Politique de Certification

Certigna Services CA

*(Certificats de services applicatifs *)*

OID = 1.2.250.1.177.2.5.1

Réf. 2015-106	Version 1.1

SOMMAIRE

SUIVI DES MODIFICATIONS

Date	Version	Auteur	Evolution du document
19/10/2015	1.0	R. DELVAL	Création
08/01/2016	1.1	V.WYON	Gestion du multi-domaines, de l'OID OV du cabforum et du champ « localityName »

1. Introduction

1.1. Présentation générale

1.1.1. Objet du document

Dhimyotis s'est doté d'une Autorité de Certification (AC) Certigna Services CA pour délivrer des certificats destinés à des services applicatifs.

La présente Politique de Certification (PC) expose les pratiques que l'AC applique et s'engage à respecter dans le cadre de la fourniture de son service de certification électronique. La PC identifie également les obligations et exigences portant sur les autres intervenants, les utilisateurs de certificat.

L'attention du lecteur est attirée sur le fait que la compréhension de la présente PC suppose qu'il soit familiarisé avec les notions liées à la technologie des Infrastructures de Gestion de Clés (IGC).

La présente PC vise la conformité à la PC Type « Certificats électroniques de services applicatifs » [RGS_A_3], pour le niveau * du Référentiel Général de Sécurité (RGS) élaboré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et aux exigences du CA/BROWSER FORUM.

1.1.2. Conventions de rédaction

Dans la suite du document les règles spécifiques à un type d'usage et/ou un type de serveur seront indiquées dans un tableau :

[usage(s)] et/ou [Type de serveur]
Description de la règle…

1.2. Identification du document

La PC est identifiée par l'OID suivant : 1.2.250.1.177.2.5.1 et permet de couvrir les gabarits de certificats suivants :

Usage(s)	**Niv. RGS**	**Type de serveur**	**OID**
Authentification de type serveur SSL/TLS	*	pro (entreprises/administration)	1.2.250.1.177.2.5.1.1.1
Authentification serveur de type client	*	pro (entreprises/administration)	1.2.250.1.177.2.5.1.2.1

1.3. Définitions et acronymes

1.3.1. Acronymes

Les acronymes utiles à la bonne compréhension de la présente PC sont les suivants :

AA	Autorité Administrative
AAP	Autorité d'Approbation des Politiques
AC	Autorité de Certification
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
AH	Autorité d'Horodatage
ANSSI	Agence nationale de la sécurité des systèmes d'information
ANTS	Agence Nationale des Titres Sécurisés
CGU	Conditions Générales d'Utilisation
CNIL	Commission Nationale de l'Informatique et des Libertés
CSR	Certificate Signature Request
DN	Distinguished Name
DNS	Domain Name System
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
FQDN	Fully Qualified Domain Name
ICD	International Code Designator
IGC	Infrastructure de Gestion de Clés (= PKI : Public Key Infrastructure)
INPI	Institut National de la Propriété Industrielle
LAR	Liste des certificats d'AC Révoqués
LCP	Lightweight Certificate Policy
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification
PCA	Plan de Continuité d'Activité
PP	Profil de Protection
PKCS	Public Key Cryptographic Standards
PSCE	Prestataire de Services de Certification Électronique
PSCO	Prestataire de Services de Confiance
RC	Responsable du Certificat
RSA	Rivest Shamir Adelman
SGMAP	Secrétariat Général pour la Modernisation de l'Action Publique
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

1.3.2. Définitions

Les termes utiles à la bonne compréhension de la PC sont les suivants :

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

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins du service auquel le certificat est rattaché.

Autorités administratives - Ce terme générique désigne les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

Autorité de Certification – 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).

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

Certificat électronique - Fichier électronique attestant du lien entre une clé publique et l'identité de son propriétaire (personne physique ou service applicatif). Cette attestation prend la forme d'une signature électronique réalisée par un PSCE. Il est délivré par une AC.
Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Composante - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptographie 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 - Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Dispositif de protection des éléments secrets - Désigne un dispositif de stockage des éléments secrets remis au RC (ex. clé privée, code PIN, …). Il peut prendre la forme d'une carte à puce, d'une clé USB à capacité cryptographique ou se présenter au format logiciel (ex. 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.

FQDN - Nom de domaine pleinement qualifié indiquant la position absolue d'un nœud dans l'arborescence DNS et précisant les domaines de niveau supérieur jusqu'à la racine.

Infrastructure de Gestion de Clés - 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 AC, d'un opérateur de certification, d'une

autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, …

Liste des Autorités révoquées - Liste comprenant les numéros de série des certificats des autorités intermédiaires ayant fait l'objet d'une révocation, et signée par l'AC racine.

Liste des Certificats Révoqués - Liste comprenant les numéros de série des certificats ayant fait l'objet d'une révocation, et signée par l'AC émettrice.

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

Prestataire de services de certification électronique (PSCE) - Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des RC et utilisateurs de ces 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.

Promoteur d'application - Un responsable d'un service de la sphère publique accessible par voie électronique.

Qualification d'un prestataire de services de certification électronique - Le Décret RGS décrit la procédure de qualification des PSCO. Un PSCE étant un PSCO particulier, la qualification d'un PSCE est un acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) à certaines exigences d'une PC Type pour un niveau de sécurité donné et correspondant au service visé par les certificats.

Qualification d'un produit de sécurité - Acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le RGS. La procédure de qualification des produits de sécurité est décrite dans le décret RGS. Le RGS précise les trois processus de qualification : qualification de niveau élémentaire, qualification de niveau standard et qualification de niveau renforcé.

Responsable du certificat - Personne en charge et responsable du certificat électronique de service applicatif.

RSA - Algorithme à clés publiques du nom de ses inventeurs (Rivest, Shamir et Adleman).

Système d'Information - Tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Usager - Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives.

Utilisateur de certificat - Entité ou personne physique qui utilise un certificat et qui s'y fie pour vérifier une signature électronique ou une valeur d'authentification provenant d'un RC ou chiffrer des données à destination d'un RC.
Nota - Un agent d'une autorité administrative qui procède à des échanges électroniques avec une autre autorité administrative est, pour cette dernière, un usager.

1.4. Entités intervenant dans l'IGC

1.4.1. Autorité 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 IGC. L'AC est responsable de la mise en application de la PC à l'ensemble de l'IGC qu'elle a mise en place.

Pour les certificats signés en son nom, l'AC assure les fonctions suivantes :
- Fonctions d'enregistrement et de renouvellement ;
- Fonction de génération des certificats ;
- Fonction de génération d'éléments secrets ;
- Fonction de publication des conditions générales, de la PC, des certificats d'AC et des formulaires de demande de certificat ;
- Fonction de gestion des révocations ;
- Fonction d'information sur l'état des certificats via la liste des certificats révoqués (LCR) mise à jour à intervalles réguliers et selon un mode requête/réponse en temps réel (OCSP) ;

L'AC assure ces fonctions directement ou en les sous-traitant, tout ou partie. Dans tous les cas, l'AC en garde la responsabilité.

L'AC s'engage à respecter les obligations décrites dans la présente PC. Elle s'engage également à ce que les composants de l'IGC, internes ou externes à l'AC, auxquels elles incombent les respectent aussi.

Enfin, les parties de l'AC concernées par la génération des certificats et la gestion des révocations sont 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, les cadres dirigeants, leur personnel d'encadrement et leur personnel ayant des rôles de confiance, sont 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 ont une structure documentée qui préserve l'impartialité des opérations.

1.4.2. Autorité d'enregistrement

L'AE assure les fonctions suivantes déléguées par l'AC, en vertu de la présente PC :
- La prise en compte et la vérification des informations du futur responsable de certificat (RC) et du service applicatif auquel le certificat est rattaché, ainsi que de l'entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- La prise en compte et la vérification des informations, le cas échéant, du futur mandataire de certification* et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- L'établissement et la transmission de la demande de certificat à l'AC ;
- L'archivage des dossiers de demande de certificat ;
- La conservation et la protection en confidentialité et intégrité des données personnelles d'authentification du responsable du certificat ou du MC ;
- La vérification des demandes de révocation de certificat.

L'AE assure ces fonctions directement ou en les sous-traitant en partie à des autorités d'enregistrement déléguées. Dans tous les cas, l'AE en garde la responsabilité.

Sauf indication contraire, dans le présent document la mention AE couvre l'autorité d'enregistrement et les autorités d'enregistrement déléguées.

** L'AE offre la possibilité à l'entité cliente d'utiliser un mandataire de certification désigné et placé sous sa responsabilité pour effectuer tout ou partie des opérations de vérification des informations. Dans ce cas, l'AE s'assure que les demandes soient complètes et effectuées par un mandataire de certification dûment autorisé.*

Dans tous les cas l'archivage des pièces du dossier d'enregistrement (sous forme électronique et/ou papier) est de la responsabilité de l'AE.

1.4.3. Responsables de certificats électroniques de services

Dans le cadre de la présente PC, un Responsable de Certificat (RC) est une personne physique qui est responsable de l'utilisation du certificat électronique identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité également identifiée dans ce certificat. Le RC a un lien contractuel / hiérarchique / réglementaire avec cette entité.
Le RC respecte les conditions qui lui incombent, conditions définies dans cette PC et dans les CGU.

Il est à noter que le certificat étant attaché au service applicatif et non au RC, ce dernier peut être amené à changer en cours de validité du certificat : départ du RC de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.

L'entité doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RC de ses fonctions et lui désigner un successeur. L'AC révoquera un certificat électronique pour lequel il n'y a plus de RC explicitement identifié.

Dans la suite du document le terme « entité » est utilisé pour désigner une entreprise ou une administration. La dénomination « entreprise » recouvre les entreprises au sens le plus large, à savoir toutes personnes morales de droit privé : sociétés, associations ainsi que les artisans et travailleurs indépendants.

1.4.4. Utilisateurs de certificats

Un utilisateur de certificat peut être :

Authentification de type serveur SSL/TLS
Une personne accédant à un serveur et qui utilise le certificat du serveur et un module de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat du serveur, afin d'établir une clé de session partagée entre son poste et le serveur.

Authentification serveur de type client
Un service applicatif accédant à un serveur informatique et qui utilise un certificat et un applicatif de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat, et afin d'établir une clé de session partagée entre les deux serveurs.

Les utilisateurs de certificats doivent prendre toutes les précautions décrites dans la PC ainsi que dans les CGU.

1.4.5. Autres participants

L'AC s'appuie également sur des AED pour sous-traiter une partie des fonctions de l'AE.

Un opérateur d'AED a le pouvoir :
- d'autoriser, d'effectuer une demande de certificat ou de renouvellement de certificat ;
- d'effectuer une demande de révocation de certificat ;
- le cas échéant, d'enregistrer les mandataires de certification au sein des entités émettrices de demandes de certificat.

Il assure pour l'AC, dans le contexte de la délivrance de certificat, la vérification d'identité des futurs responsables de certificats et des services applicatifs dans les mêmes conditions et avec le même niveau de sécurité que ceux requis pour l'opérateur d'AE. Il est pour cela en relation directe avec l'AE.

Les engagements de l'opérateur d'AED à l'égard de l'AC sont précisés dans un contrat écrit avec l'entité responsable de l'opérateur ainsi que dans la lettre d'engagement que doit signer ce dernier. Ces deux documents précisent notamment que l'opérateur d'AED doit effectuer de façon impartiale et scrupuleuse les contrôles d'identité des futurs responsables de certificats et mandataires de certification, et respecter les parties de la PC et de la DPC lui incombant.

L'AC offre la possibilité à l'entité cliente de désigner un ou plusieurs mandataires de certification (MC). Ce mandataire a, par la loi ou par délégation, le pouvoir :

- d'autoriser, d'effectuer une demande de certificat ou de renouvellement de certificat portant le nom de l'entité ;
- d'effectuer une demande de révocation de certificat portant le nom de l'entité.

Le mandataire de certification peut être un représentant légal ou toute personne que ce dernier aura formellement désignée.

Il assure pour l'AC, dans le contexte de la délivrance de certificat, la vérification d'identité des futurs responsables de certificats et des services applicatifs dans les mêmes conditions et avec le même niveau de sécurité que ceux requis pour l'opérateur d'AE. Il est pour cela en relation directe avec l'Autorité d'Enregistrement.

Les engagements du mandataire à l'égard de l'AC sont précisés dans un contrat écrit avec l'entité responsable du MC ainsi que dans la lettre d'engagement que doit signer le mandataire. Ces deux documents précisent notamment que le MC doit effectuer correctement et de façon indépendante les contrôles des dossiers des futurs responsables de certificats et des services applicatifs, et doit respecter les parties de la PC et de la DPC lui incombant.

L'entité doit signaler sans délai à l'AC le départ du MC de ses fonctions et lui désigner éventuellement un successeur.

Le MC ne doit pas avoir accès aux données d'activation de la clé privée associée au certificat délivré au responsable de certificat.

1.5. Usage des certificats

1.5.1. Domaines d'utilisation applicables

Bi-clés et certificats des services applicatifs

Authentification de type serveur SSL/TLS
Authentification du serveur auprès de personnes, dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS ou IPsec visant à établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés. L'établissement de la clé de session peut se faire par un mécanisme cryptographique asymétrique, de type RSA (génération de la clé symétrique par le client et chiffrement de cette clé symétrique par la clé publique du serveur) ou de type Diffie-Hellman (obtention de la clé symétrique via un algorithme combinant la clé privée du client et la clé publique du serveur, et inversement).

Authentification serveur de type client
Authentification du serveur auprès d'autres serveurs, dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS ou IPsec visant à établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés. L'établissement de la clé de session peut se faire par un mécanisme cryptographique asymétrique, de type RSA (génération de la clé symétrique par le client et chiffrement de

cette clé symétrique par la clé publique du serveur) ou de type Diffie-Hellman (obtention de la clé symétrique via un algorithme combinant la clé privée du client et la clé publique du serveur, et inversement).

Les certificats électronique objets de la présente PC sont utilisés par des applications pour lesquelles les besoins de sécurité sont moyens eu égard aux risques qui les menacent.

Bi-clés et certificats d'AC et de composantes

L'AC dispose d'une seule bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur (Certigna Root CA). La bi-clé de l'AC permet de signer les différents types d'objets qu'elle génère : certificats des services applicatifs, LCR.

Les opérateurs de l'IGC disposent de certificats permettant de s'authentifier sur cette IGC. Pour les opérateurs d'AE (les opérateurs d'AED n'étant pas concernés), ce certificat permet de signer les demandes de certificats et de révocation avant leur transmission à l'AC. Ces certificats sont émis par une IGC distincte, interne à Dhimyotis, et dont le niveau de sécurité est adapté à celui requis pour l'AC.

1.5.2. Domaines d'utilisation interdits

Les usages autres que ceux cités dans le paragraphe précédent sont interdits.

L'AC s'engage à respecter ces restrictions et à imposer leur respect par les RC et les utilisateurs de certificats. A cette fin, elle publie à destination des RC, MC et utilisateurs potentiels des CGU qui peuvent être consultées sur le site http://www.certigna.fr avant toute demande ou toute utilisation d'un certificat.

1.6. Gestion de la PC

1.6.1. Entité gérant la PC

Dhimyotis dispose d'un Comité de Sécurité présidé par l'Officier de Sécurité.

Ce comité est responsable de l'élaboration, du suivi, de la modification et de la validation de la présente PC. Il statue sur toute modification nécessaire à apporter à la PC à échéance régulière.

1.6.2. Point de contact

Dhimyotis - Certigna
20 allée de la Râperie
Zone de la plaine
59650 Villeneuve d'Ascq

1.6.3. Entité déterminant la conformité de la DPC avec la PC

Le Comité de Sécurité s'assure de la conformité de la DPC par rapport à la PC. Il peut, le cas échéant, se faire assister par des experts externes pour s'assurer de cette conformité.

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

La DPC traduit en termes technique, organisationnel et procédural les exigences de la PC en s'appuyant sur la politique de sécurité de l'entreprise. Le Comité de Sécurité s’assure que les moyens mis en œuvre et décrits dans la DPC répondent à ces exigences selon le processus d’approbation mis en place. Un contrôle de conformité de la DPC par rapport à la PC est effectué par un cabinet d'audit externe lors des audits réalisés en vue de la qualification initiale et/ou d'un audit de surveillance. Toute demande de mise à jour de la DPC suit également ce processus.

Toute nouvelle version approuvée de la DPC est publiée sans délai.

2. Responsabilité concernant la mise à disposition des informations

2.1. Entités chargées de la mise à disposition des informations

L'IGC met à disposition des utilisateurs et des applications utilisatrices des certificats qu'elle émet des informations sur l'état de révocation des certificats en cours de validité émis par l'AC.

Ces informations sont publiées au travers de plusieurs serveurs :
- Serveur Web (2) :
    - http://crl.certigna.fr/servicesca.crl
    - http://crl.dhimyotis.com/servicesca.crl
- Serveur OCSP (2) :
    - http://servicesca.ocsp.certigna.fr
    - http://servicesca.ocsp.dhimyotis.com

2.2. Informations devant être publiées

L'AC publie à destination des RC et utilisateurs de certificats :
- La PC;
- Les Conditions Générales d'Utilisation des services de certification de l'AC;
- Les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, …) ;
- Le certificat d'AC Certigna Root CA et le certificat d'AC intermédiaire en cours de validité ;
- La liste des certificats révoqués (LAR / LCR) ;
- La DPC sur demande expresse auprès de Dhimyotis.

Remarque : compte tenu de la complexité de lecture d'une PC pour les RC ou les utilisateurs de certificats non spécialistes du domaine, l'AC publie en dehors des PC et DPC des CGU que le futur RC est dans l'obligation de lire et d'accepter lors de toute demande de certificat (demandes initiales et suivantes, en cas de renouvellement) auprès de l'AE.

2.2.1. Publication de la documentation

Publication de la PC, des conditions générales et des formulaires

La PC, les conditions générales d'utilisation des services de certification de l'AC et les différents formulaires nécessaires pour la gestion des certificats sont publiés sous format électronique à l'adresse http://www.certigna.fr

La PC est également publiée à l'adresse http://www.dhimyotis.com

Publication de la DPC

L'AC publie, à destination des RC et utilisateurs de certificats, et sur leur demande, sa DPC pour rendre possible l'évaluation de la conformité avec sa politique de certification. Les détails relatifs à ses pratiques ne sont toutefois pas rendus publics.

Publication des certificats d'AC

Les RC et les utilisateurs de certificat peuvent accéder aux certificats d'AC qui sont publiés aux adresses :
- http://www.certigna.fr/autorites
- http://www.dhimyotis.com/autorites

2.2.2. Publication de la LCR

La liste des certificats révoqués est publiée sous format électronique aux adresses décrites dans le chapitre 2.1 ci-dessus. Ces adresses sont également indiquées dans les certificats émis par l'AC.

2.2.3. Publication de la LAR

La liste des certificats d'autorité intermédiaire révoqués est publiée sous format électronique aux adresses décrites dans le chapitre 2.1 ci-dessus. Ces adresses sont également indiquées dans les certificats émis par l'AC racine Certigna Root CA.

2.3. Délais et fréquences de publication

2.3.1. Publication de la documentation

La PC, les CGU des services de certification de l'AC et les différents formulaires nécessaires pour la gestion des certificats sont mis à jour si nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC. La fonction de publication de ces informations (hors informations d'état des certificats) est disponible les jours ouvrés.

2.3.2. Publication des certificats d'AC

Les certificats d'AC sont diffusés préalablement à toute diffusion de certificats émis par l'AC et de LCR correspondantes.

La disponibilité des systèmes publiant les certificats d'AC est garantie 24 heures sur 24, 7 jours sur 7.

2.3.3. Publication de la LCR

La LCR est mise à jour au minimum toutes les 24 heures, et à chaque nouvelle révocation.

2.3.4. Publication de la LAR

La LAR est mise à jour au maximum tous les ans, et à chaque nouvelle révocation.

2.4. Contrôle d'accès aux informations publiées

L’accès aux informations publiées à destination des utilisateurs est libre.

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

3. Identification et Authentification

3.1. Nommage

3.1.1. Types de noms

Dans chaque certificat, l'AC émettrice (correspondant au champ « issuer ») et le service applicatif d'authentification serveur (champ « subject ») sont identifiés par un « Distinguished Name » DN de type X.501.

3.1.2. Nécessité d'utilisation de noms explicites

Le DN du certificat permet d'identifier le service applicatif et est construit à partir de l'identité du serveur.

Le DN a la forme suivante :
{
C = Pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée,
L = Ville où est implantée l'entité,
O = Nom de l'entité à laquelle appartient le RC,
OU = ICD + identifiant de l'entité à laquelle appartient le RC conformément à la législation et aux réglementations en vigueur.
OI = Informations sur le justificatif d'identité de l'entité
CN = FQDN du service applicatif (dans le cas du multi-domaine, le FQDN placé dans le CN doit également être présent dans la liste des FQDN du champ SAN) ou identité du serveur,
serialNumber = Série de caractères composée d'un aléa pour assurer l'unicité
}

L'identité du serveur est la raison sociale de l'entité séparée de la fonction du serveur par un tiret.

3.1.3. Anonymisation ou pseudonymisation des serveurs

L'AC n'émet pas de certificat comportant une identité anonyme.

3.1.4. Règles d'interprétation des différentes formes de noms

Aucune interprétation n'est faite sur le nom des certificats.

3.1.5. Unicité des noms

La combinaison du pays, de l'entité et du FQDN ou de l'identité du serveur identifie de manière univoque le titulaire du certificat.

Durant toute la durée de vie de l'AC, le FQDN d'un serveur rattaché à une entité ne peut être attribué à une autre entité

3.1.6. Identification, authentification et rôle des marques déposées

L'AC est responsable de l'unicité des noms des services utilisés dans ses certificats et de la résolution des litiges portant sur la revendication d'utilisation d'un nom. Cet engagement de responsabilité s'appuie sur le niveau de contrôle assuré lors du traitement des demandes de certificats. L'AC peut éventuellement vérifier l'appartenance de la marque auprès de l'INPI.

3.2. Validation initiale de l'identité

L'enregistrement d'un RC peut se faire soit directement auprès de l'AE (AE ou AED), soit via un mandataire de certification de l'entité. Dans ce dernier cas, le mandataire de certification doit être préalablement enregistré auprès de l'AE.

3.2.1. Méthode pour prouver la possession de la clé privée

L'AC s'assure de la détention de la clé privée par le RC avant de certifier la clé publique. Pour ceci, L'AE génère la bi-clé du ou le RC génère lui-même sa bi-clé et fournit à l'AC une preuve de possession de sa clé privée en signant sa demande de certificat (Certificate Signing Request au format PKCS#10).

3.2.2. Validation de l'identité d'un organisme

Cf. chapitre 3.2.3

3.2.3. Validation de l'identité d'un individu

La validation initiale d’une personne physique est réalisée dans les cas suivants.

Enregistrement d'un RC sans MC pour un certificat à émettre

L'enregistrement du service applicatif pour lequel un certificat doit être délivré se fait via l’enregistrement du RC correspondant.

Le RC devra démontrer qu’il dispose du droit d’utiliser le nom de domaine inclus dans le FQDN (titularité des droits sur le nom de domaine ou droit d’utilisation de la part de l’entité titulaire des droits).

L’enregistrement du futur RC représentant une entité nécessite la validation de l'identité "personne morale" de cette entité, de l'identité "personne physique" du futur RC, et du rattachement du futur RC à cette entité.

Le dossier de demande de certificat, transmis à l'AE, doit comprendre :

- La demande de certificat (formulaire disponible sur le site de Certigna http://www.certigna.fr), datée de moins de trois mois, remplie et co-signée par un représentant légal de l'entité et par le RC comportant notamment
    - L'acceptation des termes et conditions (conditions générales d'utilisation) ;
    - L'identité du serveur à utiliser dans le certificat (FQDN) ;
    - Les données personnelles d'identification du RC ;
    - Les informations d'identification de l'entité ;
    - Les coordonnées d'un représentant légal de l'entité (nom, entité, adresse, téléphone, email) ;
    - Les coordonnées du futur RC (nom, entité, adresse, téléphone, e-mail)
- Un mandat signé, et daté de moins de trois mois, par un représentant légal de l'entité désignant le futur RC comme étant habilité à être RC pour le service auquel le certificat doit être délivré. Ce mandat doit être signé pour acceptation par le futur RC ;
- La photocopie d'un document officiel d'identité en cours de validité du futur RC ou une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintien un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent. La photocopie du document d'identité est certifiée conforme par le futur RC (date, de moins de 3 mois, et signature précédées de la mention "copie certifiée conforme à l'original") ;
- La photocopie d'un document officiel d'identité en cours de validité du représentant légal ou une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintien un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent. La photocopie du document d'identité est certifiée conforme par le futur RC (date, de moins de 3 mois, et signature précédées de la mention "copie certifiée conforme à l'original") ;
- Des informations d'identification de l'entité :
    - Pour une entreprise :
        - Tout document attestant de la qualité du représentant légal (par exemple, un exemplaire des statuts de l'entreprise, en cours de validité, portant signature de ses représentants) ;
        - Toute pièce, valide au moment de l'enregistrement, portant le numéro SIREN de l'entreprise (extrait KBIS ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements) ou, à défaut, une autre pièce valide attestant l'identification unique de l'entreprise qui figurera dans le certificat.
    - Pour une administration :
        - Une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative.

L'authentification du futur RC par l'AE (opérateur d'AE ou opérateur d'AED) est réalisée par l'envoi du dossier soit par courrier postal, soit sous forme dématérialisée (dossier scanné puis transmis par courrier électronique).

Le RC est informé que les informations personnelles d'identité pourront être utilisées comme données d'authentification lors d'une éventuelle demande de révocation.

Enregistrement du mandataire de certification (MC)

Le mandataire de certification (MC) doit s'enregistrer auprès de l'AE pour pouvoir se substituer à l'AE dans le processus d'enregistrement des demandeurs de certificats.

L'enregistrement d'un MC nécessite la validation de l'identité "personne morale" de l'entité pour laquelle le MC interviendra, de l'identité "personne physique" du futur MC, et du rattachement du futur MC à cette entité.

A cette fin, le mandataire de certification doit transmettre à l'AE un dossier d'enregistrement comprenant les pièces suivantes :

- Une demande écrite signée, datée de moins de 3 mois, par un représentant légal de l'entité;
- Un mandat signé, daté de moins de 3 mois, par un représentant légal de l'entreprise désignant le mandataire. Ce mandat est également signé par le mandataire de certification pour acceptation ;
- Un engagement signé, daté de moins de 3 mois, du mandataire de certification à :
    - Effectuer correctement et de façon indépendante les contrôles des dossiers des futurs demandeurs tels que définis dans la PC;
    - Informer l'AE en cas de départ de l'entité.
- La photocopie d'un document officiel d'identité en cours de validité du futur mandataire ou une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintien un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent. La photocopie du document d'identité est certifiée conforme par le futur RC (date, de moins de 3 mois, et signature précédées de la mention "copie certifiée conforme à l'original") ;
- Des informations d'identification de l'entité :
    - Pour une entreprise :
        - Tout document attestant de la qualité du représentant légal (par exemple, un exemplaire des statuts de l'entreprise, en cours de validité, portant signature de ses représentants) ;
        - Toute pièce, valide au moment de l'enregistrement, portant le numéro SIREN de l'entreprise (extrait KBIS ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements) ou, à défaut, une autre pièce valide attestant l'identification unique de l'entreprise qui figurera dans le certificat.
    - Pour une administration :
        - Une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative.

Le mandataire de certification est informé que les informations personnelles d'identité pourront être utilisées comme données d'authentification lors d'une éventuelle demande de révocation.

L'authentification du MC par l'AE s'effectue via l'envoi du dossier papier par courrier accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, MC) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ces papiers d'identité, précédées de la mention "copie certifiée conforme à l'original"). Cette authentification peut également se faire sous forme dématérialisée à condition que les

différentes pièces justificatives du dossier soient signées à l'aide d'un procédé de signature électronique conforme aux exigences du niveau * et que la signature soit vérifiée et valide au moment de l'enregistrement. Si le mandataire n'est pas équipé d'un certificat de niveau * ou supérieur, les dossiers ne pourront être envoyés sous forme dématérialisée. Dans ce cas, chaque dossier ne sera validé qu'après réception des documents originaux par courrier.
Le mandataire de certification est informé que les informations personnelles d'identité pourront être utilisées comme données d'authentification lors d'une éventuelle demande de révocation.

Enregistrement d'un RC via un MC

L'enregistrement d'un RC via un MC nécessite la validation par le MC de l'identité "personne physique" du futur RC et de son rattachement à l'entité pour laquelle le MC intervient.

Le dossier de demande de certificat établi avec le MC, doit comprendre :
- Une demande de certificat écrite, datée de moins de 3 mois, signée par le MC et le futur RC et comportant l'identité du service (FQDN) concerné par cette demande ;
- La photocopie d'un document officiel d'identité en cours de validité du futur RC ou une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintien un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent. La photocopie du document d'identité est certifiée conforme par le futur RC (date, de moins de 3 mois, et signature précédées de la mention "copie certifiée conforme à l'original") ;
- L'acceptation des termes et conditions (CGU) ;

Le dossier est envoyé par courrier à l'AE pour conservation, et éventuellement sous forme électronique.

Le RC est informé que les informations personnelles d'identité pourront être utilisées comme données d'authentification lors d'une éventuelle demande de révocation.

3.2.4. Informations non vérifiées du serveur

Sans objet.

3.2.5. Validation de l'autorité du demandeur

Cette étape est effectuée en même temps que la validation de l'identité de la personne physique (directement par l'AE ou par le MC).

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

L'AC n'émet pas de nouveau certificat pour une bi-clé précédemment émise. Le renouvellement passe par la génération d'une nouvelle bi-clé et d'une nouvelle demande de certificat.

3.3.1. Identification et validation pour un renouvellement courant

La vérification de l'identité du RC est identique à la demande initiale.

3.3.2. Identification et validation pour un renouvellement après révocation

La vérification de l'identité du RC est identique à la demande initiale.

3.4. Identification et validation d'une demande de révocation

La demande de révocation du certificat par le RC, un représentant légal de l'entité, un opérateur d'AED, ou le cas échéant un MC, peut s'effectuer par l'un des moyens suivants :

- Via l'espace client du site Certigna http://www.certigna.fr en sélectionnant le certificat à révoquer.

  Le demandeur s'authentifie sur le site avec son identifiant/mot de passe, sélectionne le certificat à révoquer, et renseigne les réponses aux questions secrètes qu'il a personnalisé lors de sa souscription pour permettre la révocation du certificat.

- Par courrier : demande remplie et signée à partir du formulaire de révocation d'un certificat et de l'adresse postale disponibles sur le site de Certigna http://www.certigna.fr. Le demandeur s'authentifie en joignant la photocopie de sa pièce d'identité au courrier envoyé.

  La demande papier doit comporter les éléments suivants :
  - Le prénom et le nom du RC ;
  - L'adresse e-mail du RC ;
  - L'identité du service concerné (FQDN)
  - La raison de la révocation.

  Si le RC n'est pas le demandeur :
  - Le prénom et le nom du demandeur ;
  - La qualité du demandeur (responsable légal, opérateur d'AED, MC);
  - L'identité du service concerné (FQDN)
  - Le numéro de téléphone du demandeur.

  Le formulaire papier peut également être transmis sous format électronique. La demande électronique peut être signée par une personne habilitée à l'aide d'un certificat électronique de signature de même niveau ou supérieur (un opérateur d'AED ou le cas échéant un MC).

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

La demande de certificat doit émaner d'un représentant légal de l'entité, d'un MC dûment mandaté pour cette entité, avec un consentement préalable du futur RC.

La demande peut être transmise (dossier d'enregistrement) à l'AE par un opérateur d'AED.

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

Le dossier de demande est établi soit directement par le futur RC à partir des éléments fournis par son entité, soit par son entité et signé par le futur RC. Le dossier est transmis directement à l'AE si l'entité n'a pas mis en place de MC. Le dossier est remis à ce dernier dans le cas contraire. Lors de l'enregistrement du futur RC, ce dernier doit fournir une adresse mail qui permet à l'AE de prendre contact pour toute question relative à son enregistrement. Le MC doit également fournir une adresse mail lors de son enregistrement, pour que l'AE puisse prendre contact avec ce dernier pour toute question relative à l'enregistrement des RC.

Le dossier de demande de certificat doit contenir les éléments décrits au chapitre 3.2.3.

4.2. Traitement d'une demande de certificat

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

L'AE effectue les opérations suivantes lors du traitement d'une demande de certificat qui lui a été transmise :

- Validation de l'identité du futur RC le cas échéant ;
- Validation de l'identité de l'entité et de son représentant légal ;
- validation du FQDN du serveur informatique auquel le certificat est rattaché. L'AE, ou le MC, vérifiera que le FQDN du serveur est correctement formaté et ne contient pas le caractère NUL.
- Validation du dossier et de la cohérence des justificatifs présentés ;
- Assurance que le futur RC a pris connaissance des modalités applicables pour l'utilisation du certificat.

L'identité du futur RC et du représentant légal est approuvée si les pièces justificatives fournies sont valides à la date de réception.

Dans le cas d'une demande via un opérateur d'AED, ce dernier retransmet le dossier à l'AE après avoir effectué les opérations ci-dessus. L'AE s'assure alors que la demande correspond au mandat de l'opérateur d'AED.

Dans le cas d'une demande via un MC, ce dernier retransmet le dossier à l'AE après avoir effectué en partie les opérations ci-dessus (validation de l'identité du futur RC, validation du dossier, assurance de la prise de connaissance des conditions générales). L'AE s'assure alors que la demande correspond au mandat du MC.

Dans tous les cas, le dossier de demande est archivé par l'AE.

4.2.2. Acceptation ou rejet de la demande

La demande de certificat s'effectue, pour rappel, en deux étapes distinctes :
- L'envoi de la demande électronique (CSR) ;
- L'acquisition de la demande (réception du dossier papier de demande signé ou éventuellement de sa version dématérialisée).

Après traitement de la demande (contrôle du dossier, rapprochement et contrôle de cohérence avec la CSR), en cas de rejet, l'AE le notifie au RC, le cas échéant à l'opérateur d'AED, ou au MC.

La justification d'un éventuel refus est effectuée par l'AE en précisant la cause :
- Le dossier de demande est incomplet (pièce manquante) ;
- Une des pièces du dossier est non valide (date de signature supérieure à 3 mois, date de validité de la pièce est dépassée, etc.) ;
- La demande ne correspond pas au mandat de l'opérateur d'AED ou du MC;
- La demande électronique (CSR) n'est pas cohérente avec le dossier de demande (des informations telles que l'identité, la fonction du serveur ou le nom de l'organisation sont différentes).

En cas d'acceptation par l'AE, après génération du certificat par l'AC, l'AE envoie un mail au RC pour effectuer l'importation du certificat.

4.2.3. Durée d'établissement du certificat

A compter de la réception du dossier d'enregistrement complet et de la demande électronique (CSR), le certificat est établi dans un délai de cinq jours ouvrés.

4.3. Délivrance du certificat

4.3.1. Actions de l'AC concernant la délivrance du certificat

Suite à la validation par l'AE, l'AC déclenche le processus de génération du certificat destiné au RC.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres 5 et 6 ci-dessous, notamment la séparation des rôles de confiance.

(cf. chapitre 5.2).

4.3.2. Notification par l'AC de la délivrance du certificat

Le certificat complet et exact est mis à disposition de son RC (depuis l'espace client). Le RC s'authentifie sur son espace client pour accepter son certificat ou remplit un formulaire papier.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

L'acceptation peut être réalisée de deux façons.

- Soit lors de l'installation du certificat le RC choisit d'accepter ou non le certificat depuis son espace client. La notification d'acceptation ou de refus est transmise automatiquement à l'AC.
- Soit le RC notifie l'acceptation ou non du certificat en complétant un formulaire papier qui sera envoyé par courrier ou remis lors d'un face à face.

En cas d'échec de l'envoi, l'acceptation est tacite dans un délai de 7 jours à compter de l'envoi du certificat. En cas de détection d'incohérence entre les informations figurant dans l'accord contractuel et le contenu du certificat, le RC doit refuser le certificat, ce qui aura pour conséquence sa révocation.

4.4.2. Publication du certificat

Aucune publication n'est effectuée après l'acceptation du certificat par son RC.

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

L'AE est informée de la génération du certificat par l'AC. C'est elle qui est responsable de la délivrance du certificat généré au RC.

4.5. Usages de la bi-clé et du certificat

4.5.1. Utilisation de la clé privée et du certificat par le RC

Les RC doivent respecter strictement les usages autorisés des bi-clés et des certificats cités au chapitre 1.5.1. Dans le cas contraire, leur responsabilité pourrait être engagée.

Les usages autorisés de la bi-clé et du certificat associé sont indiqués dans le certificat lui-même, via l'extension Key Usage.

Ces usages sont aussi indiqués dans les CGU qui, faisant partie du dossier d'enregistrement, sont portées à la connaissance du RC ou du MC par l'AC avant d'entrer en relation contractuelle.

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

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

4.6. Renouvellement d'un certificat

L'AC n'émet pas de nouveau certificat pour une bi-clé précédemment émise. Le renouvellement passe par la génération d'une nouvelle bi-clé et une nouvelle demande de certificat (cf. chapitre 4.1). Le RC s'engage, en acceptant les CGU, à générer une nouvelle bi-clé à chaque demande.

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

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

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des serveurs, et les certificats correspondants, sont renouvelés au moins tous les trois ans (cf. période de validité chapitre 6.3.2).

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

Le déclenchement de la fourniture d'un nouveau certificat est à l'initiative du RC (pas d'existence de processus automatisé).

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

La génération de la CSR reste toujours sous la responsabilité du RC, de l'opérateur d'AE, de l'opérateur d'AED ou le cas échéant du MC. L'importation du nouveau certificat est également effectuée sous la responsabilité du RC.

4.8. Modification du certificat

La modification des certificats n'est pas autorisée. En cas de nécessité de changement d'informations présentes dans le certificat (principalement le DN), un nouveau certificat doit être délivré après révocation de l'ancien.

4.9. Révocation et suspension des certificats

4.9.1. Causes possibles d'une révocation

Certificats des serveurs

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat :
- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple, changement de société du serveur), ceci avant l'expiration normale du certificat ;
- Le RC n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le RC, l'entité, le cas échéant le MC ou l'opérateur d'AED, n'a pas respecté ses obligations découlant de la PC;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- La clé privée du serveur est suspectée de compromission, est compromise, est perdue ou volée (ou éventuellement les données d'activation associées à la clé privée) ;
- Le RC, le représentant légal de l'entité à laquelle il appartient, le cas échéant le MC, ou l'opérateur d'AED demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du serveur et/ou de son support) ;
- L'arrêt définitif du serveur ou la cessation d'activité de l'entité de rattachement du serveur ;
- Le certificat de signature de l'AC est révoqué (ce qui entraîne la révocation de tous les certificats en cours de validité signés par la clé privée correspondante);
- Pour des raisons techniques (échec de l'envoi du certificat, …).

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance, le certificat concerné est révoqué.

Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC :
- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la présente PC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

4.9.2. Origine d'une demande de révocation

Certificats des serveurs

Les personnes ou entités qui peuvent demander la révocation d'un certificat de serveur sont les suivantes :
- Le RC du certificat ;
- Un représentant légal de l'entité à laquelle est rattaché le RC ;
- Le cas échéant le MC;
- L'AC;
- L'AE ou AED.

Le RC est informé, en particulier par le biais des CGU qu'il a acceptées, des personnes ou entités susceptibles d'effectuer une demande de révocation pour le certificat.

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.

4.9.3. Procédure de traitement d'une demande de révocation

Certificat de serveurs

La demande de révocation est effectuée auprès de l'AE, d'un MC ou de l'AC.

Les étapes sont les suivantes :
- Le demandeur de la révocation transmet sa demande à l'AE, par courrier ou en ligne ;
- L'AE authentifie et valide la demande de révocation selon les exigences décrites au chapitre 3.4 ;
- Le numéro de série du certificat est inscrit dans la LCR et la base de certificats, utilisé pour le répondeur OCSP, est mise à jour ;
- Dans tous les cas, le RC est informé de la révocation par mail ;
- L'opération est enregistrée dans les journaux d'événements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat;
- L'AC ne publie pas dans la LCR les causes de révocation des certificats.

Certificats d'une composante de l'IGC

Dans le cas où l'AC racine Certigna Root CA décide de révoquer le certificat de l'AC (suite à la compromission d’une des clés privées), cette dernière informe par mail l'ensemble des RC que leurs certificats ne sont plus valides car l'un des certificats de la chaîne de certification n'est plus valide. Cette information sera relayée également directement auprès des entités et le cas échéant de leur MC.

Le contact identifié sur le site du SGMAP (http://www.ssi.gouv.fr) est immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification.

Le SGMAP et l'ANSSI se réservent le droit de diffuser par tout moyen l'information auprès des promoteurs d'application au sein des autorités administratives et auprès des usagers.

4.9.4. Délai accordé au RC pour formuler la demande de révocation

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

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

Certificats de serveurs

La fonction de gestion des révocations est disponible les heures ouvrées pour les révocations en ligne.

Dans tous les cas, le délai maximum de traitement d'une demande de révocation est de 72 heures. 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.

La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations est de 2 heures les jours ouvrés.

La durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations est de 16 heures les jours ouvrés.

Certificats d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un événement décrit dans les causes de révocation possibles pour ce type de certificat.

La révocation du certificat de signature de l'AC (signature de certificats/LCR/réponses OCSP) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

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

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

4.9.7. Fréquence d'établissement des LCR

La LCR est émise au minimum toutes les 24 heures. En outre, une nouvelle LCR est systématiquement et immédiatement publiée après la révocation d'un certificat.

4.9.8. Délai maximum de publication d'une LCR

Une LCR est publiée dans un délai maximum de 30 minutes suivant sa génération.

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

L'AC Certigna dispose d'un répondeur OCSP disponible aux adresses suivantes : http://servicesca.ocsp.certigna.fr et http://servicesca.ocsp.dhimyotis.com en complément à la publication des LCR sur les sites en ligne.

Le répondeur OCSP répond aux exigences d'intégrité, de disponibilité et de délai de publication décrites dans cette PC.

Les réponses OCSP sont signées avec la clé privée associée à un certificat dédié à cet usage et qui est émis par l'AC.

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

Cf. 4.9.6

4.9.11. Autres moyens disponibles d'information sur les révocations

Sans objet

4.9.12. Exigences spécifiques en cas de compromission de la clé privée

Les RC sont tenus d'effectuer une demande de révocation dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée. Pour les certificats d'AC, outre les exigences du chapitre 4.9.3 ci-dessus, la révocation suite à une compromission de la clé privée fait 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.).

En cas de compromission de sa clé privée ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le RC s'oblige à interrompre immédiatement et définitivement l'usage du certificat et de la clé privée qui lui est associée. Pour rappel, cet engagement est pris lors de l'acceptation des CGU.

4.9.13. Suspension de certificat

Les certificats ne peuvent pas être suspendus.

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

4.10.1. Caractéristiques opérationnelles

L'AC fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante, c'est à dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR/LAR et l'état du certificat de l'AC Certigna Root CA.

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR/LAR. Ces LCR/LAR sont des LCR au format V2, publiées sur le site Web de publication (accessible avec le protocole HTTP).

4.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24 heures sur 24, 7 jours sur 7.

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4 heures (jours ouvrés) et une durée maximale totale d'indisponibilité par mois de 32 heures (jours ouvrés).

En cas de vérification en ligne du statut d'un certificat, le temps de réponse du serveur OCSP à la requête reçue est au maximum de 10 secondes. Il s'agit de la durée mesurée au niveau du serveur (requête reçue par le serveur et réponse au départ de ce dernier).

4.11. Fin de la relation entre le RC et l'AC

En cas de fin de relation contractuelle ou réglementaire entre l'AC et le RC avant la fin de validité du certificat, pour une raison ou pour une autre, le certificat est révoqué.

4.12. Séquestre de clé et recouvrement

Le séquestre des clés privées d’AC est interdit.

Les clés privées des serveurs ne font pas l’objet de séquestre.

5. Mesures de sécurité non techniques

RAPPEL - L'AC a mené 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. Sa DPC a été élaborée en fonction de cette analyse.

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

Ces informations sont précisées dans la DPC.

5.1.2. Accès physique

Un contrôle strict d'accès physique aux composants de l'IGC est effectué, avec journalisation des accès et vidéo-surveillance : le périmètre de sécurité défini autour des machines hébergeant les composantes de l'IGC n'est accessible qu'aux personnes disposant d'un rôle de confiance sur cette IGC.

En dehors des heures ouvrables, la mise en œuvre de moyens de détection d'intrusion physique et logique renforce la sécurité de l'IGC. En outre, toute personne (prestataire externe, etc.) entrant dans ces zones physiquement sécurisées ne peut pas être laissée, pendant une période de temps significative, sans la surveillance d'une personne autorisée.

5.1.3. Alimentation électrique et climatisation

Des mesures concernant la fourniture d'énergie électrique et de climatisation sont prises pour répondre aux engagements de l'AC décrits dans la présente PC sur la garantie du niveau de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et les fonctions d'information sur l'état des certificats.

5.1.4. Vulnérabilité aux dégâts des eaux

Des mesures concernant la protection contre les dégâts des eaux sont prises pour répondre aux engagements de l'AC décrits dans la présente PC sur la garantie du niveau de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et les fonctions d'information sur l'état des certificats.

5.1.5. Prévention et protection incendie

Des mesures concernant la prévention et la protection contre les incendies sont prises pour répondre aux engagements de l'AC décrits dans cette PC sur la garantie du niveau de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et les fonctions d'information sur l'état des certificats.

5.1.6. Conservation des supports

Des mesures concernant la protection des informations intervenant dans l'activité de l'IGC sont prises pour répondre aux besoins de sécurité identifiés dans l'analyse de risque.

L'AC maintient un inventaire des informations dans la liste des biens sensibles. Des mesures spécifiques sont mises en place pour éviter la compromission et le vol de ces informations.

Des procédures de gestion protègent les 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.

5.1.7. Mise hors service des supports

Les mesures prises pour la mise hors service des supports d'informations sont en conformité avec le niveau de confidentialité des informations correspondantes.

5.1.8. Sauvegardes hors site

L'IGC met en œuvre du mirroring entre le site principal et le site de secours assurant une sauvegarde des applications et des informations des composantes de l'IGC. Ce mirroring permet une continuité de l'activité en cas d'interruption de service sur le site principal et permet à l'IGC de respecter ses engagements en termes de disponibilité.

5.2. Mesures de sécurité procédurales

5.2.1. Rôles de confiance

Chaque composante de l'IGC distingue 5 rôles fonctionnels de confiance :

- **Responsable de sécurité -** Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est également responsable des opérations de génération et de révocation des certificats. Il délègue le rôle d'opérateur d'AC à une ou plusieurs personnes au sein de l'IGC, tout en conservant la responsabilité des opérations effectuées sur cette composante.

- **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.

- **Administrateur système -** Il est chargé de la mise en route, de la configuration, de l'installation et de la maintenance technique des équipements informatiques de l'AC pour l'enregistrement, la génération des certificats, et la gestion des révocations. Il assure l'administration technique des systèmes et des réseaux de la composante.

- **Opérateur -** Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.

- **Contrôleur -** Personne 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.

- **Porteur de part de secret -** Il a la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui lui sont confiées.

Les différents rôles sont définis dans la description des postes propres à chaque entité opérant une des composantes de l'IGC sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles déterminent 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.

Des mesures sont 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.

5.2.2. Nombre de personnes requises par tâche

Pour des raisons de disponibilité, chaque tâche doit pouvoir être effectuée par au moins deux personnes. Au minimum, chacune des tâches suivantes est affectée sur deux personnes distinctes :
- Administrateur système ;
- Opérateur.

Pour certaines tâches sensibles (par exemple la cérémonie des clés), plusieurs personnes sont requises pour des raisons de sécurité et de « dual control ».

5.2.3. Identification et authentification pour chaque rôle

Chaque attribution de rôle à un membre du personnel de l'IGC est notifiée par écrit. Ce rôle est clairement mentionné et décrit dans sa fiche de poste. Il est accepté explicitement par la personne concernée. L'AC fait vérifier l'identité et les autorisations de tout membre de son personnel avant l'attribution des privilèges relatifs à ses fonctions.

L'attribution d'un rôle à un membre du personnel de l'IGC suit en particulier une procédure stricte avec signature de procès-verbaux pour l'attribution de tous les éléments nécessaires à l'exécution de ce rôle dans l'IGC (clés, codes d'accès, clés cryptographiques, etc.).

5.2.4. Rôle exigeant une séparation des attributions

Concernant les rôles de confiance, les cumuls suivants sont interdits au sein de l'IGC :
- responsable de sécurité et administrateur système/opérateur/contrôleur ;
- administrateur système, opérateur et contrôleur ;

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

5.3.1. Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC doivent signer la charte de sécurité interne. Cette charte comporte notamment une clause de confidentialité qui s'applique tant à l'égard des tiers que des utilisateurs. Elle liste les rôles de chaque employé au sein de l'IGC. Elle est co-signée par l'employé et le responsable de sécurité.

L'adéquation des compétences des personnels intervenant dans l'IGC est vérifiée par rapport à ses attributions sur les composantes de cette dernière.

Le personnel d'encadrement, le responsable sécurité, les administrateurs système, disposent des expertises nécessaires à l'exécution de leur rôle respectif et sont familiers aux procédures de sécurité appliquées à l'exploitation de l'IGC.

L'AC informe tout employé intervenant dans des rôles de confiance de l'IGC de ses responsabilités relatives aux services de l'IGC et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2. Procédures de vérification des antécédents

L'AC s'assure que tout employé intervenant sur l'IGC n'a pas subi de condamnation de justice en contradiction avec ses attributions. L'employé doit à cet effet fournir une copie du bulletin n°3 de son casier judiciaire. Cette vérification est renouvelée périodiquement (au minimum tous les 3 ans).

De plus, l'AC s'assure que l'employé ne souffre pas de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

5.3.3. Exigences en matière de formation initiale

Une formation initiale aux logiciels, matériels et procédures internes de fonctionnement et de sécurité est dispensée aux employés. Cette formation est en adéquation avec le rôle que l'AC leur attribue.

Une sensibilisation sur les implications des opérations dont ils ont la responsabilité est également opérée.

5.3.4. Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation.

5.3.5. Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6. Sanctions en cas d'actions non autorisées

Tout membre du personnel de l'AC agissant en contradiction avec les politiques et les procédures établies ici et les processus et procédures internes de l'IGC, soit par négligence, soit par malveillance, verra ses privilèges révoqués et fera l'objet de sanctions administratives, voire de poursuites judiciaires.

5.3.7. 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 5.3. Ceci est traduit en clauses adéquates dans les contrats avec ces prestataires. Le cas échéant, si le niveau d'intervention le requiert, il peut être demandé au prestataire de signer la charte interne de sécurité et/ou de fournir des éléments de vérification d'antécédents.

5.3.8. Documentation fournie au personnel

Chaque employé dispose de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, l'AC lui remet les politiques de sécurité l'impactant.

Les opérateurs disposent notamment des manuels d'opérateurs correspondant aux composantes sur lesquelles ils interviennent (AE, AC).

5.4. Procédures de constitution des données d'audit

Les événements pertinents intervenant dans la gestion et l'exploitation de l'IGC sont enregistrés sous forme manuscrite ou sous forme électronique (par saisie ou par génération automatique) et ce, à des fins d'audit.

5.4.1. Type d'événements à enregistrer

Les systèmes d'exploitation des serveurs de l'IGC journalisent les événements suivants, automatiquement dès leur démarrage et sous forme électronique (liste non exhaustive) :

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Evénements liés à la 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 événements sont aussi recueillis. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques :
- Les accès physiques (enregistrés électroniquement) ;
- Les accès logiques aux systèmes ;
- Les actions de maintenance et de changement de la configuration des systèmes enregistrés manuellement ;

- 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 RC).

Des événements spécifiques aux différentes fonctions de l'IGC sont également journalisés :
- Evénements liés aux clés de signature et aux certificats d'AC ou aux données d'activation (génération, sauvegarde et récupération, révocation, destruction, destruction des supports,...) ;
- Réception d'une demande de certificat (initiale et renouvellement) ;
- Validation / rejet d'une demande de certificat ;
- Génération des certificats des serveurs ;
- Transmission des certificats aux RC et, selon les cas, acceptations / rejets explicites par les RC ;
- Publication et mise à jour des informations liées à l'AC (PC/DPC, certificats d'AC, CGU, etc.)
- Réception d'une demande de révocation ;
- Validation / rejet d'une demande de révocation ;
- Génération puis publication des LCR;
- Destruction des supports contenant des renseignements personnels sur les RC.

Le processus de journalisation permet un enregistrement en temps réel des opérations effectuées. En cas de saisie manuelle, l'écriture est faite sauf exception le même jour ouvré que l'événement.

5.4.2. Fréquence de traitement des journaux d'événements

Cf. chapitre 5.4.8

5.4.3. Période de conservation des journaux d'événements

Le délai de conservation des journaux d'événements sur site est de 1 mois. L'archivage des journaux d'événements est effectué au plus tard 1 mois après leur génération.

5.4.4. Protection des journaux d'événements

Seuls les membres dédiés de l'AC sont autorisés à traiter ces fichiers.

Les systèmes générant les journaux d'événements (exceptés les systèmes de contrôle d'accès physique) sont synchronisés sur une source fiable de temps UTC (cf. 6.8. Horodatage / système de datation).

5.4.5. Procédure de sauvegarde des journaux d'événements

Des mesures de sécurité sont mises en place par chaque entité opérant une composante de l'IGC afin de garantir l'intégrité et la disponibilité des journaux d'événements pour la composante considérée, conformément aux exigences de la présente PC. Une sauvegarde est effectuée à fréquence élevée afin d'assurer la disponibilité de ces informations.

5.4.6. Système de collecte des journaux d'événements

Des détails sont donnés dans la DPC.

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

Sans objet.

5.4.8. Evaluation des vulnérabilités

Les journaux d'événements sont contrôlés une fois par jour ouvré pour identifier des anomalies liées à des tentatives en échec (accès ou opération).

Les journaux sont analysés dans leur totalité à la fréquence d'au moins 1 fois toutes les 2 semaines et dès la détection d'une anomalie. Un résumé d'analyse est produit à cette occasion.

Un rapprochement, entre les différents journaux d'événements de fonctions qui interagissent entre elles, est effectué à la fréquence d'au moins 1 fois par mois et ce, afin de vérifier la concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie.

L'auditeur se fait assister par une personne disposant des compétences liées aux différents environnements utilisés.

5.5. Archivage des données

5.5.1. Types de données à archiver

L'AC archive :
- Les logiciels (exécutables) constitutifs de l'IGC ;
- Les fichiers de configuration des équipements informatiques ;
- Les journaux d'événement des différentes composantes de l'IGC ;
- La PC;
- La DPC;
- Les demandes de certificats électroniques ;
- Les dossiers d'enregistrement des MC;
- Les dossiers d'enregistrement des opérateurs d'AED ;
- Les dossiers de demande de certificat, avec les justificatifs d'identité ;
- Les certificats émis ;
- Les demandes de révocation ;
- Les LCR émises ;
- Les réponses OCSP.

5.5.2. Période de conservation des archives

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable, en particulier à l'article 6-II du décret d'application n°2001-272 du 30 mars 2001.

En l'occurrence, il est archivé pendant au moins sept ans, comptés au maximum à partir de l'acceptation du certificat par le RC. Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat peut être présenté par l'AC lors de toute sollicitation par les autorités habilitées. Ce dossier, complété par les mentions consignées par l'AE ou le MC, doit permettre de retrouver l'identité réelle du serveur désigné dans le certificat émis par l'AC.

Certificats, LCR / LAR et réponses OCSP émis par l'AC

Les certificats des serveurs et d'AC, ainsi que les LCR / LAR, sont archivés pendant au moins cinq ans après leur expiration.

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

Journaux d'événements

Les journaux d'événements traités au 5.4 sont archivés pendant dix ans après leur génération.

5.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives sont protégées en intégrité. Elles peuvent être relues et exploitées par les membres dédiés de l'AC. L'accès en écriture à ces fichiers est protégé (gestion des droits). L'accès en lecture à ces journaux (stockés sur les serveurs NetApp) n'est possible qu'à partir d'une machine identifiée et autorisée des réseaux internes.

5.5.4. Procédure de sauvegarde des archives

Le procédé de mirroring (automatique ou manuel en cas de reprise) garantit l'existence d'une copie de secours de l'ensemble des archives.

5.5.5. Exigences d'horodatage des données

Les données sont datées conformément au chapitre 6.8.

5.5.6. Système de collecte des archives

Pas de procédure particulière. La sauvegarde et l'archivage sont réalisés sur les deux serveurs d'archivage (par réplication et consolidation).

5.5.7. Procédures de récupération et de vérification des archives

Les archives peuvent être récupérées uniquement par les membres dédiés de l'AC autorisés à traiter ces fichiers dans un délai maximal de deux jours ouvrés.

Les données concernant les contractants peuvent être récupérées à leur demande.

5.6. Renouvellement d'une clé de composante de l'IGC

5.6.1. 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 du 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 est 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.

L'IGC Certigna communiquera en temps utiles sur son site en cas de génération d'un nouveau certificat d'AC, en invitant les utilisateurs à télécharger la nouvelle chaîne de certification.

5.6.2. Clés des autres composantes

Les bi-clés et certificats associés des composantes de l'IGC sont renouvelés soit dans les trois mois précédant leur expiration ou après révocation du certificat en cours de validité.

5.7. Reprise suite à compromission et sinistre

L'AC établit des procédures visant à assurer le maintien, dans la mesure du possible, des activités et décrit, dans ces procédures, les étapes prévues en cas de corruption ou de perte de ressources informatiques, de logiciels et de données.

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

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC.

Le cas de l'incident majeur est impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, sera faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé, etc.).

De même, si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses porteurs/ serveurs devient insuffisant pour son utilisation prévue restante, alors l'AC :

- informera tous les RC 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 sera mise à disposition des autres utilisateurs de certificats ;
- révoquera tout certificat concerné.

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

Chaque composante de l'IGC est intégrée dans le plan de continuité d'activité (PCA) de la société afin de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant des engagements de l'AC et des résultats de l'analyse de risque de l'IGC, notamment en ce qui concerne les fonctions liées à la publication et/ou liées à la révocation des certificats. Ce plan est testé au minimum une fois tous les trois ans.

5.7.3. 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 est traité dans le plan de continuité d'activité de la composante en tant que sinistre (cf. chapitre 5.7.2).

Dans le cas de compromission d'une clé d'AC, le certificat correspondant sera immédiatement révoqué (cf. chapitre 4.9). De même, tous les certificats serveurs en cours de validité émis par cette AC seront révoqués. En outre, l'AC respecte au minimum les engagements suivants :
- elle informe les entités suivantes de la compromission : tous les RC, MC 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 est mise à disposition des autres tiers utilisateurs ;
- elle indique notamment que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

Remarque : Dans le cas de l'AC Certigna Root CA, le certificat de signature n'étant pas révocable, ce sont les certificats des autorités intermédiaires qui sont révoqués en cas de compromission de la clé privée de l'AC Certigna Root CA.

5.7.4. Capacité de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la PC de l'AC (cf. chapitre 5.7.2).

L'existence de deux sites redondants (site principal et site secondaire), de liens de communication redondants et des procédures de bascule sur l'un et l'autre des deux sites garantit la continuité de service de chacune des composantes de l'IGC. Cette capacité est mise en évidence dans le PCA de la société.

5.8. Fin de vie de l'IGC

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

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

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

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

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à les transférer à une autre entité. Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AC prend les mesures suivantes :

- Elle assure la continuité du service d'archivage, en particulier des certificats et des dossiers d'enregistrement ;
- Elle assure la continuité du service de révocation, conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC;
- Elle prévient les RC dans le cas où les changements envisagés peuvent avoir des répercussions sur les engagements pris et ce, au moins sous le délai de 1 mois ;
- Elle communique aux responsables d'applications listés au chapitre 1.4.1 les principes du plan d'action destinés à faire face à la cessation d'activité ou à organiser le transfert d'activité ;
- Elle effectue une information auprès des autorités administratives. En particulier le contact auprès de le SGMAP est averti (http://www.ssi.gouv.fr). L'AC l'informera notamment de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus de transfert ou de cessation d'activité.

Cessation d'activité affectant l'AC

Dans l'hypothèse d'une cessation d'activité totale, avant que l'AC ne mette un terme à ses services, elle effectue les procédures suivantes :

- Elle informe tous les RC, les autres composantes de l'IGC et les tiers par mail de la cessation d'activité. Cette information sera relayée également directement auprès des entités et le cas échéant de leur MC;
- Elle révoque tous les certificats qu'elle a signés et qui sont encore valides ;
- Elle révoque son certificat ;
- Elle détruit la clé privée stockée dans le module cryptographique, ainsi que le contexte du module. Les porteurs de secret (clé privée et contexte) sont convoqués et détruisent leur(s) part(s) de secret. Elle s'interdit en outre de transmettre sa clé à des tiers.

Si l'AC est en faillite, c'est au tribunal de commerce de décider de la suite à donner aux activités de l'entreprise. Néanmoins, le cas échéant, Dhimyotis s'engage à accompagner le tribunal de commerce dans les conditions suivantes : avant une faillite, il y a une période préalable, générée la plupart de temps soit par plusieurs procédures d'alerte du commissaire aux comptes soit par un redressement judiciaire ; pendant cette période, Dhimyotis s'engage à préparer pour le tribunal de commerce, le cas échéant, une proposition de transfert des certificats numériques vers une autre autorité disposant d'une certification d'un niveau au moins égal au sien.

Le contact identifié sur le site de le SGMAP (http://www.ssi.gouv.fr) est immédiatement informé en cas de cessation d'activité de l'AC. Le SGMAP et l'ANSSI se réservent le droit de diffuser par tout moyen l'information auprès des promoteurs d'application au sein des autorités administratives et auprès des usagers.

L'AC tient informées le SGMAP et l'ANSSI de tout obstacle ou délai supplémentaires rencontrés dans le déroulement du processus.

6. Mesures de sécurité techniques

6.1. Génération et installation de bi-clés

6.1.1. Génération des bi-clés

Clés d'AC

Ce chapitre décrit le contexte de génération de la bi-clé de l'AC.

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé (cf. chapitre 5).

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique. La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnes dans des rôles de confiance (cf. chapitre 5.2.1), dans le cadre de « cérémonies de clés ». Ces personnes sont identifiées dans un document interne à l'IGC Certigna.

La cérémonie se déroule suivant un script préalablement défini :
- Elle se déroule sous le contrôle d'au moins une personne ayant un rôle de confiance au sein de l'IGC 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.

La génération des clés de signature d'AC s'accompagne de la génération de parts de secrets.

Les parts de secret d'IGC 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. Ces secrets sont des parties de la clé privée de l'AC décomposée suivant un schéma à seuil de Shamir (3 parties parmi 5 sont nécessaires pour reconstituer la clé privée).

Suite à leur génération, les parts de secrets ont été remises à leurs porteurs désignés au préalable et habilités à ce rôle de confiance par l'AC. Un seul porteur ne peut détenir qu'une seule part de secret d'une même AC. Les parts de secret sont placées dans des enveloppes scellées, placées elles-mêmes dans des coffres de banque.

Clés générées par le RC

La bi-clé d'un serveur est générée exclusivement sur un dispositif répondant aux exigences du chapitre 11, soit sous le contrôle du RC soit sous le contrôle de l’AC. Le RC s'engage de manière contractuelle, en acceptant les conditions générales d'utilisation, à respecter les exigences quant au dispositif qu'il utilise pour générer et stocker sa clé privée, si ce dernier n'est pas fourni par l'AC.

L'AC prendra le cas échéant les mesures nécessaires pour obtenir les informations techniques sur le dispositif du serveur et se réserve le droit de refuser la demande de certificat s'il était avéré que ce dispositif ne réponde pas à ces exigences.

Clés générées par l'AC

La génération des clés des serveurs au format logiciel est effectuée dans un environnement sécurisé. La bi-clé du serveur est générée par l'AE et est protégé par un mot de passe. La bi-clé et le mot de passe associé ne sont jamais détenus en même temps par une même personne. Le mot de passe est transmis par téléphone (ou en cas d'échec, par mail) au RC.

6.1.2. Transmission de la clé privée à son propriétaire

Dans le cas où l'AC génère la bi-clé, elle est transmise de manière sécurisée au RC.

La clé privée est protégée par une donnée d'activation transmise au RC qu'il changera lors de l'acceptation du certificat.

6.1.3. Transmission de la clé publique à l'AC

Si la bi-clé n'est pas générée par l'AE, la demande de certificat (format PKCS#10), contenant la clé du serveur, est transmise à l'AE. Cette demande est signée avec la clé privée du serveur, ce qui permet à l'AE d'en vérifier l'intégrité et de s'assurer que le serveur possède la clé privée associée à la clé publique transmise dans cette demande. Une fois ces vérifications effectuées, l'AE signe la demande puis la transmet à l'AC.

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

La délivrance de la clé publique de l'AC, qui permet à tous ceux qui en ont besoin de valider un certificat émis par l'AC en vertu de cette PC, est effectuée par un moyen garantissant intégrité et authentification de cette clé publique.

La clé publique de l'AC est diffusée dans un certificat lui-même signé par l'AC racine Certigna Root CA dont La clé publique est diffusée dans un certificat auto-signé.

Ces clés publiques d'AC, ainsi que leurs valeurs de contrôle, sont diffusées et récupérées par les systèmes d'information de tous les accepteurs de certificats par l'intermédiaire du site Internet de Certigna à l'adresse http://www.certigna.fr et http://www.dhimyotis.com (cf. 2.2.2. Publication des certificats d'AC).

6.1.5. Taille des clés

Clés d'AC

- AC Certigna Root CA
  La bi-clé d'AC est de type RSA 4096 bits
  L'algorithme de hachage est de type SHA-256 (256 bits)

- AC Certigna Services CA
  La bi-clé d'AC est de type RSA 4096 bits
  L'algorithme de hachage est de type SHA-256 (256 bits)

Clés des serveurs

Les bi-clés des services sont de type RSA 2048 bits
L'algorithme de hachage est de type SHA-256 (256 bits)

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

Les paramètres et les algorithmes de signature mis en œuvre dans les boîtiers cryptographiques, les supports matériels et logiciels sont documentés par l'AC.

Clés d'AC

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

Clés des serveurs

L'équipement de génération de bi-clés employé par le RC utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

6.1.7. Objectifs d'usage de la clé

Clés d'AC

L'utilisation de la clé privée de l'AC et du certificat associé est exclusivement limitée à la signature de certificats et de LCR (cf. chapitre 1.4.1).

Clés des serveurs

Les RC doivent respecter strictement les usages autorisés des bi-clés et des certificats cités au chapitre 1.5.1. Dans le cas contraire, leur responsabilité pourrait être engagée.

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

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

Modules cryptographiques de l'AC

Les modules cryptographiques utilisés par l'AC Certigna Root CA et l'AC Certigna Services CA pour la génération et la mise en œuvre de leurs clés de signature sont des boitiers Trustway Proteccio de la société BULL.

Ces boitiers sont des ressources exclusivement accessibles aux serveurs d'AC via un VLAN dédié.

Dispositifs de protection des clés privées des serveurs

Le module cryptographique logiciel ou matériel utilisé pour la protection et la mise en œuvre des clés privées des serveurs doit être conforme aux exigences du chapitre 11. Annexe 2 : exigences de sécurité du dispositif de protection des clés privées.

Dans le cas où c'est l'AC qui met en œuvre ces dispositifs, l'AC s'assure que :
- leur préparation est contrôlée de façon sécurisée ;
- ils sont stockés et distribués de façon sécurisée ;
- leur désactivation et réactivation sont contrôlées de façon sécurisée.

6.2.2. Contrôle de la clé privée par plusieurs personnes

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

La génération de la bi-clé est traitée au chapitre 6.1.1, l'activation de la clé privée au chapitre 6.2.8 et sa destruction au chapitre 6.2.10.

Le contrôle des clés privées de signature de l'AC est assuré par du personnel de confiance (porteurs de secrets d'AC) 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).

Dans la pratique, à la génération du secret, ce dernier est partagé en cinq parts et trois porteurs doivent être réunis pour reconstituer le secret (selon la méthode du partage de Shamir). Chaque part de secret est détenue dans un coffre attribué à son porteur.

6.2.3. Séquestre de la clé privée

Clés d'AC

Les clés privées d'AC ne sont jamais séquestrées.

Clés des serveurs

Les clés privées des serveurs ne font pas l'objet de séquestre.

6.2.4. Copie de secours de la clé privée

Clé d'AC

Les clés de l'AC font l'objet d'une copie de secours hors du module cryptographique. Cette copie est chiffrée au sein du module cryptographique. La durée de vie de la copie de secours (sous forme d'un fichier unique) est limitée dans le temps. Cette copie est en effet partagée entre plusieurs porteurs (partage de Shamir). Une fois ce partage effectué, toute trace de la copie de secours est effacée (effacement sécurisé) de la machine hôte sur laquelle la copie a été générée. L'AC garantit que les clés d'AC ne sont pas compromises pendant leur stockage ou leur transport.

Clés des serveurs

Les clés privées des serveurs ne font pas l'objet de copie de secours.

6.2.5. Archivage de la clé privée

Clé d'AC

La clé privée de l'AC n'est en aucun cas archivée.

Clés des serveurs

Les clés privées des serveurs ne sont en aucun cas archivées ni par l'AC, ni par l'une de ses composantes.

6.2.6. Transfert de la clé privée avec le module cryptographique

Pour rappel, les clés privées des serveurs sont générées sous la responsabilité de l'opérateur d'AE, d'AED, du MC ou du RC.

Les clés privées d'AC sont générées dans le module cryptographique. Comme décrit en 6.2.4, les clés privées d'AC ne sont exportables/importables du module cryptographique que sous forme chiffrée.

6.2.7. Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC sont générées et stockées dans un module cryptographique décrit au chapitre 6.2.1 conformément aux exigences du chapitre 6.2.4.

6.2.8. Méthode d'activation de la clé privée

Clés d'AC

L'activation des clés privées d'AC dans le module cryptographique (correspond à la génération ou la restauration des clés) est contrôlée via des données d'activation (cf. chapitre 6.4) et fait intervenir deux personnes ayant un rôle de confiance au sein de l'IGC (responsable sécurité, et un opérateur habilité à administrer le module cryptographique).

Clés des serveurs

Le RC reçoit par téléphone (ou en cas d'échec, par mail) les données d'activation de son certificat (mot de passe pour utiliser son certificat) qu'il modifiera au moment de l'acceptation du certificat.

6.2.9. Méthode de désactivation de la clé privée

Clés d'AC

Le module cryptographique résiste aux attaques physiques, par effacement des clés privées d'AC. Le module est apte à détecter les attaques physiques suivantes : ouverture du dispositif, retrait ou forçage.

Clés des serveurs

La méthode de désactivation de la clé privée dépend du module cryptographique utilisé par le RC.

6.2.10. Méthode de destruction des clés privées

Clés d'AC

En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), la clé est systématiquement détruite, ainsi que les parts de secrets permettant de la reconstituer. Un procès-verbal de destruction de la clé et des parts de secret est établi à l'issue de cette procédure.

Clés des serveurs

Le RC étant l'unique détenteur de sa clé privée, il est le seul à pouvoir la détruire (effacement de la clé ou destruction physique du dispositif).

6.2.11. Niveau d'évaluation sécurité du module cryptographique

Le niveau d'évaluation du module cryptographique de l'AC est précisé au chapitre 6.2.1.

Les dispositifs de protection des certificats de RC sont évalués au niveau requis pour l'usage visé, tel que précisé au chapitre 11 ci-dessous.

6.3. Autres aspects de la gestion des bi-clés

6.3.1. Archivage des clés publiques

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

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

Les bi-clés et les certificats des serveurs couverts par la présente PC ont une durée de validité de 3 ans maximum en fonction du contrat souscrit.

Pour l'IGC Certigna, la durée de validité du certificat de l'AC Certigna Root CA est de 20 ans, et celle du certificat de l'AC Certigna Services CA est de 18 ans.

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

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

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

La génération et l'installation des données d'activation du module cryptographique de l'AC s'effectuent lors de la phase d'initialisation et de personnalisation de ce module (cf. chapitre 6.1.1).

Les données d'activation correspondent au code PIN des cartes à puce d'administration du module cryptographique.

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

Pour un certificat remis sur support logiciel, les données d'activation sont transmises au RC par téléphone (ou en cas d'échec, par mail).

6.4.2. Protection des données d'activation

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

Les données d'activation ne sont en aucune manière conservées sous forme électronique ou manuscrite. Il s'agit pour rappel d'une carte 'administrateur' et du code PIN associé, détenus respectivement par le responsable sécurité et l'administrateur du module cryptographique.

En cas de panne matérielle ou d'oubli des données d'activation, il existe une seconde carte 'administrateur' dont le code PIN est détenu par le second administrateur.

Protection des données d'activation correspondant aux clés privées des serveurs

Si la bi-clé est générée par l'AE, elle génère également les données d'activation qui sont envoyés par SMS (ou, en cas d'échec, par mail) au RC, ces données d'activation ne sont pas sauvegardées par l'AE et sont modifiées par le RC lors de l'acceptation du certificat.

Une fois les données d'activation transmises au RC, l'AE ne peut plus les renvoyer. Si le RC génère lui-même son bi-clé, il génère de manière autonome et sous sa seule responsabilité ses données d'activation.

6.4.3. Autres aspects liés aux données d'activation

Sans objet.

6.5. Mesures de sécurité des systèmes informatiques

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité sur les systèmes informatiques des personnes occupant un rôle de confiance est assuré par :

- Identification et authentification forte des utilisateurs pour l'accès au système (contrôle d'accès physique pour entrer dans la salle + contrôle logique par identifiant / mot de passe ou par certificat pour accéder au système) ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- 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) ;
- Protection contre les virus informatiques et toutes formes de logiciel compromettant ou non autorisé et mises à jour des logiciels à l'aide du firewall ;
- 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 à l'aide du firewall;
- Communication sécurisée inter-site (tunnel VPN IPSec) ;
- Fonctions d'audit (non-répudiation et nature des actions effectuées).

Des dispositifs de surveillance (vidéosurveillance et alarme automatique) et des procédures d'audit des paramétrages du système, notamment des éléments de routage, sont mis en place.

6.5.2. Niveau d'évaluation sécurité des systèmes informatiques

Sans objet.

6.6. Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1. Mesures de sécurité liées au développement des systèmes

Conformément à l'analyse de risque menée, lors de la conception de tout nouveau projet de développement, une analyse sur le plan de la sécurité est réalisée et doit être approuvée par le Comité de Sécurité de l'AC.

La configuration des systèmes de l'AC ainsi que toute modification et mise à niveau sont documentées.

Le développement est effectué dans un environnement contrôlé et sécurisé exigeant un niveau élevé d'autorisation.

Afin de permettre à ses prospects ou futurs clients de tester ou de recetter certaines de leurs applications d'échange dématérialisé, l'AC a mis en place une AC de test émettant des certificats en tous points identiques aux certificats de production (seul l'émetteur du certificat diffère). Cette AC de test dispose d'une clé privée qui lui est propre. Le certificat de clé publique est auto-signé. La confiance à ce certificat nécessitant une approbation explicite de l'utilisateur, les certificats émis ont une utilisation restreinte à des fins de test exclusivement.

Les méthodes et les logiciels sont testés en premier lieu au sein de cet environnement de test Certigna avant d'être utilisés dans l'environnement de production.

Les environnements de production et de développement sont dissociés.

6.6.2. Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC est documentée et signalée à l'AC pour validation.

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

Sans objet.

6.7. Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement souhaité par l'AC.

Le réseau est équipé notamment de deux firewalls (mis en cluster) intégrant un système de détection des intrusions IPS (avec émission d'alertes).

L'AC garantit que les composants du réseau local sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de leur conformité avec les exigences spécifiées par l'AC.

6.8. Horodatage et Système de datation

Afin d'assurer une synchronisation entre les différentes datations d'événements, les différentes composantes de l'IGC synchronisent leurs horloges systèmes par rapport à une source fiable de temps UTC. Cette source est obtenue auprès de quatre serveurs de temps : Angers, Reims, IMAG (Grenoble), UNILIM (Limoges).

7. Profil des certificats et des LCR

Les certificats et les LCR produits par l'AC sont conformes au standard ITU-T Recommandation X.509 version 3.

7.1. Profil du certificat de l'AC

Champs de base

Champ	**Description**
Version	V3
Serial Number	Numéro de série unique
Signature	Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096
Issuer	DN={ } countryName : C=FR organizationName : O=Dhimyotis organizationUnitName : OU=0002 48146308100036 commonName : CN=Certigna Root CA
Validity	Dates et heures d'activation et d'expiration du Certificat
Subject	DN={ } countryName : C=FR organizationName : O=Dhimyotis organizationUnitName : OU=0002 48146308100036 organizationIdentifier : OI=NTRFR-48146308100036 commonName : CN= Certigna Services CA
Subject Public Key Info	RSA 4096 bits

Extensions

Champ	**C**	**Description**
Authority Key Identifier	N	Identifiant de la clé publique de l'autorité Certigna Root CA
Subject Key Identifier	N	Identifiant de la clé publique de l'autorité Certigna Services CA
Key Usage	O	Signature de certificat Signature de la liste de révocation
Certificate Policies	N	1.2.250.1.177.2.0.1.1 CPS=http://www.certigna.fr/autorites/
Authority Information Access	N	caIssuers=http://autorite.certigna.fr/certignarootca.der caIssuers=http://autorite.dhimyotis.com/certignarootca.der
CRL Distribution Points	N	URL=http ://crl.certigna.fr/certignarootca.crl URL=http ://crl.dhimyotis.com/certignarootca.crl
Basic Constraints	N	cA = TRUE PathLengthConstraint=0

7.2. Profil des certificats de serveurs

Authentification de type Serveur SSL/TLS *

Champs de base

Champ	Description
Version	V3
Serial Number	Numéro de série unique
Signature	Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096
Issuer	DN={ } countryName : C=FR organizationName : O=Dhimyotis organizationUnitName : OU=0002 48146308100036 organizationIdentifier : OI=NTRFR-48146308100036 commonName : CN=Certigna Services CA
Validity	Dates et heures d'activation et d'expiration du Certificat
Subject	DN={ } countryName : C=Pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée localityName : L=Ville où est implantée l'entité organizationName : O=Nom de l'entité à laquelle appartient le serveur organizationUnitName : OU=ICD + identifiant de l'entité à laquelle appartient le serveur informatique enregistré conformément à la législation et aux réglementations en vigueur organizationIdentifier : OI=Informations sur le justificatif d'identité de l'entité commonName : CN= un des FQDN du SAN serialNumber : Série de caractères composée d'un aléa pour l'unicité
Subject Public Key Info	RSA 2048

Extensions

Champ	C	Description
Authority Key Identifier	N	Identifiant de clé publique de l'autorité Certigna Services CA
Subject Key Identifier	N	Identifiant de la clé publique du serveur
Key Usage	O	Digital signature / Key Encipherment
Extended Key Usage	N	id-kp-serverAuth
Certificate Policies	N	2.23.140.1.2.2 1.2.250.1.177.2.5.1.1.1 / CPS=http://www.certigna.fr/autorites/
CRL Distribution Points	N	URL=http://crl.certigna.fr/servicesca.crl URL=http://crl.dhimyotis.com/servicesca.crl
Authority Information Access	N	URL=http://servicesca.ocsp.certigna.fr URL=http://servicesca.ocsp.dhimyotis.com caIssuers=http://autorite.certigna.fr/servicesca.der caIssuers=http://autorite.dhimyotis.com/servicesca.der
Basic Constraints	N	cA = FALSE
Subject Alternative Name	N	FQDN des différents domaines à protéger

Authentification serveur de type client *

Champs de base

Champ	Description
Version	V3
Serial Number	Numéro de série unique
Signature	Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096
Issuer	DN={ } countryName : C=FR organizationName : O=Dhimyotis organizationUnitName : OU=0002 48146308100036 organizationIdentifier : OI=NTRFR-48146308100036 commonName : CN=Certigna Services CA
Validity	Dates et heures d'activation et d'expiration du Certificat
Subject	DN={ } countryName : C=Pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée localityName : L=Ville où est implantée l'entité organizationName : O=Nom de l'entité à laquelle appartient le serveur organizationUnitName : OU=ICD + identifiant de l'entité à laquelle appartient le serveur informatique enregistré conformément à la législation et aux réglementations en vigueur organizationIdentifier : OI=Informations sur le justificatif d'identité de l'entité commonName : CN= FQDN du service applicatif ou identité du service sous la forme <identité de l'entité> - <Nom du service> serialNumber : série de caractères composée d'un aléa pour l'unicité
Subject Public Key Info	RSA 2048

Extensions

Champ	C	Description
Authority Key Identifier	N	Identifiant de clé publique de l'autorité Certigna Services CA
Subject Key Identifier	N	Identifiant de la clé publique du serveur
Key Usage	O	Digital signature
Extended Key Usage	N	id-kp-clientAuth
Certificate Policies	N	2.23.140.1.2.2 1.2.250.1.177.2.5.1.2.1 / CPS=http://www.certigna.fr/autorites/
CRL Distribution Points	N	URL=http://crl.certigna.fr/servicesca.crl URL=http://crl.dhimyotis.com/servicesca.crl
Authority Information Access		URL=http://servicesca.ocsp.certigna.fr URL=http://servicesca.ocsp.dhimyotis.com caIssuers=http://autorite.certigna.fr/servicesca.der caIssuers=http://autorite.dhimyotis.com/servicesca.der
Basic Constraints	N	cA = FALSE
Subject Alternative Name	N	Si CN = FQDN, alors le SAN contient la liste des FQDN des différents domaines

7.3. Profil des LCR

Champs de base

Champ	Description
Version	V2
Signature	Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096
Issuer	DN={ } countryName : C=FR organizationName : O=Dhimyotis organizationUnitName : OU=0002 48146308100036 organizationIdentifier : OI=NTRFR-48146308100036 commonName : CN=Certigna Services CA
This Update	Date de génération de la LCR
Next Update	Date de prochaine mise à jour de la LCR
Revoked certificates	Liste des n° de série des certificats révoqués

Extensions

Champ	C	Description
Authority Key Identifier	N	Identifiant de clé publique de l'autorité Certigna Services CA
CRL Number	N	Contient le numéro de série de la LCR

7.4. Traitement des extensions de certificats par les applications

Les extensions définies pour les certificats X509 V3 permettent d'associer des informations complémentaires à une clé publique, relatives au serveur ou à l'AC. Le caractère de criticité doit se traiter de la façon suivante selon que l'extension est critique ou non :

- si l'extension est non-critique, alors :
    - si l'application ne reconnaît pas l'OID, l'extension est abandonnée mais le certificat est accepté ;
    - si l'application reconnaît l'OID, alors :
        - si l'extension est conforme à l'usage que l'application veut en faire, l'extension est traitée.
        - si l'extension n'est pas conforme à l'usage que l'application veut en faire, l'extension est abandonnée, mais le certificat est accepté.
- si l'extension est critique, alors :
    - si l'application ne reconnaît pas l'OID, le certificat est rejeté ;
    - si l'application reconnaît l'OID, alors :
        - si l'extension est conforme à l'usage que l'application veut en faire, l'extension est traitée.
        - si l'extension n'est pas conforme à l'usage que l'application veut en faire, le certificat est rejeté.

Les extensions de la RFC 5280 décrites ci-dessous, doivent obligatoirement apparaître dans les certificats :

- **authorityKeyIdentifier :** Cette extension 'non critique' identifie la clé publique utilisée pour vérifier la signature sur un certificat. Elle permet de différencier les différentes clés utilisées par l'AC lorsque celle-ci dispose de plusieurs clés de signature.
    - Le champ authorityKeyIdentifier est obligatoirement renseigné. Il contient un identifiant unique (keyIdentifier). Cet identifiant de clé d'AC a la même valeur que le champ subject-KeyIdentifier du certificat de l'AC.
    - Les champs authorityCertIssuer et authorityCertSerialNumber ne sont pas renseignés.

- **keyUsage :** Cette extension définit l'utilisation prévue de la clé contenue dans le certificat. L'AC :
    - indique l'usage prévu de la clé comme défini au chapitre 7.2.
    - gère la criticité comme défini au chapitre 7.2.

- **certificatePolicies :** Cette extension 'non critique' définit les politiques de certification que le certificat reconnaît supporter et suivant lesquelles il a été créé. Ce champ est traité pendant la validation de la chaîne de certification. L'AC inclut le champ policyInformation en renseignant le champ policyIdentifier avec l'OID de la PC.

- **CRLDistributionPoints :** Cette extension 'non critique' identifie l'emplacement où l'utilisateur peut trouver la LCR indiquant si le certificat a été révoqué. L'AC remplit autant de champs distributionPoint, qu'elle offre de mode d'accès à la LCR. Chacun de ces champs comporte l'uniformRessourceIdentifier de la LCR.

- **SubjectKeyIdentifier :** Cette extension 'non critique' identifie la clé publique du serveur associée au certificat. Elle permet de distinguer les différentes clés utilisées par le RC. Sa valeur est la valeur contenue dans le champ keyIdentifier.

- **AuthorityInformationAccess :** Cette extension 'non critique' identifie (avec Method=OCSP) l'emplacement du(des) serveur(s) OCSP fournissant des informations sur le statut des certificats des serveurs.

Les extensions suivantes sont renseignées dans le certificat, quoique facultatives :

- **Extended Key Usage :** Cette extension 'non critique' définit l'utilisation avancée de la clé, fixée à 'authentification client' et 'sécurisation de la messagerie'

- **Basic Constraints :** Cette extension 'non critique' indique si le certificat est un certificat d'entité finale ou un certificat d'autorité.

8. 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 de l'Ordonnance n° 2005-1516 du 8 décembre 2005 (schéma de qualification des prestataires de services de confiance conformément au décret RGS) et, d'autre part, ceux que réalise ou fait réaliser l'AC afin de s'assurer que l'ensemble de son IGC (AED compris, ainsi que le cas échéant les MC) est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC. En l'occurrence, l'IGC Certigna fait appel à deux cabinets distincts pour les deux types d'audit et d'évaluation. Les chapitres suivants ne concernent que les audits et évaluations de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

L'AC peut réaliser des audits auprès des opérateurs d'AED ou des mandataires de certification au même titre que le personnel de son IGC. Il s'assure entre autres que les opérateurs d'AED ou les MC respectent les engagements vis-à-vis de sa PC et les pratiques identifiées dans sa DPC les concernant. A cette fin, la PC et la DPC leur sont remises.

8.1. Fréquences et/ou circonstances des évaluations

Un contrôle de conformité de l'AC a été effectué avant la première mise en service par rapport aux moyens et règles mentionnées dans la PC et dans la DPC.

Ce contrôle est également effectué une fois tous les trois ans, sur demande de Dhimyotis, par un organisme impartial dûment accrédité.

8.2. Identités/qualifications des évaluateurs

Le contrôle est 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.

8.3. Relations entre évaluateurs et entités évaluées

Les auditeurs et l'AC entretiennent une relation contractuelle relative à l'exécution des audits et les auditeurs sont suffisamment séparés de l'AC auditée d'un point de vue organisationnel pour fournir une évaluation objective et indépendante.

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

8.4. Sujets couverts par les évaluations

Les contrôles de conformité 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, . . .).

8.5. Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : « Amélioration », « remarque », « écart mineur », « écart majeur ».

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

- En cas d' « amélioration », et selon l'importance de l'amélioration, l'équipe d'audit émet des recommandations à l'AC pour améliorer son fonctionnement. Les améliorations sont laissées à l'appréciation de l'AC qui décide ou non des les mettre en place.
- En cas de résultat « remarque » ou « écart mineur », 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 d' « écart majeur », 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.

Chaque session d'audit permet de consulter les avis émis par l'équipe d'audit. Un contrôle de confirmation permettra de vérifier que tous les points critiques ont bien été résolus dans les délais.

8.6. Communication des résultats

Les résultats des audits de conformité effectués par le cabinet d'audit (audits récurrents) sont tenus à la disposition de l'organisme en charge de la qualification de l'AC.

9. Autres problématiques métiers et légales

9.1. Tarifs

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

La délivrance de certificats aux RC est facturée selon les tarifs affichés sur le site internet ou sur le formulaire de commande.

9.1.2. Tarifs pour accéder aux certificats

Sans objet.

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

Les informations d'état et de révocation des certificats sont libres d'accès.

9.1.4. Tarifs pour d'autres services

Le recouvrement des clés séquestrées est facturé selon des tarifs affichés sur le site internet. D'autres prestations pourront être facturées. Dans ce cas, les tarifs seront portés à la connaissance des personnes auxquelles ils s'appliquent et seront disponibles auprès de l'AC.

9.1.5. Politique de remboursement

La commande de CERTIFICAT ne peut être annulée dès lors que le dossier est en cours de traitement. Tout CERTIFICAT émis ne peut faire l'objet d'une demande de remboursement.

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

Dhimyotis a souscrit un contrat d'assurance responsabilité civile adapté aux technologies de l'information.

9.2.2. Autres ressources

Sans objet.

9.2.3. Couverture et garantie concernant les entités utilisatrices

Cf. chapitre 9.9.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :
- La partie non-publique de la DPC de l'AC;
- Les clés privées de l'AC, des composantes et des RC ;
- Les données d'activation associées aux clés privées d'AC et des serveurs ;
- Tous les secrets de l'IGC;
- Les journaux d'événements des composantes de l'IGC;
- Les dossiers d'enregistrement des serveurs ;
- Les causes de révocation des certificats.

9.3.2. Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3. Responsabilités en termes de protection des informations confidentielles

De manière générale les informations confidentielles ne sont accessibles qu'aux personnes concernées par de telles informations ou qui ont l'obligation de conserver et/ou traiter de telles informations.

Dès lors que les informations confidentielles sont soumises à un régime particulier régi par un texte législatif et réglementaire, le traitement, l'accès, la modification de ces informations sont effectués conformément aux dispositions des textes en vigueur.

L'AC applique des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles au 9.3.1, 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 en garantit l'intégrité. L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des RC à des tiers dans le cadre de procédures légales. Elle donne également accès à ces informations au RC, MC et le cas échéant à l'opérateur d'AED en relation avec le RC.

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

Toute collecte et tout usage de données à caractère personnel par l'AC sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, notamment par rapport à la CNIL et à l'article 226-13 (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002) du Code Pénal : "La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15000 euros d'amende."

Conformément à la loi informatique et libertés (article 40 de la loi du 6 janvier 1978), l'IGC Certigna donne aux RC un droit de rectification de leurs données personnelles en cas de données inexactes, incomplètes ou équivoques au moment de leur collecte. L'IGC Certigna s'engage donc à les rectifier dès lors qu'elle est informée qu'elles sont erronées.

Toute correction de données peut être demandée par simple envoi de courrier à l'autorité d'enregistrement concernée en précisant :
- Les données initiales transmises lors de l'enregistrement de la demande ;
- Les corrections à apporter ;
- Les éventuels justificatifs (photocopie de pièce d'identité).

La demande doit être datée et signée par le demandeur et envoyée à l'attention du Responsable CNIL de CERTIGNA, 20 allée de la râperie, 59650 Villeneuve d'Ascq.

9.4.2. Informations à caractère personnel

Les informations considérées comme personnelles sont les suivantes :
- Les causes de révocation des certificats des serveurs ;
- Le dossier d'enregistrement des serveurs, des opérateurs d'AED et des MC.

9.4.3. Informations à caractère non personnel

Sans objet.

9.4.4. Responsabilité en termes de protection des données personnelles

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

9.4.5. Notification et consentement d'utilisation des données personnelles

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

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

La divulgation des informations confidentielles n'est effectuée qu'aux autorités habilitées officiellement et exclusivement sur leur demande expresse en conformité avec la législation française [Loi n°90-1170 du 29 décembre 1990].

9.4.7. Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5. Droits sur la propriété intellectuelle et industrielle

La marque « Certigna » est protégée par le code de la propriété industrielle.

L'utilisation de cette marque par l'entité est autorisée uniquement dans le cadre du contrat d'abonnement.

9.6. 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 8.) et l'organisme de qualification ;
- Respecter les accords ou contrats qui les lient entre elles ou à l'entité ;
- 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.

9.6.1. Autorités de Certification

L'AC s'engage à :
- Pouvoir démontrer, aux utilisateurs de ses certificats, qu'elle a émis un certificat pour un serveur donné et que ce dernier a accepté le certificat, conformément aux exigences du chapitre 4.4 ;
- Garantir et maintenir la cohérence de sa DPC avec sa PC;
- Prendre toutes les mesures raisonnables pour s'assurer que les RC 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 RC et l'AC est formalisée par un lien contractuel / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences du RGS, par elle-même ou l'une de ses composantes. Elle a pris 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 RC 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.

9.6.2. Service d'enregistrement

Le service d'enregistrement s'engage à vérifier et à valider les dossiers de demande et de révocation de certificat.

9.6.3. Responsables de certificats

Le RC a le devoir de :
- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- Protéger la clé privée du service par des moyens appropriés à son environnement ;

- Protéger les données d'activation et, le cas échéant, les mettre en œuvre ;
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- Informer l'AC de toute modification concernant les informations contenues dans le certificat;
- Faire, sans délai, une demande de révocation du certificat auprès de l'AE, ou le cas échéant du MC de son entité, en cas de compromission ou de suspicion de compromission de la clé privée.

La relation entre le RC et l'AC ou ses composantes est formalisée par un engagement du RC visant à certifier l'exactitude des renseignements et des documents fournis. Ces informations s'appliquent également aux opérateurs d'AED et aux MC.

9.6.4. Utilisateurs de certificats

Les tiers utilisateurs doivent :
- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Pour chaque certificat de la chaîne de certification, du certificat du serveur jusqu'à l'AC racine Certigna Root CA, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (date de validité, statut de révocation) ;
- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

9.6.5. Autres participants

Sans objet.

9.7. Limite de garantie

La garantie est valable pour le monde entier hors USA et Canada.

9.8. Limite de responsabilité

Il est expressément entendu que Dhimyotis ne saurait être tenue pour responsable, ni d'un dommage résultant d'une faute ou négligence d'un accepteur et/ou des RC, ni d'un dommage causé par un fait extérieur, notamment en cas de :
- Utilisation d'un certificat pour une autre application que les applications définies au chapitre 1.5.1 de la présente PC;
- Utilisation d'un certificat pour garantir un autre objet que l'identité du serveur pour lequel le certificat a été émis ;
- Utilisation d'un certificat révoqué ;
- Utilisation d'un certificat au-delà de sa limite de validité ;
- Non-respect par les entités concernées des obligations définies aux chapitres 9.6.3 et 9.6.4 de la présente PC;
- Faits extérieurs à l'émission du certificat tels qu'une défaillance de l'application pour laquelle il peut être utilisé ;
- Force majeure comme définie par les tribunaux français.

9.9. Indemnités

Dhimyotis a notamment souscrit un contrat « Responsabilité civile après livraison ». L'étendue des garanties y est de cinq cent mille (500 000) euros par sinistre par an.

9.10. Durée et fin anticipée de validité de la PC

9.10.1. Durée de validité

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

9.10.2. Fin anticipée de validité

La publication d'une nouvelle version de la PC type RGS « Certificats électroniques de services applicatifs » peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC correspondante. Dans ce cas, cette mise en conformité n'imposera pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

Enfin, la validité de la PC peut arriver à terme prématurément en cas de cessation d'activité de l'AC (cf. chapitre 5.8).

9.10.3. Effets de la fin de validité et clauses restant applicables

La fin de validité de la PC met également fin à toutes les clauses qui la composent.

9.11. Notifications individuelles et communications entre les participants

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

- Faire valider, au plus tard un mois avant le début de l'opération, 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 ;
- En informer, au plus tard un mois après la fin de l'opération, l'organisme de qualification.

9.12. Amendements à la PC

9.12.1. Procédures d'amendements

L'AC procède à toute modification des spécifications stipulées dans la PC et la DPC et/ou des composantes de l'AC qui lui apparaît nécessaire pour l'amélioration de la qualité des services de certification et de la sécurité des processus, en restant toutefois conforme aux exigences du RGS et des documents complémentaires à ce dernier.

L'AC procède également à toute modification des spécifications stipulées dans la PC et la DPC et/ou des composantes de l'AC qui est rendue nécessaire par une législation, réglementation en vigueur ou par les résultats des Contrôles.

Toute modification majeure de la PC, et par conséquent de la DPC, donne lieu à une vérification de conformité par le Comité de Sécurité de l'AC de cette PC par rapport à la PC type. La DPC n'est applicable qu'après approbation par le Comité de Sécurité.

9.12.2. Mécanisme et période d'information sur les amendements

L'AC communique via son site Internet http://www.certigna.fr l'évolution de la PC au fur et à mesure de ses amendements.

9.12.3. 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 RC, 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.

Lorsque la modification de la PC est de nature typographique ou lorsque la modification de la PC n'impacte pas le niveau de qualité et de sécurité des fonctions de l'AC et de l'AE les OID de la PC et de la DPC correspondante ne sont pas modifiés.

9.13. Dispositions concernant la résolution de conflits

Il est rappelé que les conditions d'utilisation des certificats émis par l'AC sont définies par la présente PC et/ou par le contrat d'abonnement aux services de certification définissant les relations entre Dhimyotis d'une part et les RC d'autre part.

Les parties s'engagent à tenter de résoudre à l'amiable tout différend susceptible d'intervenir entre elles, soit directement, soit via un médiateur, dans les 2 mois de la réception du courrier avec accusé réception informant du différend. Les éventuels frais de médiation seront supportés par moitié par chacune des parties. Le cas échéant, l'affaire sera portée devant le tribunal de commerce de Lille.

9.14. Juridictions compétentes

Tout litige relatif à la validité, l'interprétation, l'exécution de la présente PC sera soumis aux tribunaux de Lille.

9.15. Conformité aux législations et réglementations

La présente PC est soumise au droit français, ainsi qu'à l'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.

9.16. Dispositions diverses

9.16.1. Accord global

Le présent document contient l'intégralité des clauses régissant l'IGC.

9.16.2. Transfert d'activités

Cf. chapitre 5.8.

9.16.3. Conséquences d'une clause non valide

En cas d'une clause non valide, les autres clauses ne sont pas remises en question.

9.16.4. Application et renonciation

Sans objet.

9.16.5. Force majeure

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

9.17. Autres dispositions

Sans objet.

10. Annexe 1 : exigence de sécurité du module cryptographique de l'AC

10.1. Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR et, des réponses OCSP), répond aux exigences de sécurité suivantes :

- Assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- Etre capable d'identifier et d'authentifier ses utilisateurs ;
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- Etre capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Si une fonction de sauvegarde et de restauration des clés 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 ;
- Le module cryptographique de l'AC doit détecter les tentatives d'altérations physiques et entrer dans un état sûr quand une tentative d'altération est détectée.

10.2. Exigences sur la qualification

Le module cryptographique utilisé par l'AC doit être qualifié au minimum au niveau élémentaire pour le niveau *, selon le processus décrit dans le RGS, et doit être conforme aux exigences du chapitre 10.1.

Le module cryptographique utilisé par l'AC est le module TrustWay Proteccio en cours de qualification au niveau renforcé, et faisant l’objet d’une dérogation par l’ANSSI pour les niveaux * et **.

Ils répondent aux exigences du chapitre 10.1.

11. Annexe 2 : exigences de sécurité du dispositif de protection des clés privées

11.1. Exigences sur les objectifs de sécurité

Le dispositif protection des clés privées, utilisé par le RC pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer son bi-clé, doit répondre aux exigences de sécurité suivantes :

- Si la bi-clé du serveur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- Détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée ;
- Garantir la confidentialité et l'intégrité de la clé privée ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Générer une fonction de sécurité qui ne peut être falsifié sans la connaissance de la clé privée ;
- Assurer la fonction de sécurité pour le RC 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.

11.2. Exigences sur la qualification

Le dispositif de protection des clés privées fourni par l'AC ou utilisé par le RC est qualifié au moins au niveau « Elémentaire » par l'ANSSI.