ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE
DIRECTION GENERALE DE LA
SECURITE DES SYSTEMES
D'INFORMATION

POLITIQUE DE CERTIFICATION DE REFERENCE

PC-TYPE D'UN PRESTATAIRE DE SERVICES DE CERTIFICATION ELECTRONIQUE (PSCE)

« en application des dispositions de l'article 7 du modèle de cahier des charges, devant accompagner la demande d'agrément d'un prestataire de services de certification électronique, annexé à l'arrêté n° 3-90-13 du 28 rabii I 1436 (20 janvier 2015) »

Version 1.3

MAI 2015

EVOLUTION DU DOCUMENT			
DATE	**VERSION**	**REDACTEUR**	**COMMENTAIRES**
22-03-2010	1.0	ANRT	
01-04-2011	1.1	ANRT	Mise à jour notamment de certaines références normatives
30-11-2012	1.2	ANRT	Précision en vue de l'harmonisation avec les exigences réglementaires
04-05-2015	1.3	DGSSI	Mise à jour suite au changement du cadre réglementaire

TABLE DES MATIERES

1. INTRODUCTION

1.1 Présentation générale

La Présente Politique de Certification Type (PC Type) est un recueil d'exigences qui portent 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).

Le présent document concerne le « service de signature électronique sécurisée» et constitue la politique de certification type (PC Type) destinée aux prestataires de services de certification électronique (PSCE) souhaitant fournir des certificats électroniques sécurisés à destination d'usagers à des fins de signature électronique sécurisée. Il a également pour objet de renseigner les promoteurs d'applications acceptant ces mêmes certificats.

Cette PC Type concerne les **familles de certificats électroniques sécurisés destinées à des services de signature électronique.** Si le PSCE gère d'autres familles de certificats, ces dernières et les Autorités de Certification correspondantes ne sont pas traitées par la présente PC Type.

L'objectif de ce document est de définir les engagements minimums qu'un PSCE doit respecter dans l'émission, la délivrance et la gestion de certificats de signature électronique sécurisée tout au long de leur cycle de vie.

La définition de la PC type fait intervenir des exigences temporelles requises pour le niveau de sécurité escompté. Le paragraphe 9.2 ci-après permet de quantifier ces valeurs.

Afin de faciliter l'utilisation et l'adoption de cette PC Type, sa structure est totalement conforme au [RFC3647].

1.2 Acronymes et Définitions

1.2.1 Acronymes

Les acronymes utilisés dans la présente PC Type sont les suivants :

AC	Autorité de Certification
DGSSI	Direction Générale de la Sécurité des Systèmes d'Information (autorité nationale d'agrément et de surveillance de la certification électronique)
AE	Autorité d'Enregistrement
AH	Autorité d'Horodatage
CEN	Comité Européen de Normalisation
DeltaLCR	Mécanisme par lequel la LCR se met à jour via des incrémentations (différence entre la précédente LCR)
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
DSA	Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de Gestion de Clés.
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Electronique
RSA	Rivest Shamir Adelman
SP	Service de Publication
IETF	Internet Engineering Task Force
FIPS	Federal Information Processing Standards Publications
NIST	National Institute of Standards and Technology
ITU	International Telecommunication Union
TS	Technical Specifications
AES	Advanced Encryption Standard
DES	Data Encryption Standard
UTC	Coordinated Universal Time

CBC-MAC	Cipher Block Chaining-Message Authentication Code
NTP	Network Time Protocol
TSP	TimeStamping Protocol
LDAP	Light Directory Access Protocol
CRL	Certificate Revocation List
ECDSA	Elliptic Curve Digital Signature Algorithm
RFC	Request For Comments
CMS	Cryptographic Message Syntax
XML	eXtensible Markup Language
ASN1	Abstract Syntax Notation One
XMLDSIG	eXtensible Markup Language Digital SIGnature
PKCS	Public-Key Cryptography Standards
SHA-1	Secure Hash Algorithm One
UH	Unité d'Horodatage

1.2.2 Terminologie

- **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 du certificat.
- **Autorité d'horodatage** - Autorité responsable de la gestion d'un service d'horodatage
- **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.
- **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.
- **Certificat électronique** - Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Dans le cadre de la présente PC Type, le terme "certificat électronique" désigne uniquement un certificat délivré à une personne physique et portant sur une bi-clé de signature, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

- **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.
- **Déclaration des pratiques de certification (DPC)** - Une DPC identifie les 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.
- **Dispositif de création de signature** électronique- Il s'agit du dispositif matériel et/ou logiciel utilisé par le porteur pour stocker et mettre en œuvre sa clé privée de signature.
- **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.
- **Politique de signature** - Ensemble de règles pour la création et la validation d'une signature électronique, vis-à-vis desquelles la signature peut être déterminée comme valide
- **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. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

1.3 Niveaux de sécurité

Les domaines d'utilisation de la signature électronique ainsi que les risques engendrés étant assez variables, il est nécessaire de définir des niveaux de sécurité adaptés à chacune des utilisations.

Ainsi, 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 tel qu'il a été modifié et complété par le décret n°2-13-881, 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 (ex : signature avec un certificat de type sécurisé) et un Dispositif de création de signature électronique.
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 (chargement à distance sur une carte à puce par exemple). 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	Au minimum, publication de la LCR. Recommandation de mise en œuvre de deltaLCR et d'un service en ligne (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 FIPS 140-2 (niveau 3). 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.
Génération des clés privées des porteurs (si elles sont générées par l'AC en dehors du dispositif de création de signature du porteur)	Génération dans un module cryptographique répondant aux exigences de la PC Type, certifié à un niveau équivalent à EAL4+ des critères communs.

Cette PC Type regroupe les exigences de qualification portant sur le niveau sécurisé.

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 Type 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 de données documents juridiques.

1.6 Identification du document

La présente PC Type peut être identifiée par son numéro d'identifiant d'objet (OID) unique. D'autres éléments, plus explicites, (nom, numéro de version, date de mise à jour) permettent également de l'identifier.

Le numéro d'OID de cette PC Type est indiqué à titre de gestion documentaire. Il ne doit pas être utilisé dans les certificats. Le PSCE doit attribuer à sa propre PC, reprenant les exigences de la présente PC Type, un OID qui sera porté dans ses certificats correspondants.

Le numéro d'OID du présent document est : [A définir par chaque PSCE]

1.7 Fonctionnalités minimales couvertes par une IGC

L'AC ou Autorité de Certification du PSCE 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 du futur porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. L'AE a également en charge, lorsque cela est nécessaire, la re-vérification des informations du porteur lors du renouvellement du certificat de celui-ci.
- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du porteur provenant du porteur.
- **Fonction de génération des éléments secrets du porteur** - Cette fonction génère les éléments secrets à destination du porteur, si l'AC a en charge une telle génération, et les prépare en vue de leur remise au porteur (par exemple, personnalisation de la carte à puce destinée au porteur, courrier sécurisé avec le code d'activation, etc.). De tels éléments secrets peuvent être, par exemple, directement la bi-clé du porteur, les codes (activation / déblocage) liés au dispositif de stockage de la clé privée du porteur ou encore des codes ou clés temporaires permettant au porteur de mener à distance le processus de génération / récupération de son certificat.
- **Fonction de remise au porteur** - Cette fonction remet au porteur au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif du porteur, clé privée 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. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides de ses porteurs.
- **Fonction de gestion des révocations** - Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
- **Fonction d'information sur l'état des certificats** : Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) et

éventuellement également selon un mode requête / réponse temps réel (OCSP).

NB : Les fonctions ci-dessus sont les fonctions minimales que doit obligatoirement mettre en œuvre une IGC gérant des certificats de signature électronique, à l'exception de la fonction de génération des éléments secrets du porteur qui est optionnelle et qui dépend des prestations effectivement offertes par l'AC.

1.8 Interactions avec l'IGC

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

- **Autorité de certification (AC)** - Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification, et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification.
- **Autorité d'Enregistrement (AE)** - A pour rôle la prise en compte et la vérification des informations du futur porteur et de son entité de rattachement le cas échéant et la constitution du dossier d'enregistrement correspondant
- **Porteur** - La 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.
- **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).
- **Utilisateur de certificat** - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du porteur du certificat.
- **Personne autorisée**- Il s'agit d'une personne autre que le porteur et le mandataire de certification et qui est autorisée par la politique de certification du PSCE ou par contrat établi avec lui à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.

L'organisation et l'ordonnancement des différentes fonctions de l'IGC les unes par rapport aux autres dépendent du modèle adopté par l'AC du PSCE. La présente PC Type n'impose aucun modèle particulier, dans la limite où le PSCE respecte les exigences qui y sont définies.

Cette organisation dépend notamment des prestations fournies par l'AC du PSCE : génération ou non de la bi-clé du porteur, fourniture ou non du dispositif de création

de signature au porteur et, si oui, fourniture avant ou après génération de la bi-clé du porteur, etc.

Le PSCE doit préciser dans sa PC les prestations effectivement fournies et son organisation fonctionnelle correspondante.

La Déclaration des Pratiques de Certification (DPC) du PSCE doit décrire l'organisation opérationnelle de son IGC et la répartition des rôles entre les différentes composantes en fonction de l'organisation fonctionnelle et de la définition des rôles décrites dans sa PC.

1.9 Responsabilités

1.9.1 De L'AC du PSCE

Quelle que soit l'organisation opérationnelle mise en œuvre par le PSCE, il reste in fine responsable vis-à-vis de toute partie externe à l'IGC (utilisateurs, autorités publiques, etc.) des prestations fournies et doit garantir le respect des engagements pris dans sa PC et sa DPC, relatifs à son activité de certification. Le cadre contractuel entre le PSCE et ses différentes composantes opérées par des éventuelles entités externes doit être clairement documenté.

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

- Être en relation par voie contractuelle / hiérarchique / réglementaire avec le porteur pour la gestion de ses certificats ;
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux porteurs, aux utilisateurs de certificats,… qui mettent en œuvre ses certificats ;
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur ;
- Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse ;
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions obligatoires de la présente PC Type, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats ;
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, et correspondant au minimum aux exigences de la présente PC Type, notamment en termes de fiabilité, de qualité et de sécurité ;

- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR et de réponses OCSP), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux porteurs et utilisateurs de certificats ;

- l'AC du PSCE doit mettre en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats :
    - Publication de sa politique de certification, couvrant l'ensemble des rubriques du [RFC3647] et conforme à la présente PC Type ;
    - Publication de la liste des certificats révoqués (porteurs et AC) ;
    - Publication des certificats de l'AC, en cours de validité ;
    - Publication, à destination des porteurs de certificats, les 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 doit être 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 du PSCE.
        - Pour les certificats d'AC, ils doivent être diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants sous délai VT::T_DIFF_AC.
- 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 doivent avoir une disponibilité de VT::T_INF_DISP avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de VT::T_INF_INDISP et une durée totale maximale d'indisponibilité par mois de VT::T_INF_MAX, ceci hors cas de force majeure.
    - Pour les certificats d'AC, les systèmes doivent avoir une disponibilité de VT::T_AC_DISP avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de VT::T_AC_INDISP et une durée totale maximale d'indisponibilité par mois de VT::T_AC_MAX, ceci hors cas de force majeure.
    - Pour les informations d'état des certificats (cf.paragraphe 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 doit être libre d'accès en lecture.

- Niveau sécurisé: L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) doit être 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 d'authentification du porteur ou, le cas échéant, du MC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

1.9.3 Du porteur des certificats

Dans le cadre de la présente PC Type, un porteur de certificats 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 doivent être 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 du PSCE 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

La présente PC Type traite des bi-clés et des certificats à destination des catégories de porteurs afin que ces derniers puissent signer électroniquement des données (documents ou messages) dans le cadre d'échanges. Une telle signature

électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

D'autres usages peuvent être autorisés par le PSCE dans sa PC, mais sous sa responsabilité et à condition que ces autres usages ne remettent pas en cause la conformité aux exigences de la présente PC Type. Notamment, l'utilisation de la clé privée du porteur et du certificat associé doit rester strictement limitée au service de signature électronique.

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. Le niveau d'assurance dépend, notamment, des moyens mis en œuvre par le PSCE tout au long du cycle de vie du certificat, ainsi que des mesures prises par le porteur afin de protéger sa clé privée.

Dans le cadre d'une application d'échanges dématérialisés de niveau sécurisé, les certificats de signature électronique objets de la présente PC Type 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.).

Certaines applications d'échanges dématérialisés peuvent nécessiter des certificats à des fins de validation ou de recette. De tels certificats doivent être identiques aux certificats "de production" fournis et gérés par l'AC du PSCE. Pour cela, une AC spécifique "de test" doit être mise en place et doit être identique à l'AC "de production".

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

Cette PC Type comporte également des exigences, lorsque nécessaire, concernant les bi-clés et certificats de l'AC (signature des certificats des porteurs, des LCR / LAR et, éventuellement, 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 du PSCE génère et signe différents types d'objets : certificats, LCR / LAR et, éventuellement, réponses OCSP. Pour signer ces objets, l'AC dispose d'au moins une bi-clé, mais il est recommandé qu'elle mette en œuvre des bi-clés séparées pour ces différents types.

Les certificats des clés publiques de ces bi-clés peuvent être générés par différentes AC. Les cas les plus courants sont les suivants :

- L'AC dispose d'une seule bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur (hiérarchie d'AC).
- L'AC dispose d'une seule bi-clé et le certificat correspondant est un certificat racine (certificat autosigné non rattaché à une AC de niveau supérieur).
- L'AC dispose de bi-clés séparées, les certificats correspondants à ces bi-clés sont rattachés à une AC de niveau supérieur (hiérarchie d'AC).

La présente PC Type recommande la mise en œuvre de ce dernier cas, qui permet notamment à l'AC de niveau supérieur de générer et diffuser de manière plus simple des LAR en cas de révocations des certificats d'AC de niveau inférieur.

Quelle que soit l'approche retenue par l'AC du PSCE (bi-clés séparées ou non), les bi-clés et certificats de l'AC pour la signature de certificats, de LCR / LAR et/ou de réponses OCSP ne doivent être utilisés qu'à cette fin.

1.11 Gestion de la PC

1.11.1 Entité gérant la PC

Le PSCE est responsable de la validation et de la gestion de la PC répondant aux exigences de la présente PC Type.

1.11.2 Point de contact

A préciser dans la PC du PSCE.

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

A préciser dans la PC du PSCE.

1.11.4 Procédures d'approbation de la conformité de la DPC

A préciser dans la PC du PSCE.

2. IDENTIFICATION ET AUTHENTIFICATION

2.1 Nommage

2.1.1 Types de noms

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

2.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les porteurs de certificats doivent être explicites. Lorsqu'un pseudonyme est utilisé, il doit être explicitement identifié comme tel dans le DN.

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

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 doit permettre 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 peut être attribué à un autre porteur. Le PSCE précisera dans sa PC et sa DPC comment il répond à cette exigence.

A noter que l'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC, mais que ce numéro est propre au certificat et non pas au porteur et ne permet donc pas d'assurer une continuité de l'identification dans les certificats successifs d'un porteur donné.

2.1.4 Identification, authentification et rôle des marques déposées

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

L'enregistrement d'un porteur peut se faire soit directement auprès de l'AE, soit via un mandataire de certification de l'entité. 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

Lorsque c'est le porteur qui génère sa bi-clé, il doit alors fournir à l'AC, via le MC le cas échéant, une preuve de possession de sa clé privée correspondant à la clé publique contenue dans la demande de certificat.

2.2.2 Enregistrement d'un porteur

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

- Une demande de certificat écrite signée, et datée de moins de 3 mois, par le futur porteur ;
- Un document officiel d'identité en cours de validité du futur porteur comportant une photographie d'identité notamment la carte d'identité nationale, le passeport, le permis de conduire ou la carte de séjour, qui est présenté à l'AE qui en conserve une copie.

Note - Le porteur doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

L'authentification du porteur par l'AE est réalisée lors d'un face-à-face physique ou par une méthode apportant un degré d'assurance équivalent. Notamment, une demande d'enregistrement doit pouvoir se faire sous forme dématérialisée à condition que la demande signée par le porteur le soit à l'aide d'un outil et d'un certificat de signature qualifiés à un niveau sécurisé et que la signature soit valide au moment de l'enregistrement.

2.2.3 Informations non vérifiées du porteur

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

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

L'AC gère et documente les demandes d'accords et les accords de reconnaissance avec des AC extérieures au domaine de sécurité auquel l'AC appartient.

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

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

Ce chapitre concerne aussi bien le cas où la bi-clé est générée par le porteur que le cas où elle est générée par l'AC.

2.3.1 Identification et validation pour un renouvellement courant

Lors du premier renouvellement, la vérification de l'identité du porteur est optionnelle. Elle est laissée à l'appréciation du PSCE qui engage sa responsabilité quant à la validité des informations contenues dans le certificat renouvelé.

Lors du premier renouvellement, l'AC doit au minimum s'assurer que les informations du dossier d'enregistrement initial sont toujours valides. Lors du renouvellement suivant, l'AE, saisit de la demande, identifiera le porteur selon la même procédure que pour l'enregistrement initial ou suivant une procédure offrant un niveau de garantie équivalent. Une demande de renouvellement de clé peut être signée à l'aide d'un outil et d'un certificat de signature sécurisée.

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 doit être identique à la procédure d'enregistrement initial ou doit être une procédure offrant un niveau de garantie équivalent.

2.3.3 Identification et validation d'une demande de révocation

- Si la demande de révocation est faite via un service téléphonique ou via un service en ligne (serveur web), le demandeur doit être formellement authentifié : vérification de l'identité du demandeur et de son autorité par rapport au certificat à révoquer. Par exemple :
    - Série d'au moins 4 ou 5 questions / réponses sur des informations propres au demandeur, dont au moins une réponse ne peut réellement être connue que du demandeur (question d'identification personnelle liée au demandeur et/ou dont la réponse a été choisie au moment de l'enregistrement ou lors du retrait du certificat utilisation d'un identifiant / mot de passe envoyé préalablement au demandeur de façon sécurisée) ;
    - Authentification en ligne à l'aide d'un certificat et d'un outil sécurisés ;
    - Signature électronique de la demande à l'aide d'un certificat et d'un outil sécurisés ;

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 le représentant d'un incapable majeur ou d'un mineur ou par un représentant légal de l'entité ou un MC dûment mandaté pour cette entité, avec dans tous les cas consentement préalable du futur porteur.

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

Les informations suivantes doivent au moins faire partie de la demande de certificat:

- le nom du porteur à utiliser dans le certificat (nom réel ou pseudonyme) ;
- les données personnelles d'identification du porteur ;
- les données d'identification de l'entité du porteur le cas échéant.

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 "personne physique" sont vérifiées conformément aux exigences décrites dans les chapitres précédents.

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

- Valider l'identité du futur porteur ;
- Vérifier la cohérence des justificatifs présentés ;
- S'assurer que le futur porteur 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 et, le cas échéant, de la bi-clé vers la fonction adéquate de l'IGC. L'AE conserve ensuite une trace des justificatifs d'identité présentés :

- Si le dossier est au format papier, sous la forme d'une photocopie signée à la fois par le futur porteur et par le PSCE, ou le MC le cas échéant, les signatures étant précédées de la mention "copie certifiée conforme à l'original" ;
- Si le dossier est au format électronique, les différents justificatifs sous une forme électronique ayant valeur légale.

3.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le porteur, ou le MC le cas échéant, en justifiant le rejet.

3.2.3 Durée d'établissement du certificat

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. A préciser par le PSCE dans sa PC, en visant une durée d'établissement la plus courte possible.

3.3 Délivrance du certificat

3.3.1 Actions de l'AC concernant la délivrance du 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 destinés au porteur : au minimum, le certificat, et, selon les cas, la bi-clé du porteur, son dispositif de création de signature, les codes d'activation, etc.

Si l'AC génère la bi-clé du porteur, le processus de génération du certificat doit être lié de manière sécurisée au processus de génération de la bi-clé : l'ordonnancement des opérations doit être assuré ainsi que, le cas échéant en fonction de l'architecture de l'IGC, l'intégrité et l'authentification des échanges entres les composantes.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres ci-dessous.

3.3.2 Notification par l'AC de la délivrance du certificat au porteur

- La remise du certificat doit se faire en mains propres (face-à-face) au minimum dans le cas où l'authentification du porteur se fait via un face-à-face et que ce face-à-face n'a pas eu lieu au moment de l'enregistrement. Si la remise du certificat ne se fait pas en mains propres, le PSCE précisera dans sa PC comment il s'assure que le certificat est bien remis au bon porteur ou à une personne dûment autorisée (par exemple, envoi sur carte à puce ou sur disquette en courrier recommandé, téléchargement grâce à un code d'accès préalablement fourni au porteur, ...).
- De plus, si l'AC n'a pas généré elle-même la bi-clé du porteur, elle doit s'assurer que le certificat est bien associé, dans l'environnement du porteur, à la clé privée correspondante (par exemple, mise à disposition d'un outil en ligne permettant de réaliser une authentification de test). Il s'agit notamment du cas où le certificat est associé à une clé privée stockée sur une carte à puce non fournie par l'AC : le certificat doit alors être téléchargé sur la bonne carte à puce.

3.4 Acceptation du certificat

3.4.1 Démarche d'acceptation du certificat

- L'AC doit obtenir confirmation de l'acceptation explicite du certificat par le porteur sous la forme d'un accord signé (papier ou électronique). L'AC doit garder une trace de l'acception du certificat par le porteur.

3.4.2 Publication du certificat

Si le certificat fait l'objet d'une publication par l'AC, les conditions d'une telle publication doivent être précisées par le PSCE dans sa PC. Notamment, cette publication ne peut avoir lieu sans l'accord du porteur du certificat et qu'après acceptation du contenu du certificat par celui-ci.

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

L'AC informe l'AE de la délivrance du certificat, qui se charge d'en informer le MC le cas échéant.

3.5 Usages de la bi-clé et du certificat

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

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de signature. 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 du porteur et du certificat associé doit par ailleurs être indiqué dans le certificat lui-même, via les extensions concernant les Key usage. Cet usage doit également être clairement explicité dans la PC du PSCE, ainsi que dans les conditions générales d'utilisation.

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

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

3.6 Renouvellement d'un certificat

Dans la présente PC, le renouvellement d'un certificat implique la génération de nouvelles bi-clés et donc la génération d'un nouveau certificat correspondant.

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

Note - Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat au porteur liée à la génération d'une nouvelle bi-clé.

3.7.1 Causes possibles de changement d'une bi-clé

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

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

Note - Dans la suite du présent chapitre, le terme utilisé est "fourniture d'un nouveau certificat". Ce terme recouvre également, dans le cas où elle est générée par l'AC, la fourniture de la nouvelle bi-clé du porteur.

3.7.2 Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat du porteur peut-être automatique ou bien à l'initiative du porteur.

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 Type.

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 ou MC par exemple) 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 (y compris un certificat d'AC pour la génération de certificats, de LCR et/ou de réponses OCSP) :

- 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'entité ;
- L'AC émettrice du certificat ou l'une de ses composantes (AE).

Note : Le porteur doit être 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'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

3.9.3 Procédure de traitement d'une demande de révocation

3.9.3.1 Révocation d'un certificat de porteur

Le PSCE doit préciser dans sa PC comment la fonction de gestion des révocations est organisée et quels sont les points d'accès à cette fonction pour les demandeurs de révocation.

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

- L'identité du porteur du certificat utilisée dans le certificat (nom, prénom, ...) ;
- Le nom du demandeur de la révocation ;
- Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer ;
- Éventuellement, la cause de révocation.

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

Le demandeur de la révocation doit être informé du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si le porteur du certificat n'est pas le demandeur, il doit également être informé de la révocation effective de son 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.

NB : Il est recommandé de ne pas publier les causes de révocation définitive des certificats. Dans le cas où l'AC publie ces causes de révocation, elle doit appliquer une procédure garantissant leur confidentialité et s'assurer de l'accord du porteur avant de publier ces informations.

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

Le PSCE précisera dans sa DPC les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

En cas de révocation d'un des certificats de la chaîne de certification, le PSCE doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés que leurs certificats ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE et aux MC. Ces derniers devront informer les porteurs de certificats en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Afin de faciliter la révocation du certificat de l'AC, il est recommandé que le certificat associé à la clé de l'AC signant les certificats porteurs soit signé par une autre AC.

Le point de contact identifié au sein de la DGSSI doit être immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification. La DGSSI se réserve le droit de diffuser par tout moyen l'information auprès des promoteurs d'applications et auprès des usagers.

3.9.4 Délai accordé au porteur pour formuler la demande de révocation

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

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

3.9.5.1 Révocation d'un certificat de porteur

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

Toute demande de révocation d'un certificat porteur doit être traitée dans un délai inférieur à VT::T_REV_TRAIT, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

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 doit être effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR et/ou de réponses OCSP) doit être effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

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

L'utilisateur d'un certificat de porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée (LCR, deltaLCR, OCSP…) est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.

3.9.7 Fréquence d'établissement des LCR

La fréquence de publication des LCR doit être conforme à VT::F_PUB_LCR.

Il est recommandé de mettre en œuvre le mécanisme des deltaLCR et de publier une deltaLCR conformément à VT::F_PUB_dLCR. Ce mécanisme permet en effet de respecter l'exigence de délai de traitement d'une demande de révocation sans avoir

à modifier la fréquence de publication des LCR. Les modalités liées à la mise en œuvre des deltaLCR devront être précisées par le PSCE dans sa PC.

3.9.8 Délai maximum de publication d'une LCR

Une LCR doit être publiée dans un délai maximum conforme à VT::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

D'autres formes de publications complémentaires (serveur OCSP par exemple) peuvent être mises en place à condition qu'elles respectent les exigences d'intégrité, de disponibilité et de délai de publication décrites dans cette PC Type. La mise en œuvre d'un service OCSP est recommandée.

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

Ces autres moyens d'information sur les révocations peuvent être mis en place à condition qu'ils respectent les exigences d'intégrité, de disponibilité et de délai de publication décrite dans la présente PC Type. A préciser par le PSCE dans sa PC.

3.9.12 Exigences spécifiques en cas de compromission de la 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 les certificats d'AC, la révocation suite à une compromission de la clé privée doit faire 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 Type.

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 doit fournir aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC Racine), c'est à dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR et l'état du certificat de l'AC Racine.
La fonction d'information sur l'état des certificats doit au moins mettre à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR / LAR. Ces LCR / LAR doivent être des LCR au format V2, publiées par exemple dans un annuaire accessible en protocole LDAP V3.

3.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats doit être disponible conformément à VT::T_ETAT_DISP.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme à VT::T_ETAT_INDIS et une durée maximale totale d'indisponibilité par mois conforme à VT::T_ETAT_MAX.

3.10.3 Dispositifs optionnels

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

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 doit être révoqué.

3.12 Séquestre de clé et recouvrement

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

Les clés privées d'AC ne doivent pas non plus être séquestrées.

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

RAPPEL - Le PSCE doit mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Il élabore sa DPC en fonction de cette analyse. Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles doivent être complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC et des résultats de l'analyse de risque.

4.1 Mesures de sécurité physique

4.1.1 Situation géographique et construction des sites

La présente PC Type ne formule pas d'exigence spécifique concernant la localisation géographique.

La construction des sites doit respecter les règlements et normes en vigueur ainsi qu'éventuellement, en fonction des résultats de l'analyse de risque, des exigences spécifiques face à des risques de type tremblement de terre ou explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques,...).

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 doivent être contrôlés.

Pour les fonctions de génération des certificats, de génération des éléments secrets du porteur et de gestion des révocations, l'accès doit être strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être 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 doit être limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, les composantes concernées de l'IGC doivent définir un périmètre de sécurité physique où sont installées ces machines. La mise en œuvre de ce périmètre doit permettre de respecter la séparation des rôles de confiance telle que prévue dans la PC du PSCE, en conformité avec la présente PC Type. Notamment, il est recommandé que tout local utilisé en commun avec d'autres fonctions que les fonctions rendues par la composante concernée soit en dehors de ce périmètre de sécurité.

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 doivent permettre de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.

Elles doivent également permettre de respecter les exigences de la présente PC Type, ainsi que les engagements pris par le PSCE dans sa PC, 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 doivent permettre de respecter les exigences de la présente PC Type, ainsi que les engagements pris par le PSCE dans sa PC, 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 doivent permettre de respecter les exigences de la présente PC Type, ainsi que les engagements pris par le PSCE dans sa PC, 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 doivent être identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations doivent être traités et conservés conformément à ces besoins de sécurité.

4.1.7 Mise hors service des supports

En fin de vie, les supports devront être, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

Les procédures et moyens de destruction et de réinitialisation doivent être conformes à ce niveau de confidentialité

4.1.8 Sauvegardes hors site

En complément de sauvegardes sur sites, il est recommandé que les composantes de l'IGC mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes doivent être 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 Type et aux engagements du PSCE dans sa PC 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 doivent respecter les exigences de la présente PC Type 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, doivent obligatoirement mettre 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

Chaque composante de l'IGC doit distinguer au moins les cinq rôles fonctionnels de confiance suivants :

- **Responsable de sécurité** - Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'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.

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

amenée 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.

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, il est demandé de répartir les fonctions sensibles sur plusieurs personnes. La présente PC Type définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC.

La DPC du PSCE devra préciser, 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'IGC doit faire vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

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

Ces contrôles doivent être décrits dans la DPC du PSCE et doivent être conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'IGC doit être notifiée par écrit.

4.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la DPC du PSCE et être conformes à la politique de sécurité de la composante concernée.

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

Chaque entité opérant une composante de l'IGC doit s'assurer 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'IGC.

L'AC doit informer toute personne intervenant dans des rôles de confiance de l'IGC :

- De ses responsabilités relatives aux services de l'IGC ;
- 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'IGC doit mettre 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 doivent être menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

4.3.3 Exigences en matière de formation initiale

Le personnel doit être 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 concerné doit recevoir une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

4.3.5 Fréquence et séquence de rotation entre différentes attributions

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. A préciser par le PSCE dans sa DPC.

4.3.6 Sanctions en cas d'actions non autorisées

A préciser par le PSCE dans sa DPC.

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 doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

4.3.8 Documentation fournie au personnel

Chaque personnel doit disposer au minimum 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.

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, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

4.4.1 Type d'évènements à enregistrer

Chaque entité opérant une composante de l'IGC doit au minimum journaliser 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'IGC :

- 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 ;
- Evènements 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 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 ;
- Evènements 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 et, éventuellement, deltaLCR ;
- Le cas échéant, requêtes / réponses OCSP.

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

- 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 doit figurer explicitement dans l'un des champs du journal d'évènements.

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

4.4.2 Fréquence de traitement des journaux d'évènements

Cf. chapitre ci dessous.

4.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements doivent être conservés sur site pendant au moins le délai VT::T_JOUR_SITE. Ils doivent être archivés le plus rapidement possible après leur génération et au plus tard sous le délai VT::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 doit être 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 doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements doivent être 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. Elle peut entraîner un besoin de protection en confidentialité.

4.4.5 Procédure de sauvegarde des journaux d'évènements

Chaque entité opérant une composante de l'IGC doit mettre 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 Type et en fonction des résultats de l'analyse de risque du PSCE.

4.4.6 Système de collecte des journaux d'évènements

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

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

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

4.4.8 Evaluation des vulnérabilités

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

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

Les journaux doivent être analysés dans leur totalité au moins à une fréquence VT::F_JOUR_ANA. Cette analyse donnera lieu à un résumé dans lequel les

éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire 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.) doit être effectué à une fréquence au moins égale à VT::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

Des dispositions en matière d'archivage doivent également être prises par l'AC. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- Les PC ;
- Les DPC ;
- Les accords contractuels avec d'autres PSCE ;
- Les certificats et LCR tels qu'émis ou publiés ;
- Les récépissés ou notifications (à titre informatif) ;
- Les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement ;
- Les journaux d'évènements des différentes entités de l'IGC ;
- Dossiers de demande de certificat.

4.5.2 Période de conservation des archives

- Dossiers de demande de certificat

Tout dossier de demande de certificat accepté doit être archivé pendant au moins cinq ans, comptés au maximum à partir de l'acceptation du certificat par son porteur.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées.

Ce dossier, complété par les mentions consignées par l'AE ou le MC, doit permettre de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

- Certificats et LCR émis par l'AC

Les certificats de clés de porteurs et d'AC, ainsi que les LCR / LAR produites, doivent être archivés pendant au moins cinq ans après l'expiration de ces certificats.

- Journaux d'évènements

Les journaux d'évènements seront archivés pendant cinq ans après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage devront offrir le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements devra être assurée tout au long de leur cycle de vie.

- Autres journaux

Pour l'archivage des journaux, autres que les journaux d'évènements, aucune exigence n'est stipulée. Le PSCE précisera dans sa DPC les moyens mis en œuvre pour archiver ces journaux.

4.5.3 Protection des archives

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

- Etre protégées en intégrité ;
- Etre accessibles aux personnes autorisées ;
- Pouvoir être relues et exploitées.

Le PSCE précisera dans sa DPC les moyens mis en œuvre pour archiver les pièces en toute sécurité.

4.5.4 Procédure de sauvegarde des archives

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. A préciser par le PSCE dans ses PC et DPC. Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

4.5.5 Exigences d'horodatage des données

Voir ci-dessus.

4.5.6 Système de collecte des archives

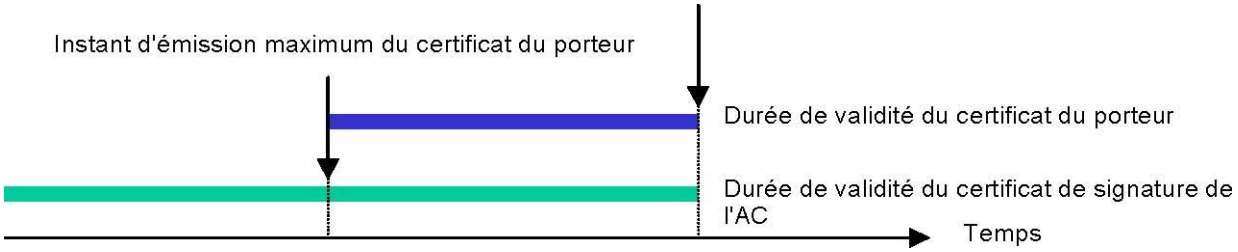
La présente PC Type ne formule pas d'exigence spécifique sur le sujet, si ce n'est que le système de collecte des archives, qu'il soit interne ou externe, doit respecter les exigences de protection des archives concernées.

4.5.7 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai inférieur à VT::T_REC_ARCH, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

4.6 Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité de ce certificat de l'AC doit être supérieure à celle des certificats qu'elle signe.



Au regard de la date de fin de validité de ce certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée doit être utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce au moins jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

4.7 Reprise suite à compromission et sinistre

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

Chaque entité opérant une composante de l'IGC doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur doit être impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé …). L'AC doit également prévenir directement et sans délai le point de contact identifié au sein de la DGSSI.

4.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Chaque composante de l'IGC doit disposer d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC Type, des engagements du PSCE dans sa propre PC et des résultats de l'analyse de risque de l'IGC, notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

Ce plan doit être testé au minimum suivant la fréquence VT::F_TEST_PLAN.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante doit être traité dans le plan de continuité de la composante.

Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué.

4.7.4 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC doivent disposer des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC Type et de la PC du PSCE.

4.8 Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC 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 la 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.

Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, le PSCE doit entre autres obligations :

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 Type. A défaut, les applications de l'Administration refuseront les certificats émis par des AC dont les LCR en cours de validité ne seraient plus accessibles, même si le certificat

du porteur est encore valide.

Des précisions quant aux engagements suivants doivent ainsi être annoncées par le PSCE dans sa PC :

1) Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des porteurs ou des utilisateurs de certificats, le PSCE doit les en aviser aussitôt que nécessaire et, au moins, sous le délai VT::T_CESS.

2) Le PSCE doit communiquer au point de contact identifié au sein de la DGSSI les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Il y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. Le PSCE devra communiquer à la DGSSI selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. Le PSCE mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Il présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les porteurs et les utilisateurs de certificats.

3) Le PSCE doit tenir informée la DGSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) ci-dessous soient à exécuter par le PSCE, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, le PSCE 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, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans sa PC.

Lors de l'arrêt du service, l'AC doit :

1) S'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;

2) Prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;

3) Révoquer son certificat ;

4) Révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;

5) Informer (par exemple par récépissé) tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

5. MESURES DE SECURITE TECHNIQUES

RAPPEL - L'AC doit mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Le PSCE élabore sa DPC en fonction de cette analyse. Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles doivent être complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC et des résultats de l'analyse de risque.

5.1 Génération et installation de bi-clés

5.1.1 Génération des bi-clés

5.1.1.1 Clés d'AC

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

Les clés de signature d'AC doivent être générées et mises en œuvre dans un module cryptographique conforme aux exigences du niveau de sécurité considéré.

La génération des clés de signature d'AC doit être effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance, dans le cadre de "cérémonies de clés". Ces cérémonies doivent se dérouler suivant des scripts préalablement définis par la maîtrise d'œuvre de l'IGC.

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

Par exemple, ces parts de secrets peuvent être des parties de la (ou des) clé(s) privée(s) d'AC, décomposée(s) suivant un schéma à seuil de Shamir (n parties parmi m sont nécessaires et suffisantes pour reconstituer la clé privée), ou encore, il peut s'agir de données permettant de déclencher le chargement sécurisé, dans un nouveau module cryptographique, de la (ou des) clé(s) privée(s) d'AC sauvegardée(s) lors de la cérémonie de clés.

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

- Les cérémonies de clés doivent se dérouler sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs 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. Il est recommandé qu'il y ait parmi les témoins un officier public (huissier ou notaire).

- Toute manipulation de données secrètes en clair (clés privées d'AC, clés privées des porteurs, parts de secrets d'IGC) doit se faire dans un environnement protégé contre les rayonnements parasites compromettant : matériels protégés, cage de Faraday, locaux limitant les risques de fuites d'information par observation visuelle ou rayonnements électromagnétiques, etc.

5.1.1.2 Clés porteurs générées par l'AC

Les exigences de ce paragraphe ne s'appliquent que si la bi-clé du porteur est générée par l'AC. La génération des clés des porteurs doit être effectuée dans un environnement sécurisé.

Les bi-clés des porteurs doivent être générées :

- Soit directement dans le dispositif de création de signature destiné au porteur conforme aux exigences du niveau de sécurité considéré ;
- Soit dans un module cryptographique conforme aux exigences du niveau de sécurité considéré, puis transférées de manière sécurisée dans le dispositif de création de signature destiné au porteur sans que l'AC n'en garde aucune copie.

5.1.1.3 Clés porteurs générées par le porteur

Dans le cas où le porteur génère sa bi-clé, cette génération doit être effectuée dans un dispositif répondant aux exigences du niveau de sécurité considéré. L'AC doit s'en assurer auprès du porteur, au minimum au travers d'un engagement contractuel clair et explicite du porteur vis-à-vis du PSCE.

5.1.1.4 Transmission de la clé privée à son propriétaire

Si l'AC génère la bi-clé du porteur, la clé privée doit être transmise au porteur de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. Cette transmission doit se faire de préférence directement dans le dispositif de création de signature destiné au porteur, ou suivant un moyen équivalent.

5.1.2 Transmission de la clé publique à l'AC

En cas de transmission de la clé publique du porteur vers une composante de l'AC (cas où la bi-clé est générée par le porteur), la clé devra être protégée en intégrité et son origine devra en être authentifiée.

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

Les clés publiques de vérification de signature de l'AC doivent être diffusées auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine.

Une clé publique d'AC peut être diffusée dans un certificat qui est soit un certificat racine autosigné, soit un certificat rattaché à une hiérarchie d'AC jusqu'à une AC racine.

Un certificat racine autosigné ne permet pas de garantir par lui-même que la clé publique correspondante appartient bien à l'AC considérée. Sa diffusion doit s'accompagner de la diffusion, via des sources de confiance, de l'empreinte numérique du certificat, et éventuellement de la clé publique, ainsi que d'une déclaration qu'il s'agit bien d'une clé publique de l'AC.

La clé publique de l'AC, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) doivent pouvoir être récupérées aisément par les utilisateurs de certificats.

5.1.4 Tailles des clés

Les clés d'AC et de porteurs doivent respecter les exigences de caractéristiques (tailles, algorithmes, etc.) définis respectivement dans les paragraphes 9.5 et 9.6.

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

L'équipement de génération de bi-clés doit utiliser 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, de LCR / LAR et/ou de réponses OCSP.

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

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

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature, ainsi que le cas échéant pour la génération des clés des porteurs, doivent être des modules cryptographiques répondant au minimum aux exigences du niveau de sécurité considéré.

5.2.1.2 Dispositifs de création de signature des porteurs

Les dispositifs de création de signature des porteurs, pour la mise en œuvre de leurs clés privées de signature, doivent respecter les exigences du niveau de sécurité considéré.

Si l'AC ne fournit pas elle-même ce dispositif au porteur, elle doit s'assurer auprès du porteur de la conformité de son dispositif de création de signature, au minimum au travers d'un engagement contractuel clair et explicite du porteur vis-à-vis du PSCE.

5.2.2 Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'AC pour l'exportation / l'importation hors / dans un module cryptographique.

Le contrôle des clés privées de signature de l'AC doit être assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets (systèmes où n exploitants parmi m doivent s'authentifier, avec n au moins égal à 2).

5.2.3 Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des porteurs ne doivent en aucun cas être séquestrées.

5.2.4 Copie de secours de la clé privée

Les clés privées des porteurs ne doivent faire l'objet d'aucune copie de secours par le PSCE.

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 doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuyer 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 doivent être effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique.

La longueur des clés symétriques de chiffrement utilisées sera de préférence au moins égale à 128 bits et en aucun cas inférieur à 100 bits (ex : **A**dvanced **E**ncryption **S**tandard (AES), triple DES).

La taille des blocs utilisés devra être au minimum de 64 bits, et de préférence de 128 bits (triple DES=64 bits, AES=128 bits). Par ailleurs, le mode opératoire utilisé doit apporter une "bonne sécurité" et permettre de protéger la clé privée de l'AC en confidentialité mais aussi en intégrité. Pour ce faire, le mode opératoire CBC-MAC pourrait être utilisé.

5.2.5 Archivage de la clé privée

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

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

Si l'AC génère les clés privées des porteurs en dehors du dispositif du porteur, le transfert doit se faire conformément aux exigences décrites ci-dessus.

Pour les clés privées d'AC, tout transfert doit se faire sous forme chiffrée, conformément aux exigences décrites ci-dessus.

5.2.7 Stockage de la clé privée dans un module cryptographique

Il est recommandé de stocker les clés privées d'AC dans un module cryptographique répondant au minimum aux exigences du niveau de sécurité considéré.

Cependant, le stockage peut être effectué en dehors d'un module cryptographique moyennant les exigences décrites ci-dessus.

5.2.8 Méthode d'activation de la clé privée

5.2.8.1 Clés privées d'AC

La méthode d'activation des clés privées d'AC dans un module cryptographique doit permettre de répondre aux exigences de sécurité considérées.

L'activation des clés privées d'AC dans un module cryptographique doit être contrôlée via des données d'activation et doit faire intervenir au moins deux personnes dans des rôles de confiance (par exemple, responsable sécurité et opérateur).

5.2.8.2 Clés privées des porteurs

La méthode d'activation de la clé privée du porteur dépend du dispositif utilisé. L'activation de la clé privée du porteur doit au minimum être contrôlée via des données d'activation et doit permettre 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 doit être automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc. Une clé privée d'AC peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation doivent permettre de répondre aux exigences du niveau de sécurité considéré.

5.2.9.2 Clés privées des porteurs

Les conditions de désactivation de la clé privée d'un porteur doivent permettre de répondre aux exigences de sécurité considérées.

5.2.10 Méthode de destruction des clés privées

5.2.10.1 Clés privées d'AC

La méthode de destruction des clés privées d'AC doit permettre de répondre aux exigences de sécurité considérées.

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

5.2.10.2 Clés privées des porteurs

Si les clés privées des porteurs sont générées par l'AC dans un module cryptographique hors du dispositif de création de signature, la méthode de destruction de ces clés privées après leur exportation hors du module cryptographique doit permettre de répondre aux exigences de sécurité considérées.

En fin de vie de la clé privée d'un porteur, la méthode de destruction de cette clé privée doit permettre de répondre aux exigences de sécurités considérées.

5.2.11 Niveau d'évaluation sécurité du module cryptographique

Les modules cryptographiques de l'AC doivent être évalués au niveau correspondant à l'usage visé.

Les dispositifs de création de signature des porteurs doivent être 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 couverts par la présente PC Type doivent avoir la même durée de vie, au moins égale à VT::T_PORT_MIN, et au maximum de VT::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. Le PSCE doit préciser dans sa PC la durée de vie des clés de signature d'AC et des certificats correspondants. Cette durée de vie doit être cohérente avec les caractéristiques de l'algorithme et la longueur de clé utilisés et doit être au maximum égale à VT::T_C_AC_MAX.

5.4 Données d'activation

5.4.1 Génération et installation des données d'activation

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

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

5.4.1.2 Génération et installation des données d'activation correspondant à la clé privée du porteur

Si l'AC génère la clé privée du porteur, elle a pour obligation de transmettre au porteur les données d'activation correspondantes par le biais d'un chemin garantissant la protection en intégrité et en confidentialité des données. Notamment, la remise de la donnée d'activation doit être séparée dans le temps ou dans l'espace de la remise de la clé privée.

Par exemple : si les éléments secrets d'un porteur sont gérés sur un support matériel dont la mise en œuvre est conditionnée par l'utilisation d'un code personnel, la fourniture du support et celle du code personnel doivent être réalisées par des moyens différents (par exemple retrait du support à un guichet de l'AE et envoi du code par un autre canal).

Si les données d'activation sont sous forme de mots de passe, le porteur doit être informé de la politique de constitution des mots de passe (par exemple, longueur d'un moins huit (8) caractères, présence d'un moins un caractère spécial, etc.).

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 données d'activation qui sont générées par l'AC pour les modules cryptographiques de l'IGC doivent être protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

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

Si les données d'activation des dispositifs de création de signature des porteurs sont générées par l'AC, elles doivent être protégées en intégrité et en confidentialité jusqu'à la remise aux porteurs.

Si ces données d'activation sont également sauvegardées par l'AC, elles doivent être protégées en intégrité et en confidentialité.

5.4.3 Autres aspects liés aux données d'activation

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

5.5 Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque que le PSCE doit mener.

5.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC doit être défini dans la DPC du PSCE. Il doit au moins répondre aux objectifs de sécurité suivants :

- Identification et authentification forte des utilisateurs 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 rapide des droits d'accès ;
- Protection du réseau contre toute intrusion d'une personne non autorisée ;
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- Fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- Eventuellement, gestion des reprises sur erreur.

Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle doit faire l'objet de mesures particulières, découlant de l'analyse de risque

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

5.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Il est recommandé que les systèmes informatiques de l'IGC mettant en œuvre le module cryptographique fassent l'objet d'une qualification.

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque que l'AC doit mener.

5.6 Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC doit être documentée et doit respecter dans la mesure du possible des normes de modélisation et d'implémentation. La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau doivent être documentées et contrôlées.

5.7 Mesures de sécurité réseau

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

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

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

5.8 Horodatage / Système de datation

Plusieurs exigences de la présente PC Type nécessitent la datation par les différentes composantes de l'IGC d'évènements liés aux activités de l'IGC.

Pour dater ces évènements, les différentes composantes de l'IGC peuvent recourir :

- Soit à une autorité d'horodatage, interne ou externe à l'IGC ;
- Soit en utilisant l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC. Pour les opérations faites hors ligne (ex : administration d'une AC Racine), cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système devra toutefois pouvoir ordonner les évènements avec une précision suffisante. Pour la synchronisation par rapport au temps UTC, il est recommandé de se référer à un système comprenant au moins deux sources indépendantes de temps. Cette synchronisation s'effectue via le protocole NTP (Network Time Protocol) décrit dans le RFC [5905].

Les protocoles d'horodatage les plus répandus sont les suivants :

- Le Time Stamping Protocol (TSP) ou [RFC3161] qui constitue la référence actuelle en matière d'horodatage et qui est le plus répandu ;
- Le protocole XADES-T : XadES prolonge la spécification de la syntaxe et du traitement XML Signature de IETF/W3C dans le domaine de la non-répudiation, en définissant des formats XML pour les signatures électroniques évoluées qui restent valides pendant de grandes périodes et qui incorporent des informations supplémentaires utiles dans les situations d'utilisations

courantes. Cela comprend la preuve de leur validité, même si le signataire ou le tiers vérifiant essayent ensuite de nier (répudier) la validité de la signature.

La mise en place d'un service d'horodatage (interne ou externe) nécessitera la mise en place d'une Politique d'Horodatage (Voir le paragraphe 9.9 pour un plan d'une Politique d'Horodatage Type) qui détaillera les aspects organisationnels, juridiques, techniques et sécuritaires associés au service d'horodatage.

6. PROFIL DES CERTIFICATS DES LCR

6.1 Profil des certificats

Le gabarit des certificats délivrés doit au moins contenir les informations suivantes :

Champ	Valeur	Détail valeur	Commentaire
Version	V3	2	Certificat x509 v3
Numéro de série			Numéro de série du certificat
Algorithme de signature	Exemple : SHA1withRSAEncryption 2048 bits	OID=1.2.840.113549.1.1.5	Identifiant de l'algorithme de signature
Emetteur	CN= O= C=		Nom de l'AC émetteur
Validité à partir de	T0		Date d'activation
Valide jusqu'au	T0 + X ans		Nombre d'années de validité
Objet	CN= O= C=		Identifiant du porteur du certificat
Clé publique	Algorithme OID RSA SubjectPublicKey=XXX 2048 bits	OID=1.2.840.113549.1.1.1	Identifiant de l'algorithme
Nom alternatif du porteur (SubjectAltName)	Email=email porteur	Extension non critique	Adresse email du porteur
Identifiant de la clé publique de l'autorité (AuthorityKeyIdentifier)	AKI ID de la clé = XXXX	Extension non critique	Identifiant de la clé publique à utiliser pour vérifier la signature d'un certificat Dérivé de la clé publique servant à vérifier la signature d'un

			certificat
Identifiant de la clé publique du sujet (SubjectKeyIdentifier)	SKI ID de la clé = XXXX	Extension non critique	Identifiant de la clé publique du certificat au cas où le même porteur aurait plusieurs bi-clés Dérivé de la clé publique du certificat
Point de distribution de la LCR	Adresse LDAP et/ou http		
Politique de certification	A déterminer		Identifiant de la politique de certification
Utilisation de la clé	NonRepudiation[1]	Extension critique	
Extended key usage		Extension non critique	Autres extensions utiles

De plus amples informations sont fournies dans le paragraphe 9.4 .

6.2 Profil des LCR

Le gabarit de la LCR est le suivant :

Champ	Valeur	Commentaires
Version		Version de la LCR utilisée
Signature	Exemple : Sha1RSA	OID de l'algorithme de signature
Issuer	DN de l'AC	DN de l'AC qui a signé la LCR
ThisUpdate	Date et heure	Date de génération de la LCR
NextUpdate	Date et heure	Prochaine date de mise à jour de la LCR
RevokedCertificates	Liste des : • User Certificate (num de série) • Revocation Date	Liste des numéros de série des certificats révoqués ainsi que leur date de révocation

Pour plus d'informations, consulter la RFC 5280.

[1] Ce bit est désormais nommé « content Commitment »

7. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits sont réalisés afin de s'assurer que l'ensemble de l'IGC du PSCE, 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, le PSCE doit procéder à un contrôle de conformité de cette composante.

Le PSCE doit également subir régulièrement un contrôle de conformité de l'ensemble de son IGC, suivant la fréquence VT::F_CONFORM et conformément à la réglementation en vigueur.

7.2 Identités des auditeurs

Le contrôle d'une composante est réalisé par la DGSSI ou par des experts désignés 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 la DGSSI ;

- En cas de résultat "A confirmer", le PSCE remet à la composante un avis précisant sous quel délai les non-conformités doivent être 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 la DGSSI et du PSCE.

8. AUTRES PROBLEMATIQUES METIERS ET LEGALES

Les points suivants devront être détaillés dans la PC :

- Tarifs :
  - Tarifs pour la fourniture ou le renouvellement de certificats ;
  - Tarifs pour accéder aux certificats ;
  - Tarifs pour accéder aux informations d'état et de révocation des certificats ;
  - Tarifs pour d'autres services ;
  - Politique de remboursement
- Responsabilité financière :
  - Couverture par les assurances ;
  - Autres ressources ;
  - Couverture et garantie concernant les entités utilisatrices.
- Confidentialité des données professionnelles :
  - Périmètre des informations confidentielles :
    - la partie non-publique de la DPC du PSCE ;
    - les clés privées de l'AC, des composantes et des porteurs de certificats ;
    - les données d'activation associées aux clés privées d'AC et des porteurs ;
    - tous les secrets de l'IGC ;
    - les journaux d'évènements des composantes de l'IGC ;
    - le dossier d'enregistrement du porteur ;
    - les causes de révocations, sauf accord explicite de publication.

8.1 Durée et fin anticipée de validité de la PC

8.1.1 Durée de validité

La PC du PSCE doit rester 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 Type peut entraîner, en fonction des évolutions apportées, la nécessité pour le PSCE de faire évoluer sa PC correspondante.

En fonction de la nature et de l'importance des évolutions apportées à la PC Type, le délai de mise en conformité sera arrêté par la DGSSI.

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

9. ANNEXES

9.1 Exigences de sécurité

9.1.1 Exigences sur les objectifs de sécurité du module cryptographique

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

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

Le module cryptographique de l'AC doit détecter les tentatives d'altérations physiques et entrer 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, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- Si la bi-clé de signature du porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- Détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- Garantir la confidentialité et l'intégrité de la clé privée ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Générer une signature qui ne peut être falsifiée sans la connaissance de la clé privée ;
- Assurer la fonction de signature pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ;
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

9.2 Variable de temps et niveaux de sécurité

La définition de la PC type fait intervenir des exigences temporelles. Le tableau suivant quantifie ces variables par niveau de sécurité :

Variable	Description	Valeur (niveau sécurisé)
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 24h
F_JOUR_RAP	Fréquence de rapprochement des journaux d'évènements.	1 fois par semaine
F_PUB_dLCR	Fréquence de publication des deltaLCR	24h
F_PUB_LCR	Fréquence de publication des LCR	24h

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.	24h/24 7j/7
T_AC_INDISP	Durée maximale d'indisponibilité par interruption (panne ou maintenance) des systèmes publiant les certificats d'AC.	1h
T_AC_MAX	Durée maximale totale d'indisponibilité par mois des systèmes publiant les certificats d'AC.	4h
T_C_AC_MAX	Durée de vie maximale d'un certificat d'AC	10 ans
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	24h
T_ETAT_DISP	Disponibilité de la fonction d'information sur l'état des certificats	24h/24 7j/7
T_ETAT_INDIS	Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des certificats	1h
T_ETAT_MAX	Durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats	4h
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	8h (jours ouvrées)
T_INF_MAX	Durée maximale totale d'indisponibilité par mois de la fonction de publication	32h (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	30min
T_REC_ARCH	Délai maximum de récupération des archives	2 jours ouvrés
T_REV_DISP	Disponibilité de la fonction de gestion des révocations	24h/24 7j/7
T_REV_INDIS	Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations	30min
T_REV_MAX	Durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations	2h
T_REV_TRAIT	Délai maximum de traitement d'une demande de révocation	24h

9.3 Détails sur le gabarit d'un certificat racine

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3. Un certificat d'AC doit respecter, de base, les exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	PC Type Signature
Version	La valeur de ce champ doit être "2", indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	Cf. chapitre 9.5 sur les exigences en matière d'algorithmes et de longueurs de clés.
Issuer	Le DN qui se trouve dans le champ "Subject" d'un certificat d'AC, dans le champ "Issuer" d'un certificat d'AC ou de porteur, ainsi que dans le champ "Issuer" d'une LCR, doit être conforme aux exigences des chapitres 3.1.1 de [RFC3739] et 5.2.4 de [ETSI_CERT]
Validity	Pas d'exigence supplémentaire par rapport au [RFC5280]
Subject	S'agissant d'un certificat d'AC, ce champ doit respecter les mêmes exigences que le champ "Issuer".
Subject Public Key Info	Cf. chapitre 9.5 ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Unique Identifiers (issuer et subject)	Les PC Types imposant l'unicité des DN des champs Issuer et Subject au sein du domaine de l'AC, les champs Unique Identifiers ne doivent pas être utilisés.
Extensions	Cf. tableau suivant

Extensions

Une extension d'un certificat est caractérisée par :

- Sa présence obligatoire ou non dans le certificat. Ceci indique si l'AC émettrice du certificat a obligation ou non d'intégrer l'extension dans tous les certificats qu'elle émet ;
- Sa criticité. Ceci indique comment les utilisateurs de certificats doivent traiter l'extension et le certificat correspondant, conformément aux principes de gestion de la criticité définis dans la recommandation UIT-T [X.509].

Champ	Obligatoire	Critique	PC Type Signature
Authority Key Identifier	O	N	Pour tous les certificats d'AC, autres que les certificats auto-signés, cette extension doit être présente, être marquée "non critique" et contenir l'identifiant de clé de la clé publique de l'AC émettrice (même valeur que le champ "Subject Key Identifier" du certificat de cette AC émettrice).
Key Usage	O	O	Cette extension doit être marquée "critique".
Certificate Policies	O	N	Cette extension doit être conforme aux exigences du chapitre 3.2.3 du [RFC3739].
Subject Alternative Name *Issuer Alternative Name*	N	N	L'identification des AC via les DN des champs Subject et Issuer étant obligatoire dans la présente PC Type, les champs Subject Alternative Name et Issuer Alternative Name peuvent être présents, mais ils doivent obligatoirement être marqués "non critique" et être conformes aux exigences du chapitre 3.2.1 du [RFC3739].
CRL Distribution Points	O	N	Pour les certificats d'AC autres que les certificats auto-signés (AC Racine), cette extension doit être présente et être conforme aux exigences du chapitre 5.4.14 de [ETSI_CERT].
Authority Information Access	O	N	Si l'AC fournit un service OCSP (ce qui est recommandé par la présente PC), cette extension doit être présente, marquée "non critique" et être conforme aux exigences du chapitre 3.1 du [RFC2560].

NB : Les autres extensions traitées dans le [RFC5280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC5280]. Notamment, les extensions obligatoires pour les certificats d'AC (Basic Constraints, Authority / Subject Key Identifiers,...) doivent être intégrées. La prise en compte des extensions non obligatoires est laissée au choix du PSCE.

9.4 Détails sur le gabarit d'un certificat porteur

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3. Un certificat doit respecter, de base, les exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	PC Type Signature
Version	La valeur de ce champ doit être "2", indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280].
Signature	Cf. chapitre 9.6 ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Issuer	Le DN qui se trouve dans le champ "Subject" d'un certificat d'AC, dans le champ "Issuer" d'un certificat d'AC ou de porteur, ainsi que dans le champ "Issuer" d'une LCR, doit être conforme aux exigences des chapitres 3.1.1 de [RFC3739] et 5.2.4 de [ETSI_CERT].
Validity	Pas d'exigence supplémentaire par rapport au [RFC5280]
Subject	Le DN qui se trouve dans le champ "Subject" d'un certificat porteur doit être conforme aux exigences des chapitres 3.1.2 du [RFC3739] et 5.2.6 de [ETSI_CERT].
Subject Public Key Info	Cf. chapitre 9.6 ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Unique Identifiers (issuer et subject)	La PC Type imposant l'unicité des DN des champs Issuer et Subject au sein du domaine de l'AC, les champs Unique Identifiers ne doivent pas être utilisés.
Extensions	Cf. tableau suivant.

Extensions

Champ	O	C	PC Type Signature
Authority Key Identifier	O	N	Pour tous les certificats porteurs, cette extension doit être présente, être marquée "non critique" et contenir l'identifiant de clé de la clé publique de l'AC émettrice (même valeur que le champ "Subject Key Identifier" du certificat de cette AC émettrice).
Key Usage	O	O	Le bit "contentCommit ment" doit être à "1", les autres bits à "0".
Certificate Policies	O	N	Cette extension doit être conforme aux exigences du chapitre 3.2.3 du [RFC3739].

Subject Alternative Name	N	N	L'identification du porteur via le DN du champ Subject étant obligatoire dans la présente PC Type, le champ Subject Alternative Name peut être présent, mais il doit obligatoirement être marqué "non critique" et être conforme aux exigences du chapitre 3.2.1 du [RFC3739].
Issuer Alternative Name	N	N	L'identification de l'AC émettrice via le DN du champ Issuer étant obligatoire dans la présente PC Type, le champ Issuer Alternative Name peut être présent, mais il doit obligatoirement être marqué "non critique".
Subject Directory Attributes	N	N	Si cette extension est utilisée, elle doit être conforme aux exigences du chapitre 3.2.2 du [RFC3739].
CRL Distribution Points	O	N	Cette extension doit être présente et être conforme aux exigences du chapitre 5.4.14 de [ETSI_CERT].
Freshest CRL	O	N	Si l'AC utilise des deltaLCR (ce qui est recommandé par la présente PC Types), cette extension doit être présente. La syntaxe de cette extension étant identique à celle de "CRL Distribution Points", elle doit être également conforme aux exigences du chapitre 5.4.14 de [ETSI_CERT].
Authority Information Access	O	N	Si l'AC fournit un service OCSP (ce qui est recommandé par la présente PC Types), cette extension doit être présente, marquée "non critique" et être conforme aux exigences du chapitre 3.1 du [RFC2560].

NB : Les autres extensions traitées dans le [RFC5280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC5280]. La prise en compte des extensions non obligatoires est au choix du PSCE.

9.5 Algorithmes de signature et taille de clés des AC

Algorithme	Longueur de clé
RSA	2048 bits
DSA	2048 bits/ q=256
ECDSA	Q=256
Hachage –SHA	SHA-224/256

9.6 Algorithmes et longueurs de clés des porteurs

Algorithme	Longueur de clé
RSA	2048 bits
DSA	2048 bits / q = 256

ECDSA (type GF(p))	q = 256
Hachage – SHA	SHA224/256

Les autres algorithmes présents dans l'annexe B du cahier des charges des prestataires de services de certification électronique, ne sont pas mentionnés ici.

9.7 Documents de références

Références	Document
[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,*
[RFC2560]	*IETF -Internet X.509 Public Key Infrastructure -Online Certificate Status Protocol,* RFC 2560
[RFC3279]	*IETF -Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure -Certificate and Certificate Revocation List (CRL) Profile*
[FIPS180-2]	*NIST -FIPS 180-2 -Secure Hash Standard, Version*
[RFC5280]	*IETF -Internet X.509 Public Key Infrastructure, Certificate and CRL Profile*, RFC 5280
[RFC3739]	*IETF -Internet X.509 Public Key Infrastructure, Qualified Certificates Profile*, RFC 3726 Date
[X.509]	*ITU -Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, Version*
[RFC3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[RFC5905]	Network Time Protocol (Version 4) Protocol and Algorithms Specification
[RFC3161]	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

9.8 Plan Type détaillé d'une Politique d'Horodatage

La mise en place d'une Politique d'Horodatage doit prendre en compte les éléments suivants :

INTRODUCTION ET OBJET DU DOCUMENT

ACTEURS DE L'HORODATAGE

- Services d'horodatage
- Autorité d'horodatage
- Service demandeur
- Commission d'approbation

POLITIQUE D'HORODATAGE

- Définition
- Identification
- Conformité
- Certificats d'horodatage

OBLIGATIONS

- Obligation de l'AH
- Obligation de l'opérateur du service d'horodatage
- Obligations et responsabilités des services demandeurs
  - Vérification de la validité des jetons dès réception
  - Archivage des jetons d'horodatage
- Obligations des utilisateurs finaux

EXIGENCES CONCERNANT LES PRATIQUES D'HORODATAGE

- Déclaration des pratiques d'horodatage de l'OSH et résume publiable des politiques
  - Déclaration des Pratiques d'Horodatage (DPH) de l'OSH
  - Résumé publiable des politiques
- Cycle de vie des clés de l'AH
  - Génération des clés
  - Protection des clés privées de l'AH
  - Renouvellement des clés de l'AH
  - Fin du cycle de vie des clés cryptographiques
  - Gestion du cycle de vie des UH utilisées pour la signature des jetons d'horodatage

- Production des jetons d'horodatage
    - Jeton d’horodatage
    - Synchronisation avec l’UTC
    - Disponibilité du service
- Validité d'un jeton d'horodatage
    - Durée de validité d’un jeton d’horodatage
    - Vérification d’un jeton d’horodatage par le service demandeur
- Gestion et exploitation de l'AH
    - Gestion de la sécurité
    - Classification des biens
    - Sécurité du personnel
    - Sécurité physique
    - Sécurité d’exploitation
    - Zonage des locaux
    - Gestion des accès aux composantes du système d’horodatage de l’AH
    - Maintenance et déploiement de l’AH
    - Mesures à prendre en cas de compromission
    - Fin du cycle de vie de l’AH
    - Données enregistrées par l’AH

ADMINISTRATION DE LA POLITIQUE D’HORODATAGE

- Procédures de modification de la politique d'horodatage
- Procédures de publication et de notification