.1.

La communication de la PC de cette AC est restreinte aux auditeurs.

9.4. Documents de référence

References	Document
[FIPS 140-2]	*Federal Information Processing Standards : Security Requirements for Cryptographic Modules*
[ETSI_CERT]	*ETSI -TS 102 280 -X.509 V3 Certificate Profile for Certificates issued to Natural Persons*
[ETSI_QC]	ETSI -TS 101 862 - Qualified certificate profile version 1.3.1 (2004-03)
[RFC 2560]	X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP
[RFC 3279]	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC 3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[RFC 3739]	IETF - Internet X.509 Public Key Infrastructure, Qualified Certificates profile
[RFC 5280]	*IETF -Internet X.509 Public Key Infrastructure, Certificate and CRL Profile*, RFC 5280

[X.509]	*ITU - Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, 6th edition.*

9.5. Algorithmes de signature et taille des clés de l'AC

Pour les clés publiques de l'AC, la taille initiale des clés et le choix initial des algorithmes est le suivant :

Algorithme	**Longueur de clé**
RSA	2048 bits
Hachage	SHA-256

Les algorithmes et la taille des clés pourront être modifiés, sans remettre en cause cette PC, au profit d'algorithmes offrant des résistances égales ou supérieures.

9.6. Algorithmes de signature et taille des clés des porteurs

Pour les clés publiques des porteurs, la taille initiale des clés et le choix initial des algorithmes est le suivant :

Algorithme	**Longueur de clé**
RSA	2048 bits

Les algorithmes et la taille des clés pourront être modifiés, sans remettre en cause cette PC, au profit d'algorithmes offrant des résistances égales ou supérieures.

9.7. Algorithmes de signature et taille des clés des serveurs OCSP

Pour les clés publiques des serveurs OCSP, la taille initiale des clés et le choix initial des algorithmes est le suivant :

Algorithme	**Longueur de clé**
RSA	2048 bits
Hachage	SHA-256

Les algorithmes et la taille des clés pourront être modifiés, sans remettre en cause cette PC, au profit d'algorithmes offrant des résistances égales ou supérieures.

FIN DU DOCUMENT