Référentiel Certification Electronique

Annexe 2

Politique de Certification Type

« Certificats Electroniques de personne »

Adaptée à la loi sur la Transactions Electroniques et son décret d'application (décret 2018-062)

Version 1

Mise à jour : Décembre 2019

Sommaire

I.Introduction

I.1. Présentation générale

I.1.1. Objet du document

Le présent document « Politique de Certification Type, Certificats Electroniques de personne » (PC Type Personne) est basé sur le Référentiel Général de Sécurité Français. Il fait partie du Référentiel des exigences applicables aux PSCE (« Référentiel Certification Electronique »). Il en constitue l'Annexe 2.

Cette Annexe technique liste les règles que les Prestataires de Services de Certification Electronique (« PSCE »), délivrant des Certificats Electroniques à des personnes doivent respecter. Les PSCE délivrant des Certificats Electroniques à des Services applicatifs se reporteront à l'Annexe 3 du Référentiel Certification Electronique.

Ce document distingue trois niveaux de sécurité aux exigences croissantes : *, ** et ***. Il distingue, par ailleurs, trois usages de Certificats Electroniques pouvant être combinés : Signature Electronique, Authentification, et Confidentialité.

Les exigences, communes à tous les niveaux et particulières à un niveau donné, spécifiées dans la présente PC Type doivent être respectées intégralement par les PSCE moyennant l'exception suivante : dans la présente PC Type, un certain nombre de recommandations sont formulées, en lieu et place d'obligations.

Cette PC Type n'est pas une PC à part entière : elle ne peut pas être utilisée telle quelle par un PSCE en tant que PC pour être mentionnée dans ses Certificats et sa Déclaration des Pratiques de Certification (« DPC »). Un PSCE doit en reprendre, dans sa propre PC, l'ensemble des exigences correspondant au niveau visé.

Afin de favoriser l'interopérabilité, dans le cadre de la sécurisation des échanges Electroniques des règles et recommandations sur les formats de Certificats et de listes de révocations, compatibles avec la norme [X.509] sont formulées l'Annexe 4 du Référentiel Certification Electronique.

I.1.2. Conventions de rédaction

De manière à mettre en exergue les règles spécifiques à un « niveau de sécurité », à un « type d'usage » ou à un « type de Porteur », celles-ci seront présentées dans un encadré, le titre du cadre précisant son périmètre d'application (usage du Certificat Electronique, niveau de sécurité et type de Porteur du Certificat Electronique). La forme est la suivante :

[Usage]	**[Niveau de sécurité]**	**[Type de Porteur]**
Intitulé de la règle …		

Les exigences qui ne sont pas encadrées s'appliquent de manière identique aux trois niveaux.

I.2. Identification du document

La présente PC Type est dénommée « Politique de Certification Type – Certificats Electroniques de Personne ».

Elle peut être identifiée par son « nom », son « numéro de version » et sa « date de mise à jour ».

I.3. Définitions et acronymes

I.3.1. Acronymes

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

AC	Autorité de Certification (*différente avec l'Autorité de Certification Togolaise*)
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
AH	Autorité d'Horodatage
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
IGC	Infrastructure de Gestion de Clés
LAR	Liste des Certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
OC	Opérateur 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
SSI	Sécurité des Systèmes d'Information
URL	Uniform Resource Locator

I.3.2. Définitions

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

Applications utilisatrices - Services applicatifs exploitant les Certificats émis par l'AC pour des

besoins d'Authentification, de Chiffrement ou de Signature du Porteur du Certificat ou des besoins d'Authentification ou de Cachet du serveur auquel le Certificat est rattaché.

Autorité Administrative – Tout organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

Autorité d'Horodatage - Autorité responsable de la gestion d'un Service d'Horodatage.

Autorité de Certification (AC) (différent de l'Autorité de Certification Togolaise) - 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 PC. Le terme d'Autorité de Certification désigne l'AC chargée de l'application de la Politique de Certification, répondant aux exigences de la présente PC Type, au sein du PSCE souhaitant faire qualifier la famille de Certificats correspondante.

Certificat Electronique - Document sous forme Electronique attestant du lien entre une clé publique et l'identité de son titulaire. Cette attestation émise par un Prestataire de Service de Certification Electronique (PSCE) est utilisé pour permettre les usages définis. Il est délivré par une Autorité de Certification. Le Certificat est valide pendant une durée donnée précisée dans celui-ci. Les usages des Certificats Electroniques régis par le présent document sont la Signature Electronique, l'Authentification, la Confidentialité ou toute combinaison de ces usages.

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 Electronique aux Utilisateurs et en conformité avec la ou les Politiques de Certification qu'elle s'est engagée à respecter.

Dispositif de protection des éléments secrets - Un dispositif de protection des éléments secrets désigne un dispositif de stockage des éléments secrets remis au Porteur (exemples : clé privée, code PIN, etc.). Il peut prendre la forme d'une carte à puce, d'une clé USB à capacités cryptographique ou se présenter au format logiciel (exemple fichier PKCS#12).

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

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 (AC), d'un Opérateur de Certification (OC), d'une Autorité d'Enregistrement centralisée et/ou locale (AE), d'une entité d'archivage, d'une entité de publication, etc.

Politique de Certification (PC) - Ensemble de règles, identifié par un nom, 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.

Produit de sécurité - Un dispositif, logiciel ou matériel, qui met en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information ou d'un système.

Qualification d'un Prestataire de Services de Certification Electronique - Le Référentiel Certification Electronique décrit la procédure de qualification des PSCE. La qualification d'un PSCE est un acte par lequel l'Autorité de Certification Togolaise atteste de la conformité du PSCE et de ses Services de Confiance aux exigences du Référentiel Certification Electronique ainsi que de la LTE et son décret d'application.

Système d'information – Tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie Electronique entre entités et/ou Utilisateurs.

I.4. Entités intervenant dans l'IGC

Les entités intervenantes dans une Infrastructure de Gestion de Clés sont les suivants :

- Autorité de Certification (AC)
- Autorité d'Enregistrement (AE)
- Porteurs de Certificats (PC)
- Utilisateurs de Certificats (UC)

L'AC inclut notamment les rôles suivants qui peuvent être opérés en interne ou confiés à des tiers sous réserve de répondre aux exigences du présent Référentiel à savoir, les Opérateurs de Certification (OC), les Autorités de Validation (AV), les Autorités de Révocation.

I.4.1. Autorités de Certification

L'AC 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.

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI dans le domaine (cf. les normes ETSI_QCP et ETSI_NQCP), la décomposition fonctionnelle d'une IGC qui est retenue dans la présente PC Type est la suivante[1] :

[1] Cette décomposition est donnée à titre d'illustration pour les besoins de la présente PC Type et n'impose aucune restriction sur la décomposition d'une implémentation effective d'une IGC.

- **Autorité d'enregistrement (AE)[2]** - Cette fonction vérifie et valide 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. Et, en général, délivre le Certificat au Porteur.
- **Fonction de génération des Certificats** - Cette fonction génère (création du format, Signature Electronique 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 soit du Porteur, soit de la fonction de génération des éléments secrets du Porteur, si c'est cette dernière qui génère la bi-clé du Porteur.
- **Fonction de génération des éléments secrets du Porteur** - Cette fonction génère les éléments secrets à destination du Porteur, si l'OC 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 réalisée par l'AE** - Cette fonction remet au Porteur au minimum son Certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC et l'OC (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) ou selon un mode requête / réponse temps réel (OCSP).

[2] Les documents de l'ETSI, notamment les normes ETSI_QCP et ETSI_NQCP, utilisent le terme Service d'Enregistrement. Le [RFC3647], utilise le terme Autorité d'Enregistrement. En cohérence avec ce dernier document, il est conservé l'utilisation du terme Autorité d'Enregistrement, mais qui doit être compris, dans la présente PC Type, en tant que fonction et non pas en tant que composante technique de l'IGC.

Une IGC gérant des Certificats de Confidentialité peut assurer au surplus les fonctions suivantes :

- **Fonction de gestion des recouvrements** - Cette fonction traite les demandes de recouvrement de clés privées des Porteurs (notamment identification et Authentification du demandeur) et détermine les actions à mener. Dans le cas d'une décision positive, le recouvrement est réalisé par la fonction de séquestre et recouvrement.
- **Fonction de séquestre et recouvrement** - Cette fonction fournit la capacité de séquestrer de manière sécurisée les clés privées de Confidentialité des Porteurs, puis de les recouvrer en cas de besoin, sur la base de demandes authentifiées et traitées par la fonction de gestion des recouvrements (cf. chapitre IV.12).

Les fonctions ci-dessus, à l'exception des fonctions de génération des éléments secrets, de séquestre et de recouvrement, sont les fonctions minimales que doit obligatoirement mettre en œuvre une IGC gérant des Certificats Electroniques.

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

- **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.
- **Utilisateur de Certificat** - L'entité ou la personne physique qui reçoit un Certificat et qui s'y fie pour vérifier une Signature Electronique ou une valeur d'Authentification provenant du Porteur du Certificat ou chiffrer des données à destination du Porteur du Certificat**.**
- **Personne autorisée** - Il s'agit d'une personne autre que le Porteur qui est autorisée par la Politique de Certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du Porteur (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du Porteur 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. La présente PC Type n'impose aucun modèle particulier, dans la limite où l'AC respecte les exigences qui y sont définies.

Cependant, les parties de l'AC concernées par la génération de Certificats et la gestion des révocations doivent être indépendantes d'autres organisations en ce qui concerne leurs décisions concernant la mise en place, la fourniture, le maintien et la suspension des Services en particulier, leurs cadres dirigeants, leur personnel d'encadrement et leur personnel ayant des rôles de confiance, doivent être libres de toute pression d'ordre commercial, financier ou autre, qui pourraient influer négativement sur la confiance dans les Services fournis par l'AC. Les parties de l'AC concernées par la génération de Certificat et de la gestion des révocations doivent avoir une structure documentée qui préserve l'impartialité des opérations.

L'organisation adoptée dépend notamment des prestations fournies par l'AC : génération ou non de la bi- clé du Porteur, fourniture ou non du dispositif de protection des éléments secrets au Porteur et, si oui, fourniture avant ou après génération de la bi-clé du Porteur, etc.

L'AC doit préciser dans sa PC les prestations effectivement fournies et son organisation fonctionnelle correspondante.

Dans la pratique, la mise en œuvre opérationnelle de ces fonctions peut être effectuée par une ou plusieurs composante(s) de l'IGC (opérateurs techniques et/ou autorités tel que OC, AE, SP, AH, …), qui peuvent être internes à l'AC et/ou opérées par des entités externes.

La Déclaration des Pratiques de Certification (DPC) de l'AC 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.

Quelle que soit l'organisation opérationnelle mise en œuvre, l'AC 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. En particulier, les Politiques et les procédures, en fonction desquelles l'AC fonctionne, doivent être non- discriminatoires.

Le cadre contractuel entre l'AC et ses différentes composantes opérées par des entités externes doit être clairement documenté.

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, les exigences qui incombent à l'AC en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- Être une entité légale au sens de la loi Togolaise.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux solutions d'application d'échanges dématérialisés, aux Porteurs, aux Utilisateurs de Certificats, ceux qui mettent en œuvre ses Certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions obligatoires de la présente PC Type, notamment en matière de génération des Certificats, de remise au Porteur, de gestion des révocations et d'information sur l'état des Certificats.
- Élaborer, mettre en œuvre, contrôler et maintenir de façon itérative les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels.

	Niveau (***)	
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. Elle élabore sa DPC en fonction de cette analyse.		

	Niveaux (*) et (**)	
Il est recommandé que l'AC mène une analyse de risque.		

- 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. À ce titre, elle doit posséder un ou des systèmes de gestion de la qualité et de la sécurité de l'information adaptés aux Services de Certification qu'elle assure.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les Certificats correspondants (Signature de Certificats, de LCR 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.
- Suivre les demandes en capacité et réaliser des projections concernant les futurs besoins en capacité afin de garantir la disponibilité du Service, notamment en matière de capacité de traitement et de stockage.

		[Entreprise] [Administration]
Être en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des Certificats des Porteurs de cette entité.		

		[Particulier]
Être en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des Certificats des Porteurs de cette entité.		

I.4.2. Autorité d'enregistrement

L'AE a pour rôle de vérifier l'identité du futur Porteur de Certificat. Pour cela, l'AE assure les tâches 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, 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).

		[Entreprise] [Administration]
La prise en compte et la vérification des informations du futur Porteur et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant.		

		[Particulier]
La prise en compte et la vérification des informations du futur Porteur et la constitution du dossier d'enregistrement correspondant.		

I.4.3. Porteurs de Certificats

Dans le contexte du présent Référentiel, un Porteur de Certificats ne peut être qu'une personne physique qui utilise sa clé privée et le Certificat Electronique associé :

- pour son propre compte, dans le cas des particuliers ;
- pour ses activités en lien avec l'entité, identifiée dans le Certificat Electronique, avec laquelle il a une relation contractuelle, hiérarchique ou réglementaire.

Le Porteur respecte les conditions qui lui incombent définies dans la PC de l'AC, qui doit reprendre les conditions définies dans la présente PC Type.

I.4.4. Utilisateurs de Certificats

[Confidentialité]		
Un Utilisateur (ou accepteur) de Certificats Electroniques de Confidentialité peut être notamment : - Un Service en ligne qui utilise un dispositif de Chiffrement pour chiffrer des données ou un message à destination du Porteur du Certificat ; - Une personne qui émet un message chiffré à l'intention du Porteur du Certificat Electronique.		
[Authentification]		
Un Utilisateur (ou accepteur) de Certificats Electroniques d'Authentification peut être notamment : - Un Service en ligne qui utilise un Certificat et un dispositif de vérification d'Authentification soit pour valider une demande d'accès faite par le Porteur du Certificat dans le cadre d'un contrôle d'accès, soit pour authentifier l'origine d'un message ou de données transmises par le Porteur du Certificat ; - Un Utilisateur destinataire d'un message ou de données et qui utilise un Certificat et un dispositif de vérification d'Authentification afin d'en authentifier l'origine.		

[Signature]		
Un Utilisateur (ou accepteur) de Certificats de Signature Electronique peut être notamment : - Un Service en ligne qui utilise un dispositif de vérification de Signature pour vérifier la Signature Electronique apposée sur des données ou un message par le Porteur du		

Certificat ;

- Un Utilisateur qui signe Electroniquement un document ou un message ;
- Un Utilisateur destinataire d'un message ou de données et qui utilise un Certificat et un dispositif de vérification de Signature afin de vérifier la Signature Electronique apposée par le Porteur du Certificat sur ce message ou sur ces données.

Les Utilisateurs de Certificats doivent prendre toutes autres précautions prescrites dans les éventuels accords ou tout autre document, notamment ceux précisés aux chapitres IX.5.3 et IX.5.4. En particulier, l'AC doit respecter ses responsabilités envers les Utilisateurs qui ont « raisonnablement » confiance dans un Certificat.

I.4.5. Autres participants

Composantes de l'IGC

La décomposition en fonctions de l'IGC est présentée au chapitre I.4.1 ci-dessus. Les composantes de l'IGC mettant en œuvre ces fonctions devront être présentées dans la DPC de l'AC.

I.5. Usage des Certificats

I.5.1. Domaines d'utilisation applicable

I.5.1.1. Bi-clés et Certificats des Porteurs

Usages des Certificats Electroniques des Porteurs :

[Confidentialité]		
Lorsque le Certificat Electronique délivré par le PSCE est un Certificat de Confidentialité, les usages sont : - Déchiffrement : à l'aide de sa clé privée, un Porteur déchiffre les données qui lui ont été transmises dans le cadre d'échanges dématérialisés, chiffrées à partir de sa clé publique ; - Chiffrement : à l'aide de la publique du destinataire, une personne chiffre des données. Cela couvre notamment le cas de Chiffrement par une clé symétrique de fichiers ou de messages, clé elle-même protégée par un mécanisme cryptographique asymétrique, de type RSA (Chiffrement de la clé symétrique par la clé publique du Porteur et Déchiffrement par sa clé privée) ou de type Diffie- Hellman (obtention de la clé symétrique, par l'émetteur d'un message, via un algorithme combinant la clé privée de l'émetteur et la clé publique du destinataire, et inversement pour l'obtention de cette clé symétrique par le destinataire du message).		

[Authentification]		

Lorsque le Certificat Electronique délivré par le PSCE est un Certificat d'Authentification, les usages sont l'Authentification des Porteurs auprès de serveurs distants ou auprès d'autres personnes. Il peut s'agir d'Authentification dans le cadre d'un contrôle d'accès à un serveur ou une application, ou de l'Authentification de l'origine de données dans le cadre de la messagerie Electronique.

[Signature]		
Lorsque le Certificat Electronique délivré par le PSCE est un Certificat de Signature Electronique, les usages sont la Signature Electronique de données. Une telle Signature Electronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.		

[Authentification et Signature]		
Lorsque le Certificat Electronique délivré par le PSCE est un Certificat double usage Signature Electronique + Authentification, les usages sont l'ensemble de ceux identifiés ci-dessus pour les usages séparés d'Authentification et de Signature.		

Certaines applications d'échanges dématérialisés peuvent nécessiter des Certificats à des fins de tests ou de recette. De tels Certificats doivent pouvoir être distingués des Certificats "de production" fournis et gérés par l'AC. Dans certains cas, une AC spécifique "de test" pourra être mise en place.

[Signature]		
Nota - S'agissant de Signatures Electroniques devant pouvoir être vérifiées potentiellement longtemps (plusieurs années) après la fin de validité des Certificats correspondants, il est recommandé que les applications s'appuient sur des Politiques de Signatures formalisées déterminant, notamment, les informations à conserver (Certificats, statuts de ces Certificats,…) et le recours éventuel à des Services d'Horodatage et d'archivage sécurisé.		

Niveaux de sécurité :

	Niveau (***)	
Les Certificats Electronique objets de la présente PC Type sont utilisés par des applications pour lesquelles les besoins de sécurité sont très forts eu égard aux risques très élevés qui les menacent (usurpation d'identité, …).		

	Niveau (**)	
Les Certificats Electronique objets de la présente PC Type sont utilisés par des applications pour lesquelles les besoins de sécurité sont forts eu égard aux risques élevés qui les menacent (usurpation d'identité, …).		

	Niveau (*)	
Les Certificats Electronique objets de la présente PC Type sont utilisés par des applications pour lesquelles les besoins de sécurité sont moyens eu égard aux risques qui les menacent.		

I.5.1.2. Bi-clés et Certificats d'AC et de composantes

Cette PC Type comporte également des exigences concernant les bi-clés et Certificats de l'AC (Signature des Certificats des Porteurs, des LCR / LAR ou 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 génère et signe différents types d'objets : Certificats, LCR / LAR ou 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 en particulier pour les réponses OCSP.

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

1) L'AC dispose d'une seule bi-clé et le Certificat correspondant est rattaché à une AC de niveau supérieur (hiérarchie d'AC).

2) 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). Elle émet des Certificats d'Utilisateurs finaux.

3) L'AC dispose de bi-clés distinctes, le Certificat correspondant à la bi-clé de Signature de Certificats est un Certificat racine (Certificat autosigné non rattaché à une AC de niveau supérieur) et les Certificats des autres bi-clés sont signés par cette bi-clé de Signature de Certificats de l'AC. Les Certificats d'Utilisateurs finaux sont signés par ces autres bi-clés.

4) L'AC dispose de bi-clés distinctes, le Certificat correspondant à la bi-clé de Signature de Certificats est rattaché à une AC de niveau supérieur (hiérarchie d'AC) et les Certificats correspondant aux autres bi-clés sont signés par cette bi-clé de Signature de Certificats de l'AC.

5) L'AC dispose de bi-clés distinctes, les Certificats correspondant à ces bi-clés sont rattachés à une AC de niveau supérieur (hiérarchie d'AC).

Le cas n°2 est à éviter pour des services de confiance.

La présente PC Type recommande la mise en œuvre du cas n°5, 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 (bi-clés séparées ou non), les bi-clés et Certificats de l'AC pour la Signature de Certificats, de LCR / LAR ou de réponses OCSP ne doivent être utilisés qu'à cette fin. Ils ne doivent notamment être utilisés ni à des fins de Confidentialité, ni à des fins d'Authentification.

Conformément au [CWA14167-1], les différentes clés internes à l'IGC peuvent être décomposées suivant les catégories suivantes :

- la (ou les) clé(s) de Signature d'AC, utilisée(s) pour signer les Certificats générés par l'AC ainsi que les informations sur l'état des Certificats (LCR / LAR ou réponses OCSP) ;
- les clés d'infrastructure, utilisées par les systèmes intervenant dans l'IGC à des fins d'Authentification, de Signature des journaux d'évènements, de Chiffrement des données échangées ou stockées au sein de l'IGC, etc. ;
- les clés de contrôle, assignées au personnel de l'IGC afin de s'authentifier vis-à-vis des différents systèmes, de signer et/ou de chiffrer des messages ou des données échangés, etc.

Les deux derniers types de clés peuvent être des clés asymétriques et/ou symétriques.

Ces différents types de clés, et éventuellement les Certificats correspondants, doivent être couverts par leurs propres engagements, complets et à part entière. Ces engagements doivent faire partie directement de la propre PC de l'AC, couvrant les Certificats de Porteurs (cf. chapitre I.1), ou bien faire l'objet de PC séparées (par exemple, PC d'une AC Racine couvrant les Certificats d'AC).

La PC de l'AC répondant à la présente PC Type doit au minimum reprendre les exigences de cette dernière sur les Certificats d'AC et de composantes. En cas de traitement de ces Certificats dans des PC séparées, ces PC doivent être cohérentes avec les exigences de la PC de l'AC et de la présente PC Type.

I.5.2. Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des Certificats sont définies au chapitre IV.5 ci-dessous, en fonction du niveau de sécurité. L'AC doit respecter ces restrictions et imposer leur respect par ses Porteurs et ses Utilisateurs de Certificats.

À cette fin, elle doit communiquer à tous les Porteurs et Utilisateurs potentiels les termes et conditions relatives à l'utilisation du Certificat.

I.6. Gestion de la PC

I.6.1. Entité gérant la PC

La direction de l'AC est responsable de la validation et de la gestion de la PC répondant aux exigences de la présente PC Type.

I.6.2. Point de contact

À préciser dans la PC de l'AC.

I.6.3. Entité déterminant la conformité d'une DPC avec cette PC

L'AC doit être pourvue d'une direction ayant autorité et une responsabilité finale pour déterminer la conformité de la DPC avec la PC.

I.6.4. Procédures d'approbation de la conformité de la DPC

L'AC doit mettre en place un processus d'approbation de la conformité de la DPC avec la PC.

L'AC est responsable de la gestion (mise à jour, révisions) de la DPC. Toute demande de mise à jour de la DPC doit suivre le processus d'approbation mis en place. Toute nouvelle version de la DPC doit être publiée, conformément aux exigences du paragraphe II.2 sans délai.

II. Responsabilités concernant la mise à disposition des informations devant être publiées

II.1. Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des Porteurs et des Utilisateurs de Certificats, l'AC doit mettre en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des Certificats (cf. chapitre I.4.1 ci-dessus).

La PC de l'AC doit préciser les méthodes de mise à disposition et les URL correspondantes (annuaire accessible par le protocole LDAP et/ou HTTP, serveur Web, serveur OCSP, etc.).

II.2. Informations devant être publiées

L'AC a pour obligation de publier au minimum les informations suivantes à destination des Porteurs et Utilisateurs de Certificats :

- sa Politique de Certification, couvrant l'ensemble des rubriques du [RFC3647][3] et conforme à la présente PC Type, ainsi que les éventuels documents complémentaires (par exemple, profils des Certificats s'ils sont définis dans un document séparé) ;
- la liste des Certificats révoqués (Porteurs et AC) ;
- les Certificats de l'AC, en cours de validité ;
- si l'AC est rattachée à une hiérarchie d'AC, les Certificats en cours de validité des AC de cette hiérarchie, les différentes Politiques de Certification correspondantes et les éventuels documents complémentaires, ceci jusqu'à l'AC Racine ;
- pour les Certificats d'AC autosignés (AC Racine), les informations permettant aux Utilisateurs de Certificats de s'assurer de l'origine de ces Certificats (cf. chapitre VI.1.4) et de leur état (cf. chapitre IV.10).

L'AC a l'obligation de publier, à destination des Porteurs et Utilisateurs de Certificats, sa déclaration des pratiques de Certification ainsi que toute autre documentation pertinente pour

[3] Si sa PC n'est pas strictement conforme au plan du [RFC3647], l'AC devra y joindre un tableau de correspondance démontrant la complétude de sa PC par rapport au [RFC3647].

rendre possible l'évaluation de la conformité avec sa Politique de Certification. Cependant, elle n'est en général pas tenue de rendre publics tous les détails relatifs à ses pratiques.

L'AC a également pour obligation de publier, 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.).

De plus, compte tenu de la complexité de lecture d'une PC pour des Porteurs ou des Utilisateurs de Certificats non spécialistes du domaine, il est obligatoire que l'AC publie également des conditions générales d'utilisation correspondant aux "PKI Disclosure Statement" (PDS) définis dans les normes [ETSI_NQCP] et [RFC3647].

Il est recommandé que ces conditions générales aient une structure conforme à celle décrite en Annexe B de [ETSI_NQCP] et reprennent ainsi, à destination des Porteurs et des Utilisateurs de Certificats, les informations pertinentes de la PC de l'AC :

- les conditions d'usages des Certificats et leurs limites,
- l'identifiant : OID de la PC applicable,
- les obligations et responsabilités des différentes parties, notamment les exigences relatives à la vérification du statut de révocation d'un Certificat pour les Utilisateurs,
- les garanties et limites de garanties de l'AC,
- les informations sur comment vérifier un Certificat,
- la durée de conservation des dossiers d'enregistrement et des journaux d'évènements,
- les procédures pour la résolution des réclamations et des litiges,
- le système légal applicable,
- si l'AC a été déclarée conforme à la Politique identifiée et dans ce cas au travers de quel schéma.

Ces conditions générales font notamment partie intégrante du dossier d'enregistrement.

Le moyen utilisé pour la publication de ces informations, sauf pour les LCR / LAR (cf. chapitre IV.10), est libre mais doit être précisé dans la PC de l'AC. Il doit garantir l'intégrité, la lisibilité, la compréhensibilité et la clarté des informations publiées.

II.3. Délais et fréquences de publication

Les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.) doivent être publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC. En particulier, toute nouvelle version doit être communiquée au Porteur lors d'une demande de renouvellement de clé et doit faire l'objet d'un nouvel accord. Les systèmes publiant ces informations doivent au moins être disponibles les jours ouvrés.

Les Certificats d'AC doivent être diffusés préalablement à toute diffusion de Certificats de Porteurs et/ou de LCR correspondants et les systèmes les publiant doivent avoir une disponibilité

de 24h/24 et 7j/7[4].

Les délais et fréquences de publication des informations d'état des Certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux chapitres IV.9 et IV.10.

Il est à noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une indisponibilité de cette information.

II.4. Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des Utilisateurs de Certificats doit être libre d'accès en lecture.

	Niveau (***)	
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).		

	Niveau (**)	
- L'accès en modification aux systèmes de publication des informations d'état des Certificats (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). - L'accès en modification aux systèmes de publication des autres informations doit être strictement limité aux fonctions internes habilitées de l'IGC, au moins au travers d'un **contrôle d'accès de type mots de passe** basé sur une Politique de gestion stricte des mots de passe.		

	Niveau (*)	
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 moins au travers d'un **contrôle d'accès de type mots de passe** basé sur une Politique de gestion stricte des mots de passe.		

[4] Le PSCE décrira dans sa PC/DPC les moyens mis en œuvre pour respecter cet engagement.

III. Identification et Authentification

III.1. Nommage

III.1.1. Types de noms

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

Dans chaque Certificat conforme à la norme [X.509], l'AC émettrice (issuer) et le Porteur (subject) sont identifiés par un "Distinguished Name" (DN) répondant aux exigences de la norme [X.501].

Des règles sur la construction du DN de ces champs sont précisées dans l'Annexe 4 du Référentiel Certification Electronique.

III.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.

III.1.3. Pseudonymisation des Porteurs

L'AC doit pouvoir à tout moment être en mesure de fournir, moyennant le respect de ses obligations en matière de protection des données personnelles (cf. chapitre IX.4), l'identité réelle du Porteur en conservant les caractéristiques et références des documents présentés par le Porteur pour justifier de son identité.

L'identifiant d'un Porteur dans son Certificat peut être un pseudonyme à condition d'être identifié comme tel.

III.1.4. Règles d'interprétation des différentes formes de nom

L'Annexe 4 du Référentiel Certification Electronique fournit des règles à ce sujet. Le cas échéant des précisions seront fournies par l'AC dans sa PC.

III.1.5. Unicité des noms

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.

Ce DN doit pour cela respecter les règles correspondantes définies dans l'Annexe 4 du Référentiel Certification Electronique, notamment pour le traitement des cas d'homonymie 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. L'AC précisera dans sa PC et sa DPC comment elle répond à cette exigence.

Il est à 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.

III.1.6. 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.

Des précisions seront fournies dans la PC de l'AC.

III.2. Validation initiale de l'identité

L'enregistrement d'un Porteur se fait directement auprès de l'AE.

La vérification et la validation initiales de l'identité d'une entité, d'une personne physique et éventuellement de son rattachement à une entité, est ainsi réalisée dans les cas suivants :

		[Entreprise] [Administration]
Enregistrement d'un Porteur : validation par l'AE de l'identité "personne morale" de l'entité de rattachement du Porteur, de l'identité "personne physique" du futur Porteur et du rattachement du futur Porteur à l'entité.		

		[Particulier]
Enregistrement d'un Porteur [PARTICULIER] : validation par l'AE de l'identité "personne physique" du futur Porteur.		

Pour des raisons de simplicité de présentation, ces différents cas sont regroupés dans le chapitre III.2.3.

III.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, une preuve de possession de sa clé privée correspondant à la clé publique contenue dans la demande de Certificat.

III.2.2. Validation de l'identité d'un organisme

Cf. chapitre III.2.3.

III.2.3. Validation de l'identité d'un individu

III.2.3.1. Enregistrement d'un Porteur [Particulier]

Dossier d'enregistrement :

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 carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie,
- l'adresse postale et / ou l'adresse mail permettant à l'AC de contacter le Porteur,
- les conditions générales d'utilisation signées.

[Signature]	**Niveau (***)**	
l'engagement relatif à l'utilisation d'un dispositif sécurisé de création de Signature conforme aux exigences de l'Annexe 3, dans le cas où le PSCE ne le délivre pas.		

Nota 1 – Certaines pièces constitutives du dossier d'enregistrement, ou leur Signature par le Porteur, peuvent être fournies ou réalisées lors de la remise du Certificat par l'AC.

Nota 2 - 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.

Nota 3 - Lorsque le Porteur est un mineur ou un incapable majeur, la demande de Certificat écrite est signée par son représentant (tuteur ou administration légale). Ce dernier joint également à la demande un document officiel de sa propre identité et un document justifiant son statut de représentant du mineur ou de l'incapable majeur.

Procédure de vérification de l'identité du Porteur :

	Niveau (***)	
La vérification de l'identité du Porteur par l'AE est réalisée lors d'un face-à-face physique[5].		

	Niveau (**)	
L'Authentification du Porteur par l'AE est réalisée lors d'un face-à-face physique[6] ou sous forme		

[5] Ce face-à-face physique peut être réalisé lors de la remise par l'AC au porteur du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du futur porteur. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

dématérialisée à condition que la demande soit signée par le Porteur à l'aide d'un procédé de Signature Electronique conforme au minimum aux exigences du niveau (**)[7] décrites dans l'Annexe 1 du Référentiel Certification Electronique.

	Niveau (*)	
L'Authentification du Porteur peut notamment se faire : - Soit par l'envoi du dossier papier à l'AE accompagné d'une photocopie du document d'identité du futur Porteur certifiée conforme par lui-même (date, de moins de 3 mois, et Signature du futur Porteur sur la photocopie de ses papiers d'identité, précédées de la mention "copie certifiée conforme à l'original"). - Soit via une demande d'enregistrement dématérialisée signée Electroniquement par le futur Porteur à l'aide d'un procédé de Signature Electronique conforme aux exigences du niveau (*) décrites dans l'Annexe 3 du Référentiel Certification Electronique et que la Signature soit vérifiée et valide au moment de l'enregistrement. - Soit par la communication d'un élément propre au futur Porteur permettant de l'identifier au sein d'une base de données pré-établie.		

III.2.3.2. Enregistrement d'un Porteur [Entreprise] / [Administration]

L'enregistrement du futur Porteur représentant une entité nécessite, l'identification de cette entité, l'identification de la personne physique et la preuve du rattachement de la personne physique à l'entité.

Dossier d'enregistrement :

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

- un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le futur Porteur auquel le Certificat doit être délivré. Ce mandat doit être signé pour acceptation par le futur Porteur bénéficiaire,
- [Entreprise] toute pièce, valide lors de la demande de Certificat (Certificat d'Identification) attestant de l'existence de l'entreprise, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le Certificat,
- [Entreprise] tout document attestant de la qualité du signataire de la demande de Certificat,
- un document officiel d'identité en cours de validité du futur Porteur ou une carte professionnelle délivrée par une autorité administrative, comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour). Ces documents sont transmis à l'AE qui en conserve une copie ou les traces,
- l'adresse postale et / ou l'adresse mail permettant à l'AC de contacter le Porteur,

---

[6] Cf. note de bas de page n°5.

[7] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

- les conditions générales d'utilisation signées.

[Signature]	**Niveau (***)**	
l'engagement relatif à l'utilisation d'un dispositif sécurisé de création de Signature conforme aux exigences de l'Annexe 3, dans le cas où le PSCE ne le délivre pas.		

Nota 1 - Le Porteur doit être informé que les informations personnelles d'identité pourront être utilisées comme élément 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.

Nota 2 – Ce dossier d'enregistrement peut être complété, si non complet à l'issue de la phase d'enregistrement, lors de la remise du Certificat (et éventuellement de la bi-clé).

Procédure d'enregistrement du Porteur :

	Niveau (***)	
L'Authentification du Porteur par l'AE est réalisée lors d'un face-à-face physique[8].		

	Niveau (**)	
L'Authentification du Porteur par l'AE est réalisée lors d'un face-à-face physique[9] ou sous forme dématérialisée à condition que la demande soit signée par le Porteur à l'aide d'un procédé de Signature Electronique conforme au minimum aux exigences du niveau (**)[10] décrites dans l'Annexe 1 du Référentiel Certification Electronique et que la Signature soit vérifiée et valide au moment de l'enregistrement.		

	Niveau (*)	
L'Authentification du Porteur peut notamment se faire : - Soit par l'envoi du dossier papier à l'AE accompagné d'une photocopie du document		

[8] Le face-à-face physique peut être réalisé lors de la remise par l'AC au porteur du certificat ainsi que du dispositif de stockage de la bi-clé si et seulement si cette dernière est générée par l'AC. Si tel est le cas, l'AC décrira dans sa PC la façon dont elle s'assure de la fiabilité des informations contenues dans le dossier d'enregistrement du futur porteur. Il est toutefois recommandé de procéder au face-à-face physique dès la phase d'enregistrement.

[9] CF. note de bas de page n° 8.

[10] Il est recommandé que le procédé de signature électronique soit conforme aux exigences du niveau (***) afin que la signature soit présumée fiable.

d'identité du futur Porteur certifiée conforme par lui-même (date, de moins de 3 mois, et Signature du futur Porteur sur la photocopie de ses papiers d'identité, précédées de la mention "copie certifiée conforme à l'original"). - Soit via une demande d'enregistrement dématérialisée signée Electroniquement par le futur Porteur à l'aide d'un procédé de Signature Electronique conforme aux exigences du niveau (*) décrites dans l'Annexe 3 du Référentiel Certification Electronique et que la Signature soit vérifiée et valide au moment de l'enregistrement. - Soit par la communication d'un élément propre au futur Porteur permettant de l'identifier au sein d'une base de données pré-établie.

III.2.4. Informations non vérifiées du Porteur

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

III.2.5. Validation de l'autorité du demandeur

		[Entreprise] / [Administration]
Cette étape est effectuée en même temps que la validation de l'identité de la personne physique (directement par l'AE).		

III.2.6. 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.

III.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 (cf. chapitre IV.6).

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.

III.3.1. Identification et validation pour un renouvellement courant

	Niveau (**) et (***)	
Lors du premier renouvellement, l'AC doit au minimum s'assurer que les informations du dossier d'enregistrement initial sont toujours valides et que le Certificat à renouveler existe, et est toujours valide.		

	Niveau (*)	
Lors du premier renouvellement, la vérification de l'identité du Porteur est optionnelle. Elle est laissée à l'appréciation de l'AC qui engage sa responsabilité quant à la validité des informations contenues dans le Certificat renouvelé.		

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

III.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.

III.4. Identification et validation d'une demande de révocation

	Niveau (***)	
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 (cf. chapitre III.2.3), utilisation d'un identifiant / mot de passe envoyé préalablement au demandeur de façon sécurisée).		

	Niveau (**)	
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 3 ou 4 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).		

	Niveau (*)	

Si la demande de révocation est faite via un Service téléphonique ou via un Service en ligne (serveur web), elle doit faire l'objet d'un minimum d'Authentification : vérification d'une ou deux informations de base du demandeur (adresse, n° de téléphone, etc.) et de son autorité par rapport au Certificat à révoquer.

Une demande de révocation peut également être faite par courrier ou par télécopie. Elle doit alors être signée par le demandeur et le Service de gestion des révocations doit s'assurer de l'identité du demandeur (vérification de la Signature manuscrite par rapport à une Signature préalablement enregistrée) et de son autorité par rapport au Certificat à révoquer.

IV. Exigences opérationnelles sur le cycle de vie des Certificats

IV.1. Demande de Certificat

IV.1.1. Origine d'une demande de Certificat

		[Entreprise] / [Administration]
Un Certificat peut être demandé par un représentant légal de l'entité après consentement préalable du futur Porteur ou après vérification que le futur Porteur a été informé de ses responsabilités et les a accepté au sein d'une attestation personnelle de responsabilité.		
		[**Particulier**]
Un Certificat ne peut être demandé que par le futur Porteur ou par le représentant d'un incapable majeur ou d'un mineur.		

IV.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 (cf. chapitre III.2 ci- dessus) :

- le nom du Porteur à utiliser dans le Certificat (nom réel ou pseudonyme) ;
- les données personnelles d'identification du Porteur[11] ;

		[Entreprise] / [Administration]
les données d'identification de l'entité.		

[11] Afin de pouvoir traiter les cas d'homonymie, le nom et le prénom doivent être complétés par une donnée complémentaire qui permet d'assurer l'unicité des DN durant toute la durée de vie de l'AC.

[Confidentialité]		
Le cas échéant, la demande de Certificat (cf. chapitre III.2 ci-dessus) doit intégrer les informations concernant la demande de séquestre de la clé privée du Porteur correspondant au Certificat sur lequel porte la demande et la durée souhaitée de conservation de la clé privée séquestrée.		

		[Entreprise] / [Administration]
Le dossier de demande est établi soit directement par le futur Porteur à partir des éléments fournis par son entité, soit par son entité et signé par le futur Porteur.		

		[Particulier]
Le dossier de demande est établi par le futur Porteur et transmis à l'AE.		

Par ailleurs, l'AE doit s'assurer de disposer d'une information permettant de contacter le futur Porteur du Certificat.

IV.2. Traitement d'une demande de Certificat

IV.2.1. Exécution des processus d'identification et de validation de la demande

Les identités "personne physique" et, le cas échéant, "personne morale" sont vérifiées conformément aux exigences du chapitre III.2.

L'AE doit effectuer les opérations suivantes :

- valider l'identité du futur Porteur ;
- vérifier la cohérence des justificatifs présentés ;
- vérifier que le futur Porteur a pris connaissance des modalités applicables pour l'utilisation du Certificat. (voir les conditions générales d'utilisation), à moins que cette vérification ne soit effectuée lors de la remise de la carte.

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 (cf. chapitre I.4.1).

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 l'AE, les Signatures étant précédées de la mention "copie certifiée conforme à l'original" ;
- si le dossier est au format Electronique, les différents justificatifs ou les informations de traçabilité (sous une forme Electronique ayant valeur légale.

IV.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le Porteur en justifiant le rejet.

IV.2.3. Durée d'établissement du Certificat

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

IV.3. Délivrance du Certificat

IV.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[12], et, selon les cas, la bi-clé du Porteur, son dispositif de protection des éléments secrets**,** les codes d'activation, etc. (cf. chapitre I.4.1).

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. Par ailleurs, la clé privée doit être transmise de façon sécurisée au Porteur, en en garantissant l'intégrité et la Confidentialité.

Les conditions de génération des clés et des Certificats et les mesures de sécurité à respecter sont précisées aux chapitres V et VI ci-dessous, notamment la séparation des rôles de confiance (cf. chapitre V.2).

IV.3.2. Notification par l'AC de la délivrance du Certificat au Porteur

	Niveau (**) et (***)	
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 (cf. chapitre III.2). Si la remise du Certificat ne se fait pas en mains propres, l'AC précisera dans sa PC comment elle 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,...).		

	Niveau (***)	
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'une application 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		

[12] Si la bi-clé est générée par le Porteur, la clé publique doit être transmise à l'AC.

puce.

	Niveau (*)	
Le Certificat peut-être transmis par message Electronique à une adresse fournie par le Porteur, ou bien l'URL permettant de télécharger le Certificat peut être envoyée à une telle adresse.		

Le Certificat complet et exact doit être mis à la disposition de son Porteur.

Nota – Si la remise du Certificat doit se faire en mains propres auprès de l'AE, le Porteur sera également tributaire des modalités d'accueil de l'AE.

IV.4. Acceptation du Certificat

IV.4.1. Démarche d'acceptation du Certificat

	Niveau (***)	
L'AC doit obtenir confirmation de l'acceptation explicite du Certificat par le Porteur sous la forme d'un accord signé (papier ou Electronique) ou de l'attestation personnelle de responsabilité (cf. IV.1.1). L'AC doit garder une trace de l'acceptation du Certificat par le Porteur.		

	Niveau (**)	
L'AC doit obtenir confirmation de l'acceptation du Certificat par le Porteur, si possible de façon explicite sous la forme d'un accord signé (papier ou Electronique), ou de l'attestation personnelle de responsabilité (cf. IV.1.1). Si la remise du Certificat au Porteur peut faire l'objet d'une date connue avec un degré suffisant de certitude, l'AC peut s'appuyer sur un mécanisme d'acceptation tacite du Certificat moyennant un délai maximum laissé au Porteur, à compter de la date de réception de son Certificat, pour signaler sa non-acceptation du Certificat. La première utilisation du Certificat peut également valoir acceptation tacite. Dans le cas d'une acceptation tacite, les obligations du Porteur et le délai correspondant doivent être clairement mentionnés dans la PC de l'AC ainsi que dans les conditions générales d'utilisation (cf. chapitre II.2) et/ou le contrat Porteur. L'AC doit garder une trace de l'acceptation du Certificat par le Porteur si celle-ci est explicite.		

	Niveau (*)	
L'acceptation peut être tacite à compter de la date d'envoi du Certificat (ou des informations de téléchargement) au Porteur. Le processus d'acceptation du Certificat et les obligations correspondantes du Porteur doivent être clairement mentionnés dans la PC de l'AC ainsi que		

dans les conditions générales d'utilisation (cf. chapitre II.2) et/ou le contrat Porteur.

IV.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 l'AC 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.

IV.4.3. Notification par l'AC aux autres entités de la délivrance du Certificat

L'AC informe l'AE de la délivrance du Certificat.

IV.5. Usages de la bi-clé et du Certificat

IV.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 à la fonction de sécurité concernée (cf. chapitre I.5.1.1). 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 usages des clés. Cet usage doit également être clairement explicité dans la PC de l'AC, ainsi que dans les conditions générales d'utilisation et/ou le contrat Porteur. Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du Porteur par l'AC avant d'entrer en relation contractuelle.

IV.5.2. Utilisation de la clé publique et du Certificat par l'Utilisateur du Certificat

Cf. chapitre précédent et chapitre I.5.

Les Utilisateurs de Certificats doivent respecter strictement les usages autorisés des Certificats. Toute utilisation en dehors de l'usage normal du Certificat relève de la responsabilité du porteur.

IV.6. Renouvellement d'un Certificat

Conformément au [RFC3647], la notion de "renouvellement de Certificat" correspond à la délivrance d'un nouveau Certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au Certificat précédent (y compris la clé publique du Porteur).

Dans la cadre de la présente PC Type, il ne peut pas y avoir de renouvellement de Certificat sans renouvellement de la bi-clé correspondante. Aussi, si c'est l'AC qui génère les bi-clés des Porteurs, elle doit garantir qu'un Certificat correspondant à une bi-clé existante ne peut pas être renouvelé au sens du [RFC3647]. Dans le cas contraire, elle doit s'en assurer

auprès du Porteur, au minimum au travers d'un engagement contractuel clair et explicite du Porteur vis-à-vis de l'AC.

IV.7. Délivrance d'un nouveau Certificat suite à changement de la bi-clé

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

IV.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 à une fréquence conforme au tableau suivant :

Description	**Niveau ***	**Niveau ****	**Niveau *****
Durée de vie maximale d'une bi-clé et d'un Certificat Porteur : Particulier	5 ans 3 ans	5 ans 3 ans	5 ans 3 ans

Par ailleurs, une bi-clé et un Certificat peuvent être renouvelés par anticipation, suite à la révocation du Certificat du Porteur (cf. chapitre IV.9, notamment le chapitre IV.9.1.1 pour les différentes causes possibles de révocation).

Nota - 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.

IV.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.

[ENTREPRISE] [ADMINISTRATION] L'entité peut également être à l'initiative d'une demande de fourniture d'un nouveau Certificat pour un Porteur qui lui est rattaché.

IV.7.3. Procédure de traitement d'une demande d'un nouveau Certificat

L'identification et la validation d'une demande de fourniture d'un nouveau Certificat sont précisées au chapitre III.3 ci-dessus.

Pour les actions de l'AC, cf. chapitre IV.3.1.

IV.7.4. Notification au Porteur de l'établissement du nouveau Certificat

Cf. chapitre IV.3.2.

IV.7.5. Démarche d'acceptation du nouveau Certificat

Cf. chapitre IV.4.1.

IV.7.6. Publication du nouveau Certificat

Cf. chapitre IV.4.2.

IV.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau Certificat

IV.8. Modification du Certificat

Conformément au [RFC3647], la modification d'un Certificat correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre IV.7) et autres qu'uniquement la modification des dates de validité (cf. chapitre IV.6).

La modification de Certificat n'est pas recommandée dans la présente PC Type. Toutefois, si elle est mise en œuvre, elle doit modifier le numéro de série du Certificat, révoquer le Certificat initial et ne concerner que les Certificats d'Utilisateurs finaux.

IV.9. Révocation et suspension des Certificats

IV.9.1. Causes possibles d'une révocation

IV.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 (par exemple changement du nom de famille suite à un mariage), ceci avant l'expiration normale du Certificat ;
- le Porteur n'a pas respecté les modalités applicables d'utilisation du Certificat ;
- le Porteur et/ou l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du Porteur ;
- la clé privée du Porteur est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- le Porteur ou une entité autorisée (représentant légal de l'entité) demande la révocation du Certificat (notamment dans le cas d'une destruction ou altération de la clé privée du Porteur et/ou de son support) ;
- le décès du Porteur ou la cessation d'activité de l'entité du Porteur.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau Certificat notamment), le Certificat concerné doit être révoqué.

IV.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.

IV.9.2. Origine d'une demande de révocation

IV.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 ;
- l'AC émettrice du Certificat ou l'une de ses composantes (AE) ;

		[Entreprise] / [Administration]
un représentant légal de l'entité.		

Nota : Le Porteur doit être informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son Certificat.

IV.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.

IV.9.3. Procédure de traitement d'une demande de révocation

IV.9.3.1. Révocation d'un Certificat de Porteur

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre III.4.

L'AC 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 (n° de série,...) ;
- 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 selon l'une des solutions suivantes :

- via une LCR signée par l'AC elle-même soit par une entité désignée par l'AC ;
- via un Service OCSP dont la réponse est soit signée par le Certificat de l'AC ayant émis le Certificat à révoquer ou par un Certificat de répondeur OCSP lui-même signé par l'AC ayant émis le Certificat à révoquer (cf. chapitre IV.9.9).

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.

IV.9.3.2. Révocation d'un Certificat d'une composante de l'IGC

L'AC 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, l'AC 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. 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 obligatoire que le Certificat associé à la clé de l'AC signant les Certificats Porteurs soit signé par une autre AC et ne soit pas autosigné.

IV.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.

IV.9.5. Délai de traitement par l'AC d'une demande de révocation

IV.9.5.1. *Révocation d'un Certificat de Porteur*

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

IV.9.5.2. *Disponibilité du système de traitement des demandes de révocation*

La fonction de gestion des révocations doit être disponible aux heures ouvrées au niveau * et

24h/24 et 7j/7 aux niveaux ** et ***. Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de Service (panne ou maintenance) conforme au tableau suivant :

Description	**Niveau ***	**Niveau ****	**Niveau *****
Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations	2h (jours ouvrées)	2h	1h

Cette fonction doit avoir une durée maximale totale d'indisponibilité par mois conforme au tableau suivant :

Description	**Niveau ***	**Niveau ****	**Niveau *****
Durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations	16h (jours ouvrées)	8h	4h

Toute demande de révocation d'un Certificat Porteur doit être traitée dans un délai inférieur à 72h pour un niveau * et inférieur à 24h pour les niveaux ** et ***. 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.

IV.9.5.3. *Révocation d'un Certificat d'une composante de l'IGC*

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

La révocation d'un Certificat de Signature de l'AC (Signature de Certificats, de LCR / LAR ou de réponse OCSP) doit être effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

IV.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, Delta LCR, OCSP…) est à l'appréciation de l'Utilisateur selon leur disponibilité et les contraintes liées à leur emploi.

IV.9.7. Fréquence d'établissement et durée de validité des LCR

Lorsque l'information sur l'état de la révocation d'un Certificat est assurée au travers de la mise en place d'un Service de LCR et, le cas échéant, de Delta LCR, la fréquence minimale de leur publication doit être de 72h pour le niveau * et 24h pour les niveaux ** et ***.

Afin d'assurer une continuité du Service dans le cas où un incident sur la publication des LCR survienne, il est recommandé que la durée de validité des LCR (et dLCR) soit le double de leur fréquence de publication. En aucun cas elle ne pourra excéder 6 jours.

Une liste de Certificats d'autorités révoqués (LAR) est une LCR qui ne contient que des numéros de Certificats d'AC. Les LAR émises par une AC racine doivent avoir une durée dictée par l'analyse de risque (s'il y en a une). Sa durée doit être au maximum d'un an ; il est recommandé, dans la plupart des cas, qu'elle soit mensuelle.

La fréquence de publication de nouvelles LAR doit être cohérente avec la durée de ces LAR (si la durée de validité d'une LAR est de 1 mois, l'émission d'une nouvelle LAR toutes les trois semaines est une fréquence adaptée).

IV.9.8. Délai maximum de publication d'une LCR

Lorsque l'information sur l'état de la révocation d'un Certificat est assurée au travers de la mise en place d'un Service de publication de LCR et, le cas échéant, de Delta LCR, celles-ci doivent être publiées et disponibles pour le téléchargement au maximum dans les 30 minutes suivant leur génération.

Le délai de publication des LAR devra être précisé dans la PC de l'AC racine.

IV.9.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des Certificats

Lorsque l'information sur l'état de la révocation d'un Certificat est assurée au travers de la mise en place d'un Service OCSP, celui-ci doit respecter les exigences d'intégrité, de disponibilité et de délai de publication décrites dans cette PC Type.

IV.9.10. Exigences de vérification en ligne de la révocation des Certificats par les Utilisateurs de Certificats

Cf. chapitre IV.9.6 ci-dessus.

IV.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.

À préciser par l'AC dans sa PC.

IV.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 sans délais après avoir eu connaissance de la compromission de la clé privée.

Pour les Certificats d'AC, outre les exigences du chapitre IV.9.3 ci-dessus, 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 de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

[Authentification]/[Signature]	**Niveau (***)**	
L'AC doit imposer au Porteur qu'en cas de compromission de la clé privée du Porteur ou de connaissance de la compromission de la clé privée de l'AC ayant émis son Certificat, le Porteur s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son Certificat associé.		

[Confidentialité]	**Niveau (***)**	
L'AC doit imposer au Porteur qu'en cas de compromission de la clé privée du Porteur, le Porteur s'oblige à interrompre immédiatement et définitivement l'usage de son Certificat de Confidentialité à des fins de Chiffrement. Le Porteur s'engage, dans la mesure des moyens disponibles, à déchiffrer les données précédemment chiffrées au moyen de son Certificat de Confidentialité. Le Porteur s'oblige à protéger ces données par tout autre moyen apte à répondre au besoin de Confidentialité identifié pour le niveau de sécurité considéré.		

IV.9.13. Causes possibles d'une suspension

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

IV.10. Fonction d'information sur l'état des Certificats

IV.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 ou des jetons OCSP 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 une solution : LCR ou OCSP.

Lorsqu'un Service de LCR / LAR est proposé, alors celles-ci doivent être au format V2.

IV.10.2. Disponibilité de la fonction d'information sur l'état des Certificats

La fonction d'information sur l'état des Certificats doit être disponible 24h/24 7j/7.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de Service (panne ou maintenance) conforme au tableau suivant :

Description	**Niveau ***	**Niveau ****	**Niveau *****
Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des Certificats	4h (jours ouvrés)	4h	2h[13]

Cette fonction doit avoir une durée maximale totale d'indisponibilité par mois conforme au tableau suivant :

Description	**Niveau ***	**Niveau ****	**Niveau *****
Durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des Certificats	32h (jours ouvrés)	16h	8h

Lorsque la fonction de vérification en ligne du statut d'un Certificat (OCSP) est mise en œuvre, le temps de réponse du serveur à la requête reçue[14] doit être au maximum de 10 secondes.

IV.10.3. Dispositifs optionnels

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

IV.11.Fin de la relation entre le Porteur et l'AC

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

IV.12. Séquestre de clé et recouvrement

Seules les clés privées associées aux Certificats Electroniques dont l'usage est la Confidentialité

[13] Il est recommandé que cette durée soit de 1h lorsque le PSCE délivre des certificats d'authentification (personne ou machine), chiffrement et de cachet à des fins de signature de contremarques de temps.

[14] Durée mesurée au niveau du serveur (requête reçue par le serveur et réponse au départ du serveur.

(Chiffrement) peuvent être séquestrées à des fins de recouvrement. Les clés privées d'AC et les clés privées associées aux Certificats Electroniques des autres usages ne doivent en aucun cas être séquestrées.

[Confidentialité]		
Afin de mettre en œuvre un mécanisme permettant de déchiffrer des informations, préalablement chiffrées, en l'absence de la clé privée d'origine du Porteur concerné (absence du Porteur, perte de sa clé privée par le Porteur, panne de son dispositif de protection de clés privées, …), plusieurs solutions sont envisageables : chiffrer systématiquement les clés symétriques de fichiers ou de messages en utilisant, en plus des clés publiques des Porteurs concernés, la clé publique d'un agent de recouvrement qui pourra, en cas de besoin, utiliser sa clé privée pour effectuer le Déchiffrement ; séquestrer les clés privées des Porteurs, et les recouvrer, au cas par cas, lorsque nécessaire. Il est hors du cadre du présent document de traiter des avantages et inconvénients des solutions permettant de déchiffrer un fichier ou un message en l'absence de la clé privée d'origine du Porteur. De plus, la présente PC Type ne traite que du recouvrement de données chiffrées suite à séquestre des clés privées de Déchiffrement des Porteurs. Le recouvrement de données chiffrées via la clé privée d'un agent de recouvrement est du ressort de l'application et de sa Politique de sécurité et est hors du cadre de la présente PC Type. Le séquestre des clés privées de Déchiffrement du Porteur par l'AC n'est pas imposé par des obligations légales. Il est cependant fortement conseillé aux AC d'offrir ce Service de séquestre à leurs clients pour des raisons de disponibilité et d'accès aux données chiffrées. En effet, en cas de perte de sa clé privée, le Porteur sera ainsi en mesure de déchiffrer la clé symétrique de fichier ou de message et de déchiffrer les données qu'il avait protégées en Confidentialité. Enfin, cette PC Type ne traite que du séquestre et du recouvrement de clés privées correspondant à des Certificats émis par l'AC elle-même en conformité avec cette même PC Type. Un Service de séquestre et de recouvrement autonome est hors du cadre de la présente PC Type.		

IV.12.1. Politique et pratiques de recouvrement par séquestre des clés

Les différentes étapes de séquestre et de recouvrement de clés privées associées aux Certificats Electroniques dont l'usage est la Confidentialité (Chiffrement) doivent respecter les exigences des chapitres qui suivent

IV.12.1.1. Demande de séquestre

[Confidentialité]		

Une demande de séquestre de clé privée est effectuée, auprès de l'AE, en même temps que la demande du Certificat correspondant et par la même personne. Cette demande doit comporter la durée souhaitée de conservation de la clé privée séquestrée, en fonction de la durée maximale pouvant être offerte par l'AC qui doit être au moins égale à la durée de validité du Certificat correspondant.

[Confidentialité]		**[Entreprise]/ administration]**
Si le demandeur n'est pas le futur Porteur, ce dernier doit en être informé et donner son consentement préalable.		

IV.12.1.2. Traitement d'une demande de séquestre

[Confidentialité]		

Une demande de séquestre d'une clé privée étant formulée en même temps et par la même personne que la demande de Certificat correspondant, le processus d'identification et de validation d'une telle demande correspond à celui d'une demande de Certificat (cf. chapitre IV.2.1).

L'AE transmet ensuite la demande de séquestre à la fonction adéquate de l'IGC (cf. chapitre I.4.1).

Les demandes de séquestre sont à archiver par l'AE au même titre que les dossiers d'enregistrement correspondants (cf. chapitre I.4.2).

Si l'AC génère la bi-clé du Porteur, la fonction de génération des éléments secrets du Porteur, suite à génération de la clé privée à séquestrer, la transmet à la fonction de séquestre et recouvrement suivant un processus qui doit en assurer, de bout en bout, la Confidentialité, l'intégrité et l'Authentification d'origine.

Si la clé privée n'est pas générée par l'AC mais par le Porteur, elle doit être remise à la fonction de séquestre et recouvrement de l'AC suivant un processus qui permet d'en assurer, de bout en bout, la Confidentialité, l'intégrité et l'Authentification d'origine.

L'intégrité et la Confidentialité des clés privées séquestrées doivent être assurées en permanence, y compris lors d'éventuels échanges internes à l'IGC. La conservation de ces clés doit se faire soit dans un module cryptographique, soit sous forme chiffrée, suivant les mêmes conditions que celles définies au chapitre VI.2.4 pour la conservation des copies de secours des clés d'AC. Les mécanismes assurant la sécurité des clés séquestrées doivent être adaptés à la durée de conservation de ces clés.

L'AC devra préciser dans sa PC quelles sont les informations permettant d'identifier de manière unique et non ambiguë chaque clé privée séquestrée (en s'appuyant, par exemple, sur le DN du Porteur, le n° de série du Certificat correspondant et/ou un n° de série propre à la clé privée). Un Porteur pouvant disposer de plusieurs clés privées, à un instant donné ainsi que suite aux renouvellements successifs de ses bi-clés, une identification reposant uniquement sur l'identification du Porteur est a priori insuffisante.

Au plus tard au moment du séquestre effectif de la clé privée concernée, l'AC doit transmettre à toute personne autorisée à demander ultérieurement le recouvrement de cette clé (cf. chapitre suivant), et dont il a connaissance à ce moment-là, ces informations d'identification de la clé privée séquestrée et qui devront être mentionnées dans toute demande de recouvrement.

IV.12.1.3. Origine d'une demande de recouvrement

[Confidentialité]		**[Particulier]**

Outre le Porteur lui-même et les entités autorisées par la loi à accéder aux clés privées séquestrées par une AC, seules les personnes explicitement désignée à l'AC par le Porteur, éventuellement sous conditions (par exemple, en cas de décès du Porteur), peuvent demander le recouvrement d'une clé privée d'un Porteur donné.

[Confidentialité]		**[Entreprise]/**
Outre le Porteur lui-même et les entités autorisées par la loi à accéder aux clés privées séquestrées par une AC, seules le représentant légal de l'entité ou toute personne explicitement désignée par un représentant légal de l'entité, cette personne pouvant être désignée nominativement ou par sa fonction, peuvent demander le recouvrement d'une clé privée d'un Porteur donné.		

IV.12.1.4. Identification et validation d'une demande de recouvrement

[Confidentialité]		
L'identité du demandeur d'un recouvrement d'une clé séquestrée doit être validée, sauf cas particulier des entités autorisées par la loi, par la fonction de gestion des recouvrements suivant les mêmes exigences que la validation initiale de l'identité d'un demandeur d'un Certificat définies au chapitre III.2. La demande de recouvrement doit comporter au minimum les informations suivantes : le motif du recouvrement de la clé privée ainsi que les informations permettant d'identifier la clé privée à recouvrer (cf. chapitre IV.12.1.2). Une fois l'identité du demandeur validée et la clé à recouvrer identifiée, la fonction de gestion des recouvrements s'assure que le demandeur est bien l'une des personnes autorisées à demander le recouvrement de la clé concernée.		

IV.12.1.5. Traitement d'une demande de recouvrement

[Confidentialité]		
Suite à identification et validation de la demande de recouvrement (cf. chapitre précédent), la fonction de gestion des recouvrements émet la demande pour effectuer le recouvrement de la clé privée concernée vers la fonction de séquestre et recouvrement de l'IGC, en protégeant cette demande en intégrité et en Confidentialité. La fonction de séquestre et recouvrement authentifie la demande de recouvrement puis saisit les personnes nécessaires pour le recouvrement de la clé privée du Porteur. La fonction de séquestre et recouvrement authentifie ces personnes préalablement à l'opération de recouvrement.		

[Confidentialité]	Niveaux (**) et (***)	
L'opération de recouvrement doit nécessiter l'Authentification d'au moins deux personnes dans des rôles de confiance (par exemple, responsable sécurité et opérateur).		
[Confidentialité]	**Niveau (*)**	
L'opération de recouvrement doit nécessiter l'Authentification d'au moins une personne dans un rôle de confiance.		

[Confidentialité]		
L'opération de recouvrement doit garantir qu'aucune autre information, que la clé privée sur laquelle porte le recouvrement, ne peut être divulguée. La fonction de séquestre et recouvrement remet ensuite de manière sécurisée la clé privée recouvrée au demandeur du recouvrement. Cette remise s'effectue avec une sécurité équivalente à la remise de la clé privée lors de la génération du Certificat du Porteur (cf. chapitres VI.1.2 et VI.4). La fonction de gestion des recouvrements a la responsabilité de l'archivage des pièces du dossier de demande de recouvrement (ou de l'envoi vers la composante chargée de l'archivage), l'archivage des informations liées à l'opération de recouvrement étant du ressort de la fonction de séquestre et recouvrement au titre de l'archivage des journaux d'évènements correspondants (cf. chapitres V.4 et V.5).		

IV.12.1.6. Destruction des clés séquestrées

[Confidentialité]		
Dès la fin de la période de conservation d'une clé séquestrée, tout exemplaire de cette clé détenue par l'AC doit être détruit de manière fiable afin de ne pouvoir ni recouvrer ni reconstituer la clé.		

IV.12.1.7. Disponibilité des fonctions liées au séquestre et au recouvrement

[Confidentialité]		

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

L'AC doit préciser dans sa PC ses engagements quant à la disponibilité de sa fonction de gestion des recouvrements et de sa fonction de séquestre et recouvrement. Elle doit également préciser ses engagements en matière de délai de traitement maximal d'une demande de recouvrement, entre la réception d'une demande de recouvrement authentifiée et la remise de la clé privée recouvrée au demandeur.

IV.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

V.Mesures de sécurité non techniques

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.

V.1. Mesures de sécurité physique

V.1.1. Situation géographique et construction des sites

La présente PC Type ne formule pas d'exigence spécifique concernant la localisation géographique de l'IGC et de ses composantes.

La construction des sites doit respecter les règlements et normes en vigueur ainsi qu'éventuellement 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,...).

V.1.2. Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des Services de l'AC, les accès aux locaux des différentes composantes de l'IGC doivent être contrôlés.

En outre, toute personne entrant dans ces zones physiquement sécurisées ne doit pas être laissée, pendant une période de temps significative, sans la surveillance d'une personne autorisée.

	Niveau (***)	

Pour les fonctions de génération des Certificats, de génération des éléments secrets du Porteur et de gestion des révocations et, le cas échéant, pour les fonctions de gestion des recouvrements et de séquestre et recouvrement :

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 de l'AC, 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.

	Niveau (**)	
Pour les fonctions de génération des Certificats, de génération des éléments secrets du Porteur et de gestion des révocations et, le cas échéant, pour les fonctions de gestion des recouvrements et de séquestre et recouvrement : L'accès doit être strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique Afin d'assurer la disponibilité des systèmes, il est recommandé que l'accès aux machines soit limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.		

Nota - 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.

V.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 l'AC 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.

V.I.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 l'AC 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.

V.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 l'AC 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.

V.1.6. Conservation des supports

Les différentes informations intervenant dans les activités de l'IGC doivent être identifiées et leurs besoins de sécurité définis (en Confidentialité, intégrité et disponibilité). L'AC doit maintenir un inventaire de ces informations. L'AC doit mettre en place des mesures pour éviter la compromission et le vol de ces informations.

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations doivent être gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils doivent être manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.

Des procédures de gestion doivent protéger ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

V.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.

V.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 de l'AC dans sa PC en matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des Certificats (cf. chapitres IV.9.5.1 et IV.10.2).

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.

	Niveaux (**) et (***)	
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 évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.). Les fonctions de sauvegarde et de restauration doivent être effectuées par les rôles de confiance appropriés et conformément aux mesures de sécurité procédurales.		

V.2. Mesures de sécurité procédurales

V.2.1. Rôles de confiance

Chaque composante de l'IGC doit distinguer au moins les cinq rôles fonctionnels[15] de confiance suivants :

- **Responsable de sécurité** - Le responsable de sécurité est chargé de la mise en œuvre et du contrôle de la Politique de sécurité d'une ou plusieurs composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et des journaux d'évènements. Il est responsable des opérations de génération et de révocation des Certificats.
- **Responsable d'application** - Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la Politique de Certification et de la déclaration des pratiques de Certification de l'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 au quotidien des applications pour les fonctions mises en œuvre par la composante.
- **Contrôleur** - Personne autorisée à accéder et en charge de l'analyse régulière des archives et de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

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, l'AC peut être amenée à distinguer également en tant que rôle de confiance, les rôles de Porteur de parts de secrets d'IGC : cf. chapitre VI.1.

[15] En fonction de la taille de l'entité concernée, de la charge de travail correspondant au rôle, etc., ainsi qu'en fonction des exigences de sécurité et de continuité d'activité, un même rôle fonctionnel peut / doit être tenu par différentes personnes.

Ces Porteurs de parts de secrets ont la responsabilité d'assurer la Confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiés.

De manière générale, des procédures doivent être établies et appliquées pour tous les rôles et les rôles de confiance ayant trait à la fourniture de Services de Certification.

Ces rôles doivent être décrits et définis dans la description des postes propre à chaque entité opérant une des composantes de l'IGC sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles doivent déterminer la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilisation des employés.

Lorsqu'appropriées, ces descriptions doivent différencier entre les fonctions générales et les fonctions spécifiques à l'AC. L'AC doit implémenter techniquement ce principe de moindre privilège via les mécanismes de contrôle d'accès qu'elle met en œuvre.

De plus, les opérations de sécurité de l'AC doivent être séparées des opérations normales. Les responsabilités des opérations de sécurité incluent :

- les procédures et responsabilités opérationnelles ;
- la planification et la validation des systèmes sécurisés ;
- la protection contre les logiciels malicieux ;
- l'entretien ;
- la gestion de réseaux ;
- la surveillance active des journaux d'audit, l'analyse des évènements et les suites ;
- la manipulation et la sécurité des supports ;
- l'échange de données et de logiciels.

Ces responsabilités sont gérées par les opérations de sécurité de l'AC, mais peuvent être effectivement réalisées par du personnel opérationnel non spécialiste (en étant supervisé), tel que défini dans la Politique de sécurité appropriée et les documents relatifs aux rôles et responsabilités.

Des mesures doivent être mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux Services de l'AC soient sortis du site sans autorisation.

V.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 (cf. chapitre VI).

La DPC de l'AC devra préciser 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.).

V.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 de l'AC 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. Ce rôle doit être clairement mentionné et décrit dans sa fiche de poste.

V.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 de l'AC et être conformes à la Politique de sécurité de la composante concernée.

	Niveaux (**) et (***)	
Concernant les rôles de confiance, les cumuls suivants sont interdits : - responsable de sécurité et ingénieur système / opérateur / contrôleur ; - ingénieur système, opérateur et contrôleur.		

	Niveau (*)	
Concernant les rôles de confiance, le cumul suivant est interdit : responsable de sécurité et ingénieur système.		

V.3. Mesures de sécurité vis-à-vis du personnel

V.3.1. Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC doivent être soumis à une clause de Confidentialité vis-à-vis de leur employeur.

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, auxquelles elle doit se conformer.

En particulier, les personnes intervenant dans des rôles de confiance doivent y être formellement affectées par l'encadrement supérieur chargé de la sécurité.

V.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.

A ce titre, l'employeur peut demander à ces personnels la communication d'une copie de leur casier judiciaire.

L'employeur peut décider en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions du personnel, de lui retirer ces attributions.

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).

V.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.

V.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.

V.3.5. Fréquence et séquence de rotation entre différentes attributions

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

V.3.6. Sanctions en cas d'actions non autorisées

À préciser par l'AC dans sa DPC.

V.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 V.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces Prestataires.

V.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. En particulier, il doit lui être remis la ou les Politique(s) de sécurité l'impactant.

V.4. Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer de façon manuelle ou automatique. Les fichiers résultants, sous forme papier ou Electronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

V.4.1. Type d'évènements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre de l'IGC, chaque entité opérant une composante de l'IGC doit au minimum journaliser les évènements tels que décrits ci-dessous, sous forme Electronique. La journalisation doit être automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

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

D'autres évènements doivent aussi être recueillis, par des moyens Electroniques 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[16] :

- réception d'une demande de Certificat (initiale et renouvellement) ;
- validation / rejet d'une demande de Certificat ;
- évènements liés aux clés de Signature et aux Certificats d'AC (génération (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 protection des éléments secrets 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 des delta LCR) ou des, requêtes / réponses OCSP**.**

[Confidentialité]		
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[17] : le cas échéant, séquestre d'une clé privée de Porteur ; réception d'une demande de recouvrement ; validation / rejet d'une demande de recouvrement ; recouvrement d'une clé privée ; remise d'une clé privée recouvrée au demandeur du recouvrement/A6].		

[16] Les évènements à journaliser doivent être adaptés à l'organisation et l'architecture de l'IGC. Notamment, les échanges entre fonctions de l'IGC et/ou entre composantes de l'IGC peuvent nécessiter une journalisation pour assurer une traçabilité des actions.

[17] Les évènements à journaliser doivent être adaptés à l'organisation et l'architecture de l'IGC. Notamment, les échanges entre fonctions de l'IGC et/ou entre composantes de l'IGC peuvent nécessiter une

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

- type de l'évènement ;
- nom de l'exécutant ou référence du système déclenchant l'évènement ;
- date et heure de l'évènement (l'heure exacte des évènements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de Certificat doit être enregistrée) ;
- 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.

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

- destinataire de l'opération ;
- nom du demandeur de l'opération ou référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'évènement ;
- toute information caractérisant l'évènement (par exemple, pour la génération d'un Certificat, le numéro de série de ce Certificat).

Les opérations de journalisation 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.

Les évènements et données spécifiques à journaliser doivent être documentés par l'AC.

V.4.2. Fréquence de traitement des journaux d'évènements

Cf. chapitre V.4.8 ci-dessous.

V.4.3. Période de conservation des journaux d'évènements

Les journaux d'évènements doivent être conservés sur site pendant au moins un (1) mois. Ils doivent être archivés le plus rapidement possible après leur génération et au plus tard sous un (1) mois (recouvrement possible entre la période de conservation sur site et la période d'archivage).

V.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

---

journalisation pour assurer une traçabilité des actions.

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).

Le système de datation des évènements doit respecter les exigences du chapitre VI.8.

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.

V.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.

V.4.6. Système de collecte des journaux d'évènements

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

V.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.

V.4.8. Évaluation 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 une (1) fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux doivent être analysés dans leur totalité au minimum selon la fréquence suivante :

Description	**Niveau ***	**Niveau ****	**Niveau *****
Fréquence d'analyse complète des journaux d'évènements	1 fois toutes les 2 semaines et dès la détection d'une anomalie	1 fois par semaine et dès la détection d'une anomalie	1 fois par jour ouvré et dès la détection d'une anomalie

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 celle déterminée dans le tableau suivant, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

Description	**Niveau ***	**Niveau ****	**Niveau *****
Fréquence de rapprochement des journaux d'évènements	1 fois par mois		1 fois par semaine

V.5. Archivage des données

V.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 conditions générales d'utilisation ;
- les accords contractuels avec d'autres AC ;
- les Certificats, LCR ou réponses OCSP 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.

V.5.2. Période de conservation des archives

V.5.2.1. Dossiers de demande de Certificat

Tout dossier de demande de Certificat accepté doit être archivé aussi longtemps que nécessaire, et pendant au moins sept (7) ans, pour les besoins de fourniture de la preuve de la Certification dans des procédures légales, conformément à la loi applicable.

Les facteurs à prendre en compte dans la détermination de la "loi applicable" sont la loi du pays dans lequel l'AC est établie.

Lorsque les Porteurs sont enregistrés par une autorité d'enregistrement dans un autre pays que celui ou l'AC est établie, alors il convient que cette AE applique également la réglementation de son propre pays.

La durée de conservation des dossiers d'enregistrement doit être portée à la connaissance du 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 TC, doit permettre de retrouver l'identité réelle des personnes physiques désignées dans le Certificat émis par l'AC.

[Confidentialité]		
Tout dossier de demande de recouvrement accepté doit être archivé pendant au moins cinq ans, comptés à partir de la fin du séquestre par l'AC de la clé privée correspondante. Au cours de cette durée d'opposabilité des documents, le dossier de demande de recouvrement doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées. Ce dossier doit permettre de retrouver l'identité réelle de la personne physique ayant demandé et obtenu le recouvrement.		

V.5.2.2. Certificats, LCR et réponses OCSP 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 (5) années après leur expiration.

Les réponses OCSP produites doivent être archivées pendant au moins trois mois après leur expiration.

V.5.2.3. Journaux d'évènements

Les journaux d'évènements traités au chapitre V.4 seront archivés pendant sept (7) années 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.

V.5.2.4. Autres journaux

Pour l'archivage des journaux autres que les journaux d'évènements traités au chapitre V.4, aucune exigence n'est stipulée. L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver ces journaux.

V.5.3. Protection des archives

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

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

L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver les pièces en toute sécurité.

V.5.4. Procédure de sauvegarde des archives

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

V.5.5. Exigences d'Horodatage des données

Cf. chapitre V.4.4 pour la datation des journaux d'évènements.

Le chapitre [VI.8] précise les exigences en matière de datation / Horodatage.

V.5.6. Système de collecte des archives

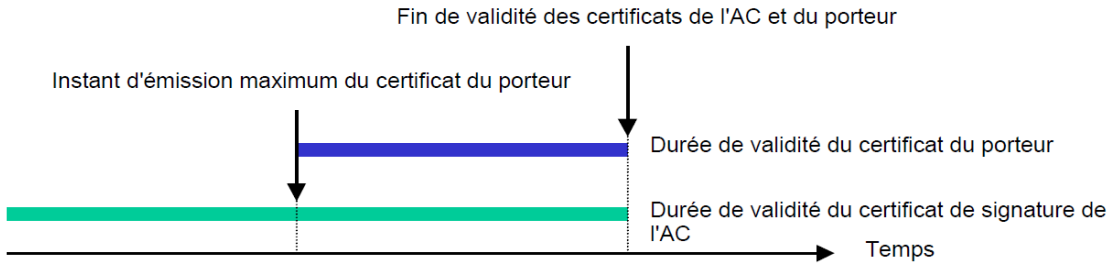
La présente PC Type ne formule pas d'exigence spécifique sur le sujet, si ce n'est que le système de collecte des archives, qu'il soit interne ou externe, doit respecter les exigences de protection des archives concernées.

V.5.7. Procédures de récupération et de vérification des archives

Les archives (papier et Electroniques) doivent pouvoir être récupérées dans un délai inférieur à deux (2) jours ouvrés, 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).

V.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 jusqu'à ce que tous les Certificats signés avec la clé privée correspondante aient expiré**.**

V.7. Reprise suite à compromission et sinistre

V.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. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

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 devra prévenir sans délai l'Autorité de Certification Togolaise.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses Porteurs devient insuffisant pour son utilisation prévue restante, alors l'AC doit :

- informer tous les Porteurs et les tiers Utilisateurs de Certificats avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres Utilisateurs de Certificats ;
- révoquer tout Certificat concerné.

V.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 de l'AC dans sa propre PC 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 ci-dessous :

V.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 en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le Certificat correspondant doit être immédiatement révoqué : cf. chapitre IV.9.

En outre, l'AC doit au minimum respecter les engagements suivants :

- informer les entités suivantes de la compromission : tous les Porteurs et les autres entités avec lesquelles l'AC a passé des accords ou a d'autres formes de relations établies, parmi lesquelles des tiers Utilisateurs et d'autres AC. En complément, cette

information doit être mise à disposition des autres tiers Utilisateurs ;

- indiquer que les Certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

V.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 de l'AC.

V.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 pour des raisons diverses.

L'AC doit prendre les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

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.

V.8.1. Transfert d'activité ou cessation d'activité[18] affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC 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, archivage de séquestre le cas échéant).

2- Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication de l'état des Certificats), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC Type. À défaut, les applications de l'Administration refuseront les Certificats émis par des AC dont les informations sur l'état de révocation des Certificats 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 l'AC dans sa PC :

1- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les

[18] Cessation d'activité d'une composante autre que l'AC.

engagements vis-à-vis des Porteurs ou des Utilisateurs de Certificats, l'AC doit les en aviser aussitôt que nécessaire et, au moins, sous le délai d'un (1) mois.

2- L'AC doit communiquer à l'Autorité de Certification Togolaise 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. Elle 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. L'AC devra communiquer à l'Autorité de Certification Togolaise, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle 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- L'AC doit tenir informée l'Autorité de Certification Togolaise de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus.

V.8.2. 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 l'AC, 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, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des Certificats et la publication des LCR conformément aux engagements pris dans sa PC.

L'AC doit stipuler dans ses pratiques les dispositions prises en cas de cessation de Service. Elles doivent inclure :

- la notification des entités affectées ;
- le transfert de ses obligations à d'autres parties ;
- la gestion du statut de révocation pour les Certificats non-expirés qui ont été délivrés.

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 Porteurs des Certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre III.2.3).

VI. Mesures de sécurité techniques

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.

VI.1. Génération et installation de bi-clés

VI.1.1. Génération des bi-clés

VI.1.1.1. Clés d'AC

La génération des clés de Signature d'AC doit être effectuée dans un environnement sécurisé (cf. chapitre V).

Les clés de Signature d'AC doivent être générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous pour le 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 (cf. chapitre V.2.1), dans le cadre de "cérémonies de clés". Ces cérémonies doivent se dérouler suivant des scripts préalablement définis.

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. Ce dernier peut le cas échéant, en accord avec le responsable de l'IGC, notamment en cas d'indisponibilité au moment où la cérémonie ce clé doit être opérée, transférer temporairement ou définitivement cette part de secret à un personnel désigné.

	Niveau (***)	

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.

	Niveau (**)	
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 un est externe à l'AC et est impartial. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.		

	Niveau (*)	
Les cérémonies de clés doivent se dérouler sous le contrôle d'au moins une personne ayant au moins un rôle de confiance et en présence de plusieurs témoins. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.		

VI.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 (cf. chapitre V).

Les bi-clés des Porteurs doivent être générées :

- soit directement dans le dispositif de protection des éléments secrets destiné au Porteur conforme aux exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré,
- soit dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré, puis transférées de manière sécurisée dans le dispositif de protection des éléments secrets destiné au Porteur.

[Confidentialité]		
Dans ce dernier cas, un séquestre de la bi-clé peut être généré par l'AC conformément à sa PC et à sa DPC.		

VI.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 chapitre XII ci-dessous pour le niveau de sécurité considéré. L'AC doit s'assurer que la clé publique exportée réside effectivement dans le dispositif de protection des éléments secrets du Porteur.

VI.1.2. Transmission de la clé privée à son propriétaire

Si l'AC génère la bi-clé du Porteur (cf. chapitre VI.1.1.2), 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 directement dans le dispositif de protection des éléments secrets du Porteur, ou suivant un moyen équivalent.

	Niveau (***)	
Si la vérification de l'identité du Porteur par l'AE via un face-à-face physique n'a pas eu lieu au moment de l'enregistrement du Porteur (chapitre III.2.3), celle-ci doit être effectuée lors de la remise de la bi-clé générée par l'AC en présence du Porteur.		

	Niveau (**)	
Si la vérification de l'identité du Porteur par l'AE via un face-à-face physique ou via l'emploi d'un procédé de Signature Electronique conforme au minimum aux exigences du niveau (**) n'a pas eu lieu au moment de l'enregistrement du Porteur (chapitre III.2.3), celle-ci doit être effectuée lors de la remise de la bi-clé générée par l'AC en présence du Porteur.		

[Signature]	**Niveau (***)**	
Une fois remise, la clé privée doit être maintenue sous le seul contrôle du Porteur.		

VI.1.3. Transmission de la clé publique à l'AC

En cas de transmission de la requête de demande de Certificat du Porteur au format PKCS#10, ou tout autre conteneur offrant les mêmes fonctions, 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.

VI.1.4. 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.

VI.1.5. Taille des clés

Les clés d'AC et de Porteurs doivent respecter les exigences de caractéristiques (tailles, algorithmes, etc.) de l'Annexe 4 du Référentiel Certification Electronique.

VI.1.6. 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. l'Annexe 4 du Référentiel Certification Electronique).

Les paramètres et les algorithmes utilisés doivent être documentés par l'AC.

VI.1.7. 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 (cf. l'Annexe 4 Référentiel Certification Electronique).

L'utilisation de la clé privée du Porteur et du Certificat associé est strictement limitée à la fonction de sécurité concernée (cf. chapitres I.5.1.1, IV.5 et l'Annexe 4 Référentiel Certification Electronique). Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques.

VI.2.1. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

VI.2.2. Standards et mesures de sécurité pour les modules cryptographiques

VI.2.2.1. *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 chapitre XI ci-dessous pour le niveau de sécurité considéré.

VI.2.2.2. *Dispositifs de protection des éléments secrets des Porteurs*

Les dispositifs de protection des éléments secrets des Porteurs, pour la mise en œuvre de leurs clés privées de personne, doivent respecter les exigences du chapitre XII ci-dessous pour le 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 protection des éléments secrets, au minimum au travers d'un engagement contractuel clair et explicite du Porteur vis-à-vis de l'AC.

En revanche, lorsque l'AC fournit ce dispositif au Porteur, directement ou indirectement, elle doit s'assurer que :

- la préparation des dispositifs de protection des éléments secrets est contrôlée de façon sécurisée par le Prestataire de Service ;
- les dispositifs de protection des éléments secrets sont stockés et distribués de façon sécurisée ;
- les désactivations et réactivations des dispositifs de protection des éléments secrets sont contrôlées de façon sécurisée.

VI.2.3. 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. La génération de la bi-clé est traitée au chapitre VI.1.1.1, l'activation de la clé privée au chapitre VI.2.8 et sa destruction au chapitre VI.2.10.

	Niveaux (**) et (***)	
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).		

	Niveau (*)	
Le contrôle des clés privées de Signature de l'AC doit être assuré par du personnel de confiance (Porteurs de secrets d'IGC).		

VI.2.4. Séquestre de la clé privée

Seules les clés privées associées aux Certificats Electroniques dont l'usage est la Confidentialité (Chiffrement) peuvent être séquestrées, conformément aux dispositions prévues dans la PC et la DPC de l'AC et en respectant les exigences de séquestre et de recouvrement du chapitre IV.12.

VI.2.5. Copie de secours de la clé privée

Hormis pour les clés privées à usage de Confidentialité, les clés privées des Porteurs ne doivent faire l'objet d'aucune copie de secours par l'AC.

Les clés privées d'AC peuvent faire l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous, 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.

Le contrôle des opérations de Chiffrement / Déchiffrement doit être conforme aux exigences du chapitre VI.2.2.

[Confidentialité]		
Les clés privées des Porteurs séquestrées par l'AC peuvent faire l'objet de copies de secours par l'AC, moyennant le respect des exigences de sécurité pour le séquestre des clés.		

VI.2.6. 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.

VI.2.7. 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 du chapitre VI.1.1.2 ci-dessus.

Pour les clés privées d'AC, tout transfert doit se faire sous forme chiffrée, conformément aux exigences du chapitre VI.2.4.

VI.2.8. 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 chapitre XI ci-dessous pour le niveau de sécurité considéré.

Cependant, dans le cas des copies de secours, le stockage peut être effectué en dehors d'un module cryptographique moyennant le respect des exigences du chapitre VI.2.4.

Quel que soit le moyen utilisé, l'AC doit garantir que les clés privées d'AC ne sont pas compromises pendant leur stockage ou leur transport.

VI.2.8. Méthode d'activation de la clé privée

VI.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 définies dans le chapitre XI pour le niveau de sécurité considéré.

	Niveaux (**) et (***)	
L'activation des clés privées d'AC dans un module cryptographique doit être contrôlée via des données d'activation (cf. chapitre VI.4) et doit faire intervenir au moins deux personnes dans des rôles de confiance (par exemple, responsable sécurité et opérateur).		

	Niveau (*)	
L'activation des clés privées d'AC dans un module cryptographique doit être contrôlée via des données d'activation (cf. chapitre VI.4) et doit faire intervenir au moins une personne ayant au moins un rôle de confiance (par exemple, responsable sécurité).		

VI.2.8.1. 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 (cf. chapitre VI.4) et doit permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

VI.2.9. Méthode de désactivation de la clé privée

VI.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 définies dans le chapitre XI pour le niveau de sécurité considéré.

VI.2.9.2. Clés privées des Porteurs

Les conditions de désactivation de la clé privée d'un Porteur doivent permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

VI.2.10. Méthode de destruction des clés privées

VI.2.10.1. Clés privées d'AC

La méthode de destruction des clés privées d'AC doit permettre de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

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.

VI.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 protection des éléments secrets, la méthode de destruction de ces clés privées après leur exportation hors du module cryptographique doit permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

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 définies dans le chapitre XII pour le niveau de sécurité considéré.

[Confidentialité]		
Lorsque la clé privée d'un Porteur n'est plus nécessaire (cf. nota ci-dessous), la méthode de destruction de cette clé privée doit permettre de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré. *Nota* - À la fin de la période de validité d'un Certificat, le passage à une nouvelle clé privée peut se faire au niveau du Porteur : soit en conservant l'ancienne et la nouvelle clé privée, afin que le Porteur continue à accéder aux données précédemment chiffrées avec son ancienne clé privée, soit en procédant à un transchiffrement de l'ancienne clé privée vers la nouvelle, dans ce cas l'ancienne clé n'a pas à être conservée.		

VI.2.11. Niveau de qualification du module cryptographique et des dispositifs de protection des éléments secrets

Les exigences de qualification des produits de sécurité de type module cryptographique et dispositif de protection des éléments secrets ne s'appliquent que lorsque :

- le PSCE fait l'objet d'une procédure de qualification de son offre de Certificats Electroniques et
- les dispositifs de protection des éléments secrets sont délivrés par le PSCE.

Ces exigences sont précisées aux chapitres XI et XII.

VI.3. Autres aspects de la gestion des bi-clés

VI.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.

VI.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 une durée de vie maximale de :

Particulier Entreprise	5 ans 3 ans	5 ans 3 ans	5 ans 3 ans

Cette durée de vie s'entend à compter de la première utilisation de la clé, ou de la première émission d'un Certificat associé à cette clé. La clé doit respecter les exigences de caractéristiques (tailles, algorithmes) de l'Annexe 4 du Référentiel Certification Electronique au démarrage de sa durée de vie.

La fin de validité d'un Certificat d'AC doit être postérieure à la fin de vie des Certificats Porteurs qu'elle émet. L'AC 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 de la date de fin de validité de l'AC qui l'a émise.

A titre d'exemple, une clé d'AC racine a une durée de vie de 12 ans, une AC intermédiaire une durée de vie de 6 ans et un Certificat délivré à une personne physique une durée de vie de 3 ans.

VI.4. Données d'activation

VI.4.1. Génération et installation des données d'activation

VI.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 (cf. chapitre V.2.1).

VI.4.2. 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'au moins 8 caractères, présence d'au moins un caractère spécial, etc.).

VI.4.2. Protection des données d'activation

VI.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.

VI.4.2.2. Protection des données d'activation correspondant aux clés privées des Porteurs

Si les données d'activation des dispositifs de protection des éléments secrets 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.

VI.4.3. Autres aspects liés aux données d'activation

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

VI.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 l'AC peut mener (cf. chapitre I.4.1).

Une analyse des objectifs de sécurité peut être effectuée en amont de tout projet d'IGC par l'AC, de façon à garantir la prise en compte de la sécurité dans les systèmes informatiques.

Le PSCE doit être en mesure de justifier, par tout moyen, qu'il a pris les mesures nécessaires pour assurer la protection des échanges d'information entre les différentes composantes de l'IGC. Il vérifie périodiquement les mesures de sécurité prises dans ce cadre. Le moyen privilégié consiste en un audit technique réalisé par un Prestataire d'audit de la sécurité des systèmes d'information qualifié.

VI.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 de l'AC. 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 des droits des Utilisateurs (permettant de mettre en œuvre la Politique de

contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles),

- 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),
- éventuellement, 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 qui peuvent découler 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.

VI.5.2. Niveau de qualification des systèmes informatiques

	Niveaux (**) et (***)	
Lorsque le PSCE souhaite faire qualifier son offre de Certificats Electroniques, il est recommandé que les systèmes informatiques de l'IGC mettant en œuvre le module cryptographique fassent l'objet d'une qualification conformément au Référentiel Certification Electronique.		

VI.6. Mesures de sécurité des systèmes durant leur cycle de vie

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 peut mener (cf. rappel au début du présent chapitre VI).

VI.6.1 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.

L'AC doit :

- garantir que les objectifs de sécurité sont définis lors des phases de spécification et de conception
- utiliser des systèmes et des produits fiables qui sont protégés contre toute modification

VI.6.2. Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC doit être signalée à l'AC pour validation. Elle doit être documentée et doit apparaître dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

VI.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes

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

VI.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.

L'AC doit garantir que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'AC.

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.).

VI.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 (cf. chapitre V.4).

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

- soit à une autorité d'Horodatage, interne ou externe à l'IGC, conforme à la Politique d'Horodatage (Référentiel Horodatage Electronique) ;
- 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, au minimum à la seconde près. Pour les opérations faites hors ligne (ex : administration d'une AC Racine), cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système devra toutefois pouvoir ordonner les évènements avec une précision suffisante. 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.

VII. Profils des Certificats, OCSP et des LCR

L'Annexe 4 du Référentiel Certification Electronique liste les règles concernant les profils des Certificats, des listes de révocation (LCR) et OCSP. Elles portent notamment sur :

- Les algorithmes et longueurs des clés cryptographiques ;
- Limitation exclusive de l'usage du Certificat Electronique.

VIII. Audit de conformité et autres évaluations

Les audits et les évaluations concernent, d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification au sens du Référentiel Certification Electronique et d'autre part, ceux que doit réaliser, ou faire réaliser, l'AC afin de s'assurer que l'ensemble de son IGC, ainsi que le cas échéant le ou les TC, est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

Les exigences en termes d'évaluation des PSCE par les organismes chargés de leur qualification selon les modalités du Référentiel Certification Electronique ne sont pas décrites ici.

La suite du présent chapitre ne concerne donc que les audits et évaluation de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

VIII.1. Fréquences et / ou circonstances des évaluations

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

L'AC doit également procéder régulièrement à un contrôle de conformité de l'ensemble de son IGC, selon la fréquence suivante :

VIII.2. Identités / qualifications des évaluateurs

Le contrôle d'une composante doit être assigné par l'AC à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

VIII.3. Relations entre évaluateurs et entités évaluées

L'équipe 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.

VIII.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

des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

Le PSCE doit également être en mesure de justifier, par tout moyen, aux auditeurs, qu'il a pris les mesures nécessaires pour assurer la protection des échanges d'information entre les différentes composantes de l'IGC. Il vérifie périodiquement les mesures de sécurité prises dans ce cadre. Le moyen privilégié consiste en un audit technique réalisé par un Prestataire d'audit de la sécurité des systèmes d'information qualifié.

VIII.5. Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : "réussite", "échec", "à confirmer".

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC 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 l'AC et doit respecter ses Politiques de sécurité internes.
- En cas de résultat "à confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

VIII.6. Communication des résultats

Les résultats des audits de conformité doivent être tenus à la disposition de l'organisme de qualification en charge de la qualification de l'AC.

IX.Autres problématiques métiers et légales

IX.1. Responsabilité financière

Conformément à ses obligations, l'AC doit prendre les dispositions nécessaires pour couvrir, éventuellement financièrement, ses responsabilités liées à ses opérations et/ou activités.

IX.1.1. Couverture par les assurances

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

IX.1.2. Autres ressources

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

IX.2.3. Couverture et garantie concernant les entités utilisatrices

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

IX.2. Confidentialité des données professionnelles

IX.2.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- la partie non-publique de la DPC de l'AC,
- 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[19],
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- les dossiers d'enregistrement des Porteurs,
- les causes de révocations, sauf accord explicite du Porteur.

[Confidentialité]		
Les clés privées de l'AC, des composantes et des Porteurs de Certificats (notamment lorsqu'elles sont séquestrées) sont aussi considérées comme des informations confidentielles.		

IX.2.2. Informations hors du périmètre des informations confidentielles

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

IX.2.3. Responsabilités en termes de protection des informations confidentielles

L'AC est tenue d'appliquer des procédures de sécurité pour garantir la Confidentialité des informations identifiées au chapitre IX.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, l'AC doit en garantir l'intégrité.

L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire Togolais. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des Porteurs à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations au Porteur.

IX.3. Protection des données à caractère personnel

IX.3.1. Politique de protection des données à caractère personnel

[19] La confidentialité des données d'activation des clés privées des porteurs doit être garantie par l'AC tant qu'elle les détient.

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire Togolais.

IX.3.2. Données à caractère personnel

Les données considérées comme personnelles sont au moins les suivantes :

- les causes de révocation des Certificats des Porteurs (qui sont considérées comme confidentielles sauf accord explicite du Porteur) ;
- le dossier d'enregistrement du Porteur.

IX.3.3. Données à caractère non personnel

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

IX.3.4. Responsabilité en termes de protection des données à caractère personnel

Cf. législation et réglementation en vigueur sur le territoire Togolais (notamment cf. chapitre X ci- dessous)

IX.3.5. Notification et consentement d'utilisation des données à caractère personnel

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

IX.3.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Cf. législation et réglementation en vigueur sur le territoire Togolais (notamment cf. chapitre X ci- dessous).

IX.3.7. Autres circonstances de divulgation de données à caractère personnel

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

IX.4. Droits de propriété intellectuelle

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. Application de la législation et de la réglementation en vigueur sur le territoire Togolais.

IX.5. Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC sont les suivantes :

- protéger et garantir l'intégrité et la Confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent,
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre VII-VIII) et l'organisme de qualification,
- respecter les accords ou contrats qui les lient entre elles ou aux Porteurs,
- documenter leurs procédures internes de fonctionnement,
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des
- prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

IX.5.1. Autorités de Certification

L'AC a pour obligation de :

- Pouvoir démontrer aux Utilisateurs de ses Certificats qu'elle a émis un Certificat pour un Porteur donné et que ce Porteur a accepté le Certificat, conformément aux exigences du chapitre ci-dessus.
- Garantir et maintenir la cohérence de sa DPC avec sa PC.
- Prendre toutes les mesures raisonnables pour s'assurer que ses Porteurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des Certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un Porteur et l'AC est formalisée par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC est responsable de la conformité de sa Politique de Certification avec les exigences émises dans la présente PC Type pour le niveau de sécurité considéré. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la présente PC Type, par elle-même ou l'une de ses composantes. Elle doit prendre les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente Politique.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des Porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des Certificats de l'AC.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des Certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses Services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de l'AC.

En cas de non-respect ponctuel des obligations décrites dans la présente PC Type, l'Administration se réserve le droit de refuser temporairement ou définitivement les Certificats de l'AC conformément à la réglementation en vigueur.

IX.5.2. Service d'enregistrement

Cf. les obligations pertinentes du chapitre IX.6.1.

IX.5.3. Porteurs de Certificats

Le Porteur a le devoir de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du Certificat ;
- protéger sa clé privée par des moyens appropriés à son environnement ;
- protéger ses données d'activation et, le cas échéant, les mettre en œuvre ;
- protéger l'accès à sa base de Certificats ;
- respecter les conditions d'utilisation de sa clé privée et du Certificat correspondant ;
- informer l'AC de toute modification concernant les informations contenues dans son Certificat ;
- faire, sans délai, une demande de révocation de son Certificat auprès de l'AE, du TC de son entreprise ou de l'AC en cas de compromission ou de suspicion de compromission de sa clé privée (ou de ses données d'activation).

La relation entre le Porteur et l'AC ou ses composantes est formalisée par un engagement du Porteur visant à certifier l'exactitude des renseignements et des documents fournis.

IX.5.4. Utilisateurs de Certificats

Les Utilisateurs utilisant les Certificats doivent :

- vérifier et respecter l'usage pour lequel un Certificat a été émis ;
- pour chaque Certificat de la chaîne de Certification, du Certificat du Porteur jusqu'à l'AC Racine, vérifier la Signature numérique de l'AC émettrice du Certificat considéré et contrôler la validité de ce Certificat (dates de validité, statut de révocation) ;
- vérifier et respecter les obligations des Utilisateurs de Certificats exprimées dans la présente PC Type.

[Confidentialité]		
Les Utilisateurs utilisant les Certificats doivent de plus contrôler que le Certificat émis par l'AC est référencé au niveau de sécurité et pour le Service de confiance requis par l'application.		

L'AC ne doit pas émettre dans sa propre PC d'obligations supplémentaires, par rapport aux obligations de la présente PC Type, à l'encontre des Utilisateurs.

IX.6. Limite de garantie

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

IX.7. Limite de responsabilité

[Signature]		
Il est rappelé que les AC qualifiées suivant la PC type Signature pour le niveau *** délivrent des Certificats qualifiés au sens du décret.		

IX.8. Indemnités

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

IX.9. Durée et fin anticipée de validité de la PC

IX.9.1. Durée de validité

La PC de l'AC doit rester en application au moins jusqu'à la fin de vie du dernier Certificat émis au titre de cette PC.

IX.9.2. 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 l'AC 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 conformément aux modalités prévues par la réglementation en vigueur.

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

IX.9.3. Effets de la fin de validité et clauses restant applicables

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

IX.10. Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC devra :

- au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et

de sécurité des fonctions de l'AC et de ses différentes composantes.

- au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

IX.11. Amendements à la PC

IX.11.1. Procédures d'amendements

L'AC devra contrôler que tout projet de modification de sa PC reste conforme aux exigences de la présente Annexe. En cas de changement important, il est recommandé à l'AC de faire appel à une expertise technique pour en contrôler l'impact.

IX.11.2. Mécanisme et période d'information sur les amendements

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

IX.11.3. Circonstances selon lesquelles l'OID doit être changé

L'OID de la PC de l'AC étant inscrit dans les Certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les Certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des Porteurs, qui ne peuvent donc pas s'appliquer aux Certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les Utilisateurs puissent clairement distinguer quels Certificats correspondent à quelles exigences.

En particulier, l'OID de la PC de l'AC doit évoluer dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente PC Type) intervient dans les exigences de la présente PC Type applicable à la famille de Certificats considérée.

IX.12. Dispositions concernant la résolution de conflits

L'AC doit mettre en place des Politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles elle fournit des Services Electroniques de confiance ou d'autres points qui y sont liés.

IX.13. Juridictions compétentes

La présente PC Type ne formule pas d'exigence spécifique sur le sujet. Application de la législation et de la réglementation en vigueur sur le territoire Togolais.

IX.14. Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC Type sont, notamment, ceux indiqués au chapitre X ci-dessous.

L'AC est notamment soumise aux dispositions prévues par l'article 31 de la [LSQ] concernant la remise des clés privées des Porteurs, si celles-ci sont séquestrées par l'AC.

IX.15. Dispositions diverses

IX.15.1. Accord global

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

IX.15.2. Transfert d'activités

Cf. chapitre V.8.

IX.15.3. Conséquences d'une clause non valide

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

IX.15.4. Application et renonciation

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

IX.15.5. Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.

IX.16. Autres dispositions

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

X. Documents cités en référence

X.1. Réglementation

LTE	Loi sur les transactions Electroniques n°2017-07 du 22 juin 2017
Décret	Décret 2018-062 portant réglementation des transactions et Services Electroniques au Togo

X.2. Documents techniques

Annexe 1	Annexe 1 du Référentiel Certification Electronique : Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques

Annexe 3	Annexe 3 du Référentiel Certification Electronique : Politique de Certification Type « Certificats Electroniques de services applicatifs »
Annexe 4	Annexe 4 du Référentiel Certification Electronique : Profils de Certificats / LCR / OCSP et Algorithmes Cryptographiques
[CWA14167-1]	CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1
[CWA14167-2]	CWA 14167-2 (2003-10) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP). Ce PP a été certifié EAL4+.
[CWA14167-3]	CWA 14167-3 (2003-10) Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)
[CWA14167-4]	CWA 14167-4 (2003-10) Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP). Ce PP a été certifié EAL4+.
[ETSI_NQCP]	ETSI TS 102 042 V1.3.4 (décembre 2007) applicable Policy Requirements for Certification Authorities issuing public key Certificates
[ETSI_QCP]	ETSI TS 101 456 V1.4.3 (mai 2007) Policy Requirements for Certification Authorities issuing qualified Certificates
[ETSI_SigPol]	ETSI TR 102 272 - ASN.1 format for Signature policies V1.1.1 (décembre 2003) ETSI TR 102 038 - XML format for Signature policies V1.1.1 (avril
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute Certificate frameworks, Recommendation X.509, version d'août 2005 (complétée par les correctifs techniques Corrigendum 1 de janvier 2007et Corrigendum 2 de novembre 2008)

XI. Exigences de sécurité du module cryptographique de l'AC

XI.1. Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de Signature (pour la génération des Certificats Electroniques, des LCR / LAR ou 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 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 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 protection des éléments secrets 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 ;
- être capable d'identifier et d'authentifier ses Utilisateurs ;
- limiter l'accès à ses Services en fonction de l'Utilisateur et du rôle qui lui a été assigné ;
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- permettre de créer une Signature Electronique 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 privées 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.

	Niveaux (**) et (***)	
Il est recommandé que le module cryptographique de l'AC détecte les tentatives d'altérations physiques et entre dans un état sûr quand une tentative d'altération est détectée.		

XI.2. Exigences sur la qualification

Le module cryptographique utilisé par l'AC doit être conforme aux exigences. Une cible de sécurité conforme au profil de protection [CWA14167-4] (ou [CWA14167-2] s'il y a une fonction de sauvegarde des clés privées de l'AC) permet au module cryptographique d'être considéré comme conforme aux exigences de la présente Annexe (hors génération des bi-clés des Porteurs). Les exigences de génération des bi-clés des Porteurs peuvent être remplies lorsque la cible de sécurité respecte le profil de protection [CWA14167-3].

XII. Exigences de sécurité du dispositif de protection des éléments secrets

Exigences sur les objectifs de sécurité

Le dispositif de protection des éléments secrets du Porteur, 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 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 des clés privées ;
- garantir la Confidentialité et l'intégrité des clés privées ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une fonction de sécurité qui ne peut être falsifiée sans la connaissance de la clé privée ;
- assurer la fonction de sécurité 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.

[Confidentialité]		
Le dispositif de protection des éléments secrets du Porteur doit répondre aux exigences de sécurité supplémentaires suivantes : - assurer la fonction de Déchiffrement, de clés symétriques de fichier ou de message, 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 symétrique de fichier ou de message, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de Déchiffrement des données ; - le cas échéant, permettre de garantir la Confidentialité, l'authenticité et l'intégrité de la clé privée lors de son export hors du dispositif, à destination d'une fonction de séquestre ou d'archivage des clés privées.		