

Politique de Certification

Certigna SSL

(Authentication Serveur)

OID = 1.2.250.1.177.1.1.1.7

Référence RD102-03

Version 7.0

Dhimyotis 

Suivi des modifications

Date	Version	Auteur	Evolution du document
02/05/2007	1.0	JD	Création
06/06/2007	1.0	Comité de direction	Validation
05/07/2007	1.1	YL	Modifications
06/07/2007	1.1	Comité de direction	Validation
12/07/2007	1.1.1	YL	Correction
26/07/2007	1.2	JD	Modifications
27/07/2007	1.2	Comité de direction	Validation
27/09/2007	1.2.1	JD	Modifications
27/09/2007	1.2.1	Comité de direction	Validation
10/08/2007	1.3	JD	Modification
18/09/2008	2.0	PM	Changement profil et OID (passage en version 2)
18/09/2008	2.0	Comité de direction	Validation
01/12/2008	2.1	YL	Changement de nomenclature pour intégration dans le nouveau référentiel commun ETSI-PRIS, et signature électronique
01/12/2008	2.1	Comité de sécurité	Validation
26/02/2010	2.2	PM	Ajout des usages msSGC et nsSGC dans l'extension Extended Key Usage Remplacement des demandes de révocation par tél par des demandes en ligne Horodatage : 4 sources de temps Etendue des garanties définie par sinistre et par an Envoi de l'AR et de l'acceptation est intégré dans processus d'installation du certificat
03/03/2010	3.0	PM	Les DPC sont rendus publics Ajout du multi-FQDN Ajout possibilité envoi dossier de demande sous forme dématérialisée Ajout mandataires de certification Ajout autorités d'enregistrement déléguées
05/07/2010	3.1	PM	Passage 72 h à 24 h pour mise à jour des LCR
08/12/2010	4.0	VW	Changement profil (ICD ou GS1 dans le champ OU) et changement OID
10/02/2011	5.0	PM	Changement de version de CryptoBox (passage en S507) et changement OID
18/02/2011	5.1	PM	Précisions (validation d'identité, journaux d'événements, reprise possibilité de dématérialiser les dossiers transmis, etc.)
01/08/2011	6.0	PM	Changement modèle de certificat : Suppression n° série dans DN

Date	Version	Auteur	Evolution du document
01/12/2011	7.0	VW	Changement des adresses LDAP dans les CRL Distribution Points Ajout URL du CPS dans l'extension Certificate Policies La longueur du bicolé d'un certificat passe à 2048 bits

Table des matières

1	Introduction	10
1.1	Présentation générale	10
1.2	Identification du document	10
1.3	Entités intervenant dans l'IGC	11
1.3.1	Autorité de certification	11
1.3.2	Autorité d'enregistrement	11
1.3.3	Gestionnaires du certificat serveur	12
1.3.4	Utilisateur de certificat	12
1.3.5	Autres participants	12
1.4	Usage des certificats	13
1.4.1	Domaines d'utilisation applicables	13
1.5	Gestion de la PC	14
1.5.1	Entité gérant la PC	14
1.5.2	Point de contact	14
1.5.3	Entité déterminant la conformité de la DPC avec la PC	14
1.5.4	Procédures d'approbation de la conformité de la DPC	14
1.6	Définitions et acronymes	14
1.6.1	Acronymes	14
1.6.2	Définitions	15
2	Responsabilité concernant la mise à disposition des informations	17
2.1	Entités chargées de la mise à disposition des informations	17
2.2	Informations devant être publiées	17
2.2.1	Publication de la documentation	18
2.2.2	Publication de la LCR	18
2.2.3	Publication de la LAR	19
2.3	Délais et fréquences de publication	19
2.3.1	Publication de la documentation	19
2.3.2	Publication des certificats d'AC	19
2.3.3	Publication de la LCR	19

2.3.4	Publication de la LAR	19
2.4	Contrôle d'accès aux informations publiées	19
2.4.1	Contrôle d'accès à la documentation	19
2.4.2	Contrôle d'accès aux certificats d'AC	20
2.4.3	Contrôle d'accès à la LCR / LAR	20
3	Identification et Authentification	21
3.1	Nommage	21
3.1.1	Types de noms	21
3.1.2	Nécessité d'utilisation de noms explicites	21
3.1.3	Anonymisation ou pseudonymisation des porteurs	22
3.1.4	Unicité des noms	22
3.1.5	Identification, authentification et rôle des marques déposées	22
3.2	Validation initiale de l'identité	22
3.2.1	Méthode pour prouver la possession de la clé privée	22
3.2.2	Validation de l'identité d'un organisme	22
3.2.3	Validation de l'identité d'un individu	22
3.2.4	Validation de l'autorité du demandeur	26
3.2.5	Critères d'interopérabilité	27
3.3	Identification et validation d'une demande de renouvellement des clés	27
3.3.1	Identification et validation pour un renouvellement courant	27
3.3.2	Identification et validation pour un renouvellement après révocation	27
3.4	Identification et validation d'une demande de révocation	27
4	Exigences opérationnelles sur le cycle de vie des certificats	29
4.1	Demande de certificat	29
4.1.1	Origine d'une demande de certificat	29
4.1.2	Processus et responsabilités pour l'établissement d'une demande de certificat	29
4.2	Traitement d'une demande de certificat	30
4.2.1	Exécution des processus d'identification et de validation de la demande	30
4.2.2	Acceptation ou rejet de la demande	30
4.2.3	Durée d'établissement du certificat	31
4.3	Délivrance du certificat	31
4.3.1	Actions de l'AC concernant la délivrance du certificat	31
4.3.2	Notification par l'AC de la délivrance du certificat	32
4.4	Acceptation du certificat	32
4.4.1	Démarche d'acceptation du certificat	32
4.4.2	Publication du certificat	32
4.4.3	Notification par l'AC aux autres entités de la délivrance du certificat	32

4.5	Usages du bi-clé et du certificat	32
4.5.1	Utilisation de la clé privée et du certificat par le gestionnaire de certificat	32
4.5.2	Utilisation de la clé publique et du certificat par l'utilisateur du certificat	33
4.6	Renouvellement d'un certificat	33
4.7	Délivrance d'un nouveau certificat suite au changement du bi-clé	33
4.7.1	Causes possibles de changement d'un bi-clé	33
4.7.2	Origine d'une demande d'un nouveau certificat	33
4.8	Modification du certificat	34
4.9	Révocation et suspension des certificats	34
4.9.1	Causes possibles d'une révocation	34
4.9.2	Origine d'une demande de révocation	35
4.9.3	Procédure de traitement d'une demande de révocation	35
4.9.4	Délai accordé au gestionnaire de certificat pour formuler la demande de révocation	36
4.9.5	Délai de traitement par l'AC d'une demande de révocation	36
4.9.6	Exigences de vérification de la révocation par les utilisateurs de certificats	37
4.9.7	Fréquence d'établissement des LCR	37
4.9.8	Délai maximum de publication d'une LCR	37
4.9.9	Disponibilité d'un système de vérification en ligne de la révocation et...	37
4.9.10	Exigences spécifiques en cas de compromission de la clé privée	37
4.9.11	Suspension de certificat	38
4.10	Fonction d'information sur l'état des certificats	38
4.10.1	Caractéristiques opérationnelles	38
4.10.2	Disponibilité de la fonction	38
4.11	Fin de la relation entre le gestionnaire de certificat et l'AC	38
4.12	Séquestre de clé et recouvrement	38
5	Mesures de sécurité non techniques	39
5.1	Mesures de sécurité physique	39
5.1.1	Situation géographique et construction des sites	39
5.1.2	Accès physique	39
5.1.3	Alimentation électrique et climatisation	39
5.1.4	Vulnérabilité aux dégâts des eaux	40
5.1.5	Prévention et protection incendie	40
5.1.6	Conservation des supports	40
5.1.7	Mise hors service des supports	40
5.1.8	Sauvegardes hors site	40
5.2	Mesures de sécurité procédurales	40
5.2.1	Comité de Direction de l'AC Certigna	40

5.2.2	Comité de Sécurité de l'AC Certigna	41
5.2.3	Rôles de confiance	41
5.2.4	Nombre de personnes requises par tâche	42
5.2.5	Identification et authentification pour chaque rôle	42
5.2.6	Rôle exigeant une séparation des attributions	42
5.3	Mesures de sécurité vis-à-vis du personnel	42
5.3.1	Qualifications, compétences et habilitations requises	42
5.3.2	Procédures de vérification des antécédents	43
5.3.3	Exigences en matière de formation initiale	43
5.3.4	Exigences et fréquence en matière de formation continue	43
5.3.5	Fréquence et séquence de rotation entre différentes attributions	43
5.3.6	Sanctions en cas d'actions non autorisées	43
5.3.7	Exigences vis-à-vis du personnel des prestataires externes	43
5.3.8	Documentation fournie au personnel	44
5.4	Procédures de constitution des données d'audit	44
5.4.1	Type d'événements à enregistrer	44
5.4.2	Fréquence de traitement des journaux d'événements	45
5.4.3	Période de conservation des journaux d'événements	45
5.4.4	Protection des journaux d'événements	45
5.4.5	Procédure de sauvegarde des journaux d'événements	45
5.4.6	Système de collecte des journaux d'événements	45
5.4.7	Notification de l'enregistrement d'un événement au responsable de l'événement	45
5.4.8	Evaluation des vulnérabilités	45
5.5	Archivage des données	46
5.5.1	Types de données à archiver	46
5.5.2	Période de conservation des archives	46
5.5.3	Protection des archives	47
5.5.4	Procédure de sauvegarde des archives	47
5.5.5	Exigences d'horodatage des données	47
5.5.6	Système de collecte des archives	47
5.5.7	Procédures de récupération et de vérification des archives	47
5.6	Changement de clé d'AC	47
5.7	Reprise suite à compromission et sinistre	48
5.7.1	Procédures de remontée et traitement des incidents et des compromissions	48
5.7.2	Procédures de reprise en cas de corruption des ressources informatiques	48
5.7.3	Procédures de reprise en cas de compromission de la clé privée de composante	48
5.7.4	Capacité de continuité d'activité suite à un sinistre	49
5.7.5	Fin de vie de l'IGC	49

5.7.6	Transfert ou cessation d'activité, affectant une composante de l'IGC . . .	49
5.7.7	Cessation d'activité affectant l'AC	50
6	Mesures de sécurité techniques	51
6.1	Génération et installation de bi-clés	51
6.1.1	Génération des bi-clés	51
6.1.2	Transmission de la clé privée à son propriétaire	52
6.1.3	Transmission de la clé publique à l'AC	52
6.1.4	Transmission de la clé publique de l'AC aux utilisateurs de certificats . .	52
6.1.5	Tailles des clés	52
6.1.6	Vérification de la génération des paramètres des bi-clés et de leur qualité	53
6.1.7	Objectifs d'usage de la clé	53
6.2	Mesures de sécurité pour la protection des clés et des modules cryptographiques	54
6.2.1	Standards et mesures de sécurité pour les modules cryptographiques . . .	54
6.2.2	Contrôle de la clé privée par plusieurs personnes	54
6.2.3	Séquestre de la clé privée	54
6.2.4	Copie de secours de la clé privée	55
6.2.5	Archivage de la clé privée	55
6.2.6	Transfert de la clé privée avec le module cryptographique	56
6.2.7	Stockage de la clé privée dans un module cryptographique	56
6.2.8	Méthode d'activation de la clé privée	56
6.2.9	Méthode de désactivation de la clé privée	56
6.2.10	Méthode de destruction des clés privées	57
6.2.11	Niveau d'évaluation sécurité du module cryptographique	57
6.3	Autres aspects de la gestion des bi-clés	57
6.3.1	Archivage des clés publiques	57
6.3.2	Durées de vie des bi-clés et des certificats	57
6.4	Données d'activation	57
6.4.1	Génération et installation des données d'activation	57
6.4.2	Protection des données d'activation	58
6.4.3	Autres aspects liés aux données d'activation	58
6.5	Mesures de sécurité des systèmes informatiques	58
6.5.1	Exigences de sécurité technique spécifiques aux systèmes informatiques .	58
6.5.2	Niveau d'évaluation sécurité des systèmes informatiques	59
6.6	Mesures de sécurité des systèmes durant leur cycle de vie	59
6.6.1	Mesures de sécurité liées au développement des systèmes	59
6.6.2	Mesures liées à la gestion de la sécurité	60
6.6.3	Niveau d'évaluation sécurité du cycle de vie des systèmes	60

6.7	Mesures de sécurité réseau	60
6.7.1	Horodatage et Système de datation	60
7	Profil des certificats et des LCR	61
7.1	Profil des certificats émis par l'AC Certigna Racine	61
7.2	Profil des certificats émis par l'AC Certigna SSL	63
7.3	Profil des LCR	65
8	Audit de conformité et autres évaluations	66
8.1	Fréquences et/ou circonstances des évaluations	66
8.2	Identités/qualifications des évaluateurs	66
8.3	Relations entre évaluateurs et entités évaluées	66
8.4	Sujets couverts par les évaluations	67
8.5	Actions prises suite aux conclusions des évaluations	67
8.6	Communication des résultats	67
9	Autres problématiques métiers et légales	68
9.1	Tarifs	68
9.1.1	Tarifs pour la fourniture ou le renouvellement de certificats	68
9.1.2	Tarifs pour accéder aux certificats	68
9.1.3	Tarifs pour accéder aux informations d'état et de révocation des certificats	68
9.1.4	Tarifs pour d'autres services	68
9.1.5	Politique de remboursement	68
9.2	Responsabilité financière	69
9.2.1	Couverture par les assurances	69
9.2.2	Autres ressources	69
9.2.3	Couverture et garantie concernant les entités utilisatrices	69
9.3	Confidentialité des données professionnelles	69
9.3.1	Périmètre des informations confidentielles	69
9.3.2	Informations hors du périmètre des informations confidentielles	69
9.3.3	Responsabilités en termes de protection des informations confidentielles	69
9.4	Protection des données personnelles	70
9.4.1	Politique de protection des données personnelles	70
9.4.2	Informations à caractère personnel	70
9.4.3	Informations à caractère non personnel	70
9.4.4	Responsabilité en termes de protection des données personnelles	70
9.4.5	Notification et consentement d'utilisation des données personnelles	71
9.4.6	Conditions de divulgation d'informations personnelles aux autorités	71
9.4.7	Autres circonstances de divulgation d'informations personnelles	71

9.5	Droits sur la propriété intellectuelle et industrielle	71
9.6	Interprétations contractuelles et garanties	71
9.6.1	Autorités de certification	71
9.6.2	Obligations communes aux composantes de l'IGC	72
9.6.3	Service d'enregistrement	72
9.6.4	Gestionnaires de certificat	72
9.6.5	Utilisateurs de certificats	73
9.6.6	Autres participants	73
9.7	Limite de garantie	73
9.8	Limite de responsabilité	73
9.9	Indemnités	74
9.10	Durée et fin anticipée de validité de la PC	74
9.10.1	Durée de validité	74
9.10.2	Fin anticipée de validité	74
9.10.3	Effets de la fin de validité et clauses restant applicables	74
9.11	Notifications individuelles et communications entre les participants	74
9.12	Amendements à la PC	75
9.12.1	Procédures d'amendements	75
9.12.2	Mécanisme et période d'information sur les amendements	75
9.12.3	Circonstances selon lesquelles l'OID doit être changé	75
9.13	Dispositions concernant la résolution de conflits	75
9.14	Juridictions compétentes	76
9.15	Conformité aux législations et réglementations	76
9.16	Dispositions diverses	76
9.16.1	Accord global	76
9.16.2	Transfert d'activités	76
9.16.3	Conséquences d'une clause non valide	76
9.16.4	Application et renonciation	76
9.16.5	Force majeure	76
9.17	Autres dispositions	76
10	Annexe 1 : exigence de sécurité du module cryptographique de l'AC	77
10.1	Exigences sur les objectifs de sécurité	77
10.2	Exigences sur la qualification	77

Chapitre 1

Introduction

1.1 Présentation générale

Dhimyotis s'est doté d'une Autorité de Certification (AC) Certigna SSL pour délivrer des certificats à ses clients. Grâce à leurs certificats, les clients peuvent équiper leurs serveurs informatiques afin que ces derniers puissent établir des sessions sécurisées SSL/TLS avec des postes clients.

La présente Politique de Certification (PC) expose les engagements de l'AC Certigna SSL concernant les certificats SSL qu'elle émet. La PC identifie également les obligations et exigences portant sur les autres intervenants, notamment les gestionnaires de certificat et 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) et notamment les termes définis au chapitre 1.6. de la PC.

La présente PC vise la conformité au document « Policy requirements for certification authorities issuing public key certificates » émis par l'European Telecommunications Standards Institute (ETSI) et référencé ETSI TS 102 042.

1.2 Identification du document

La présente PC est dénommée « Politique de Certification de l'Autorité de Certification Certigna SSL ».

Elle peut être identifiée par son numéro d'OID. Le numéro d'OID du présent document est : 1.2.250.1.177.1.1.1.7

La politique de certification de l'autorité Certigna SSL correspond à la politique LCP « Lightweight Certificate Policy » spécifiée par la norme ETSI TS 102 042 et identifiée par l'OID 0.4.0.2042.1.3

1.3 Entités intervenant dans l'IGC

1.3.1 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 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) et (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 Certigna SSL 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 influencer 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.

1.3.2 Autorité d'enregistrement

L'AE assure les fonctions suivantes qui lui sont déléguées par l'AC, en vertu de la présente PC :

- Contrôle, validation des demandes de certificat (consiste schématiquement au contrôle d'habilitation du demandeur) et leur transmission à l'AC, pour les demandes initiales et les demandes de renouvellement ;
- Contrôle, validation des demandes de révocation de certificat (consiste schématiquement au contrôle d'habilitation du demandeur) et leur transmission à l'AC ;
- Archivage des demandes (certificat et révocation) et des journaux d'événements.
- 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'AE assure ces fonctions directement ou en les sous-traitant en partie à des autorités d'enregistrement déléguées (AED) (cf. 1.3.5. Autres participants). Dans tous les cas, l'AE en garde la responsabilité.

() : 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 sont complètes et effectuées par un mandataire de certification dûment autorisé.*

1.3.3 Gestionnaires du certificat serveur

Dans le cadre de la présente PC, un gestionnaire de certificat est la personne physique responsable :

- de l'utilisation du certificat du serveur informatique identifié dans le certificat,
 - de la clé privée correspondant à ce certificat,
- pour le compte de l'entité également identifiée dans ce certificat.

Le gestionnaire de certificat a un lien contractuel ou hiérarchique avec l'entité identifiée dans le certificat.

Le gestionnaire de certificat respecte les conditions qui lui incombent définies dans la PC et dans les Conditions Générales d'Utilisation.

En cas de changement de gestionnaire de certificat, l'entité doit le signaler à l'AC et lui désigner un successeur. L'AC révoque les certificats pour lesquels il n'y a plus de gestionnaire de certificat explicitement identifié.

1.3.4 Utilisateur de certificat

Un utilisateur de certificat serveur peut être : toute entité ou personne physique qui accède à un serveur informatique identifié par ce certificat.

Les utilisateurs de certificats doivent prendre toutes les précautions décrites dans la PC ainsi que dans les Conditions Générales d'Utilisation.

1.3.5 Autres participants

L'AC Certigna SSL s'appuie également sur des autorités d'enregistrement déléguées pour soustraire une partie des fonctions de l'AE. Les opérateurs d'AE déléguée ont le pouvoir de :

- autoriser, effectuer une demande de certificat ou de renouvellement de certificat ;
- effectuer une demande de révocation de certificat ;
- le cas échéant, enregistrer les mandataires de certification au sein des entités émettrices de demandes de certificat.

Il assure pour l'autorité Certigna SSL , dans le contexte de la délivrance de certificat, la vérification d'identité des futurs gestionnaire de certificat 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 de l'opérateur d'AE déléguée 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'AE déléguée doit effectuer de façon impartiale et scrupuleuse les contrôles

d'identité des futurs gestionnaire de certificat, et respecter les parties de la PC et de la DPC lui incombant.

L'AC Certigna SSL 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 de :

- autoriser, effectuer une demande de certificat ou de renouvellement de certificat portant le nom de l'entité ;
- 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'autorité Certigna SSL , dans le contexte de la délivrance de certificat, la vérification d'identité des futurs gestionnaires de certificat et des serveurs informatiques 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 mandataire de certification doit effectuer de façon impartiale et scrupuleuse les contrôles d'identité des futurs gestionnaires de certificat et des serveurs informatiques, et respecter les parties de la PC et de la DPC lui incombant.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

Il est expressément entendu qu'un gestionnaire de certificat ne peut utiliser son certificat qu'à des fins d'établissement de sessions sécurisées de type SSL/TLS. Le certificat lui permet notamment d'authentifier un ou plusieurs noms de sous-domaine hébergés par un serveur. Tout autre usage est effectué sous la seule responsabilité du gestionnaire de certificat.

De la même façon, il est expressément entendu qu'un utilisateur de certificat ne peut se fier à un certificat qu'à des fins d'établissement de sessions sécurisées de type SSL/TLS. Toute autre utilisation est effectuée sous la seule responsabilité de l'utilisateur de certificat.

Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.5. ci-dessous. L'AC s'engage à respecter ces restrictions et à imposer leur respect par les gestionnaires de certificat et les utilisateurs de certificats. A cette fin, elle publie à destination des gestionnaires de certificat, des MC et utilisateurs potentiels les Conditions Générales d'Utilisation.

Les Conditions Générales d'Utilisation peuvent être consultées sur le site <http://www.certigna.fr> avant toute demande de certificat ou toute utilisation d'un certificat Certigna SSL .

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

L'AC Certigna SSL est responsable de l'élaboration, du suivi, de la modification et de la validation de la présente PC. Elle statue sur toute modification nécessaire à apporter à la PC à échéance régulière. Le chapitre 9.12 de la présente PC précise les procédures applicables pour l'administration de la PC.

1.5.2 Point de contact

Dhimyotis
Certigna SSL
20 allée de la râperie
59650 VILLENEUVE D'ASCQ

1.5.3 Entité déterminant la conformité de la DPC avec la PC

L'AAP (Autorité d'Approbation des Politiques) s'assure de la conformité de la DPC par rapport à la PC. Elle peut le cas échéant se faire assister par des experts externes pour s'assurer de cette conformité. L'AAP est constituée par le comité de sécurité de Dhimyotis.

1.5.4 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. L'AAP doit s'assurer que les moyens mis en œuvre et décrits dans la DPC répondent à ces exigences en respectant le processus d'approbation mis en place par l'AC. Toute demande de mise à jour de la DPC suit également ce processus. Toute nouvelle version approuvée de la DPC est publiée, conformément aux exigences du paragraphe 9.12.3 sans délai.

Le traitement des modifications est décrit dans le chapitre 9.12.1. Procédures d'amendements.

Un contrôle de conformité de la DPC par rapport à la PC peut être également effectué par le cabinet d'audit externe lors de l'audit réalisé en vue de la qualification initiale et/ou d'un audit de surveillance.

1.6 Définitions et acronymes

1.6.1 Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

AAP Autorité d'Approbation des Politiques

AC Autorité de Certification

AE Autorité d'Enregistrement
AED Autorité d'Enregistrement Déléguée
CNIL Commission Nationale de l'Informatique et des Libertés
CSR Certificate Signature Request
DN Distinguished Name
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
INPI Institut National de la Propriété Industrielle
LAR Liste des Autorités Révoquées
LCP Lightweight Certificate Policy
LCR Liste des Certificats Révoqués
MC Mandataire de Certification
OCSP Online Certificate Status Protocol
OID Object Identifier
PC Politique de Certification
PCA Plan de Continuité d'Activité
PKCS Public Key Cryptographic Standards
SSL Secure Socket Layer
TLS Transport Layer Security
URL Uniform Resource Locator
UTC Universal Time Coordinated

1.6.2 Définitions

Autorité de Certification (AC) : cf. chapitre 1.3.1.

Autorité d'Enregistrement (AE) : cf. chapitre 1.3.2.

Autorité d'Enregistrement déléguée (AED) : cf. chapitre 1.3.5.

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

Certificat électronique : Fichier électronique attestant qu'un bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié dans le certificat. Il est délivré par une autorité de certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et le bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Déclaration des Pratiques de Certification (DPC) : Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

- Infrastructure de Gestion de Clés (IGC)** : Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'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 (LAR)** : 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 (LCR)** : Liste comprenant les numéros de série des certificats ayant fait l'objet d'une révocation, et signée par l'AC émettrice.
- Politique de certification (PC)** : Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les gestionnaires de certificat et les utilisateurs de certificats.
- RSA** : Algorithme à clés publiques du nom de ses inventeurs (Rivest, Shamir et Adleman).
- Utilisateur de certificat** : cf. chapitre 1.3.4.

Chapitre 2

Responsabilité concernant la mise à disposition des informations devant être publiées

2.1 Entités chargées de la mise à disposition des informations

L'IGC met à disposition des utilisateurs des certificats qu'elle émet des informations sur l'état de révocation des certificats en cours de validité émis par l'AC Certigna SSL . Ces informations sont publiées au travers de plusieurs serveurs :

- Serveur Web (2) :
<http://crl.certigna.fr/certignassl.crl>
<http://crl.dhimyotis.com/certignassl.crl>
- Serveur LDAP (2) :
<ldap://ldap.certigna.fr/cn=Certigna%20SSL,OU=IGC,DC=certigna,DC=fr?certificateRevocationList;binary>
<ldap://ldap.dhimyotis.com/cn=Certigna%20SSL,OU=IGC,DC=certigna,DC=fr?certificateRevocationList;binary>
- Serveur OCSP (2) :
<http://ssl.ocsp.certigna.fr>
<http://ssl.ocsp.dhimyotis.com>

2.2 Informations devant être publiées

L'AC publie à destination des gestionnaires de certificat et utilisateurs de certificats :

- La PC ;
- Les Conditions Générales d'Utilisation des services de certification Certigna SSL ;
- Les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, ...) ;
- Le certificat d'AC Certigna Racine et le certificat d'AC intermédiaire Certigna SSL 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 gestionnaires de certificat ou les utilisateurs de certificat non spécialistes du domaine, l'AC publie en dehors des PC et DPC des Conditions Générales d'Utilisation que le futur gestionnaire de certificat est dans l'obligation de lire et de signer lors de toute demande de certificat (demande initiale et suivantes, en cas de renouvellement) auprès d'une 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 Certigna SSL 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 gestionnaires de certificat et utilisateurs de certificats, et sur leur demande, sa déclaration des pratiques de certification 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 gestionnaires de certificat 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>

NB : suivant le système d'exploitation et/ou le navigateur utilisé par l'utilisateur le certificat de l'AC Certigna Racine peut être automatiquement installé dans les magasins de certificats des autorités de confiance grâce aux mécanismes de mise à jour (pour les éditeurs ayant reconnu l'autorité Certigna comme autorité de confiance).

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 Certigna SSL .

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 Certigna Racine.

2.3 Délais et fréquences de publication

2.3.1 Publication de la documentation

La PC, les conditions générales d'utilisation des services de certification Certigna SSL 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 correspondants.

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 maximum 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

2.4.1 Contrôle d'accès à la documentation

La PC, les conditions générales d'utilisation des services de certification Certigna SSL et les différents formulaires nécessaires pour la gestion des certificats sont libres d'accès en lecture. La DPC est accessible en lecture sur demande expresse auprès de Dhimyotis.

2.4.2 Contrôle d'accès aux certificats d'AC

Le certificat d'AC Certigna Racine et le certificat d'AC intermédiaire Certigna SSL sont libres d'accès en lecture.

2.4.3 Contrôle d'accès à la LCR / LAR

La liste des certificats révoqués est libre d'accès en lecture. 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.

Chapitre 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 serveur (champ « subject ») sont identifiés par un « Distinguished Name » DN de type X.501, en conformité avec le RFC5280.

3.1.2 Nécessité d'utilisation de noms explicites

Le DN du certificat permet d'identifier le serveur informatique.

Il est construit à partir du FQDN principal comportant le nom de domaine auquel il est rattaché.

Le DN a la forme suivante :

```
{  
  C = Pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée,  
  CN = FQDN (Fully Qualified Domain Name) principal du serveur informatique,  
  O = Nom de l'entité à laquelle appartient le serveur informatique,  
  OU = ICD(*) + identifiant de l'entité à laquelle appartient le serveur informatique  
  enregistré conformément à la législation et aux réglementations en vigueur.  
}
```

(*) En cas d'absence d'ICD pour un pays donné, l'AC Certigna SSL utilise un substitut d'ICD construit comme suit : **G** + **Code GS1**. La liste des codes GS1 est disponible à l'adresse suivante :

http://www.gs1.org/barcodes/support/prefix_list

L'extension Subject Alternative Name (Nom Alternatif de l'Objet), contient :

- le FQDN principal du serveur ;
- ainsi que les FQDN secondaires optionnels.

Pour rappel, en cas de multiplicité, les FQDN sont rattachés au même domaine.

3.1.3 Anonymisation ou pseudonymisation des porteurs

S'agissant de certificats de serveurs informatiques, les notions d'anonymisation ou de pseudonymisation sont sans objet.

3.1.4 Unicité des noms

La combinaison du pays, du nom et de l'identifiant de l'entité à laquelle appartient le serveur, ainsi que de son FQDN principal identifie de manière univoque le titulaire du certificat.

3.1.5 Identification, authentification et rôle des marques déposées

L'AC et les AE dégagent toute responsabilité concernant les noms utilisés et communiqués par le demandeur de certificat pour identifier les serveurs, notamment en cas d'utilisation abusive d'un nom pour les certificats émis dans le cadre de la PC.

3.2 Validation initiale de l'identité

L'enregistrement d'un gestionnaire de certificat 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 futur gestionnaire de certificat avant de certifier la clé publique. Pour ceci, le futur gestionnaire de certificat génère son 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

L'enregistrement d'un serveur auquel un certificat doit être délivré se fait via l'enregistrement du gestionnaire de certificat correspondant. Ce dernier devra notamment démontrer que le nom de domaine inclus dans le (ou les) FQDN du serveur appartient bien à l'entité qu'il représente. Un gestionnaire de certificat peut être amené à changer en cours de validité du certificat serveur correspondant. Dans ce cas, tout nouveau gestionnaire de certificat doit également faire l'objet d'une procédure d'enregistrement.

Le gestionnaire de certificat est soit le responsable légal de l'entité, soit une personne physique désignée par lui. Dans ce second cas, le responsable légal devra faire un mandat écrit pour déléguer cette personne.

L'enregistrement d'un gestionnaire de certificat, et du serveur informatique correspondant, peut

se faire directement auprès d'une AE, ou via un mandataire de certification de l'entité. Dans ce dernier cas, le MC doit être préalablement enregistré par l'AE.

Enregistrement d'un gestionnaire de certificat sans MC pour un certificat à émettre

L'enregistrement du futur gestionnaire de certificat nécessite la validation de l'identité "personne morale" de l'entité de rattachement du futur gestionnaire de certificat, de l'identité "personne physique" du futur gestionnaire de certificat, de son habilitation à être gestionnaire de certificat pour le serveur informatique considéré et pour l'entité considérée, ainsi que du nom de domaine du serveur.

Le dossier de demande de certificat traité par l'AE doit comprendre :

- La demande de certificat Certigna SSL (formulaire disponible sur le site de Certigna <http://www.certigna.fr>), datée de moins de trois mois, remplie et signée par le gestionnaire de certificat comportant notamment :
 - Une acceptation des termes et conditions (conditions générales d'utilisation signées) ;
 - Le(s) FQDN à utiliser dans le certificat (FQDN principal et le cas échéant les FQDN secondaires) ;
 - Les coordonnées du futur gestionnaire de certificat (nom, entreprise, adresse, téléphone, e-mail).
- La photocopie d'une pièce d'identité officielle (comportant une photo d'identité) en cours de validité au moment de l'enregistrement du futur gestionnaire de certificat, certifiée conforme par ce dernier (date, de moins de 3 mois, et signature précédées de la mention "copie certifiée conforme à l'original").
- Un mandat signé, et daté de moins de trois mois, par un représentant légal de l'entité désignant le cas échéant le futur gestionnaire de certificat comme étant habilité à être gestionnaire de certificat pour le serveur informatique auquel le certificat doit être délivré. Ce mandat doit être signé pour acceptation par le futur gestionnaire de certificat ;
- Des informations d'identification de l'entité :
 - Si l'entité est une entreprise (autre qu'une association)*
 - 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 ou SIRET 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.
 - Si l'entité est une association*
 - une photocopie du procès verbal de l'assemblée générale signé par ses représentants.
 - Si l'entité est une administration*
 - une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative.
- La preuve de possession par l'entité du nom de domaine correspondant au(x) FQDN ;
- La photocopie d'une pièce d'identité officielle (comportant une photo d'identité) en cours de validité au moment de l'enregistrement du représentant légal (signataire des pièces du dossier), certifiée conforme par ce dernier (date, de moins de 3 mois, et signature précédées de la mention "copie certifiée conforme à l'original").

L'authentification du gestionnaire de certificat par l'AE (opérateur d'AE ou opérateur d'AED) s'effectue par l'envoi du dossier par courrier postal ou de façon dématérialisée (dossier scanné puis transmis par courrier électronique).

Le gestionnaire de certificat 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 nouveau gestionnaire de certificat sans MC pour un certificat déjà émis

En cas de changement de gestionnaire de certificat pour un certificat serveur en cours de validité, le nouveau gestionnaire de certificat doit faire l'objet d'une procédure d'enregistrement.

Le dossier d'enregistrement déposé directement auprès d'une AE ou d'une AED doit au moins comprendre :

- Un mandat daté de moins de trois mois, désignant le futur gestionnaire de certificat comme étant habilité à être le nouveau gestionnaire de certificat pour le serveur informatique auquel le certificat a été délivré, en remplacement de l'ancien gestionnaire de certificat. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur gestionnaire de certificat ;
- Des informations d'identification de l'entité :
 - Pour une entreprise :*
 - Tout document attestant de la qualité du signataire du mandat ;
 - Pour une autorité administrative :*
 - Une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative.
 - Pour une association :*
 - une photocopie du procès verbal de l'assemblée générale signé par ses représentants.
- La photocopie d'une pièce d'identité officielle (comportant une photo d'identité) en cours de validité au moment de l'enregistrement du futur gestionnaire de certificat, certifiée conforme par ce dernier (date, de moins de 3 mois, et signature précédées de la mention "copie certifiée conforme à l'original") ;
- La photocopie d'une pièce d'identité officielle (comportant une photo d'identité) en cours de validité au moment de l'enregistrement du représentant légal (signataire des pièces du dossier), certifiée conforme par l'AE ou éventuellement par un officier public (notaire ou huissier de justice) : date, de moins de 3 mois, et signature précédées de la mention "copie certifiée conforme à l'original" ;
- L'acceptation des termes et conditions (conditions générales d'utilisation signées).

L'authentification du futur gestionnaire de certificat par l'AE (opérateur d'AE ou opérateur d'AED) s'effectue par l'envoi du dossier par courrier postal ou de façon dématérialisée (dossier scanné puis transmis par courrier électronique).

Enregistrement du mandataire de certification (MC)

Le mandataire de certification 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 de façon impartiale et scrupuleuse les contrôles d'identité des futurs gestionnaire de certificat tels que définis dans la PC ;
 - Informer l'AE en cas de départ de l'entité.
- La photocopie d'une pièce d'identité officielle (comportant une photo d'identité) en cours de validité au moment de l'enregistrement du futur mandataire, certifiée conforme par ce dernier (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 (autre qu'une association)*
 - 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 association*
 - une photocopie du procès verbal de l'assemblée générale signé par ses représentants.
 - 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 mandataire est réalisée lors d'un face à face physique. Lors de ce face-à-face, une demande de certificat Certigna ID PRIS *** Pro est effectuée. Ce certificat permettra de transmettre sous forme dématérialisée les dossiers de demande de certificat ou les demandes de révocation.

Enregistrement d'un gestionnaire de certificat via un MC

L'enregistrement d'un gestionnaire de certificat via un MC nécessite la validation par le MC de l'identité "personne physique" du futur gestionnaire de certificat 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 ou le futur gestionnaire et comportant un ou plusieurs FQDN ;
- Un mandat daté de moins de trois mois, désignant le futur gestionnaire comme étant habilité à être gestionnaire pour le serveur informatique auquel le certificat doit être délivré. Ce mandat doit être signé par le MC et co-signé, pour acceptation, par le futur gestionnaire.
- La preuve de possession par l'entité du nom de domaine correspondant au(x) FQDN ;
- La photocopie d'une pièce d'identité officielle (comportant une photo d'identité) en cours de validité au moment de l'enregistrement du futur gestionnaire de certificat, certifiée conforme par le gestionnaire de certificat (date, de moins de 3 mois, et signature précédées de la mention "copie certifiée conforme à l'original") ;
- L'acceptation des termes et conditions (conditions générales d'utilisation signées).

L'authentification du futur gestionnaire de certificat par le mandataire de certification s'effectue par l'envoi du dossier par courrier postal ou de façon dématérialisée (dossier scanné puis transmis par courrier électronique).

Le dossier est envoyée par courrier à l'AE pour conservation, et éventuellement sous forme électronique signé avec le certificat Certigna ID PRIS *** Pro du MC.

Le gestionnaire de certificat 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 nouveau gestionnaire via un MC pour un certificat déjà émis

En cas de changement de gestionnaire pour un certificat serveur en cours de validité, le nouveau gestionnaire doit faire l'objet d'une procédure d'enregistrement en remplacement de l'ancien gestionnaire.

Le dossier d'enregistrement, déposé auprès d'un MC, doit au moins comprendre :

- La photocopie d'une pièce d'identité officielle (comportant une photo d'identité) en cours de validité au moment de l'enregistrement du futur gestionnaire, certifiée conforme par ce dernier ou par le MC (date, de moins de 3 mois, et signature précédées de la mention "copie certifiée conforme à l'original").
- Un mandat daté de moins de trois mois, désignant le futur gestionnaire comme étant habilité à être le nouveau gestionnaire pour le serveur informatique auquel le certificat doit être délivré, en remplacement de l'ancien gestionnaire. Ce mandat doit être signé par le MC et co-signé, pour acceptation, par le futur gestionnaire.

L'authentification du futur gestionnaire de certificat par le mandataire de certification s'effectue par l'envoi du dossier par courrier postal ou de façon dématérialisée (dossier scanné puis transmis par courrier électronique).

Le dossier est envoyée par courrier à l'AE pour conservation, et éventuellement sous forme électronique signée avec le certificat Certigna ID PRIS *** Pro du MC.

3.2.4 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).

3.2.5 Critères d'interopérabilité

En cas de demande de certification croisée avec l'AC Certigna, que cette demande émane de cette dernière ou de l'autorité tierce, l'AAP de l'AC Certigna SSL s'engage à effectuer une étude préalable d'impact.

Cette étude comprend :

- L'analyse de la Politique de Certification de l'AC tierce et l'assurance d'un niveau d'exigence équivalent à la sienne ;
- L'analyse des contraintes d'exploitation de l'AC tierce et l'assurance d'un niveau de continuité équivalent au sien ;
- Un audit du site d'exploitation de l'AC tierce.

Tout accord contractuel de reconnaissance mutuelle précisera les limites de responsabilités respectives de chaque autorité.

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

L'AC n'émet pas de nouveau certificat pour un bi-clé précédemment émis. Le renouvellement passe par la génération d'un nouveau bi-clé et d'une nouvelle demande de certificat (cf. chapitre 4.6.).

3.3.1 Identification et validation pour un renouvellement courant

La vérification de l'identité du gestionnaire de certificat, du responsable légal et de l'entité est identique à celle effectuée lors de la demande initiale.

3.3.2 Identification et validation pour un renouvellement après révocation

La vérification de l'identité du gestionnaire de certificat est identique à celle effectuée lors de la demande initiale. L'entité doit effectuer une nouvelle demande au travers du processus initial d'enregistrement tel que décrit en 3.2. Un nouveau bi-clé sera par conséquent généré préalablement à l'émission de la nouvelle demande.

3.4 Identification et validation d'une demande de révocation

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

- Courrier : demande remplie et signée à partir du formulaire de révocation d'un certificat disponible sur le site de Certigna <http://www.certigna.fr> ;

- En ligne (remplissage du formulaire en ligne disponible sur le site de Certigna : <http://www.certigna.fr>).

L'adresse postale du service de révocation est disponible sur le site de Certigna <http://www.certigna.fr>

La demande papier doit comporter les éléments suivants :

- Le prénom et le nom du gestionnaire de certificat ;
- L'adresse e-mail du gestionnaire de certificat ;
- Le FQDN principal du serveur ;
- La raison de la révocation ;
- *Si le gestionnaire de certificat n'est pas le demandeur :*
- Le prénom et le nom du demandeur ;
- La qualité du demandeur (représentant légal, opérateur d'AED, MC) ;
- Le numéro de téléphone du demandeur.

Si la demande est transmise sous format électronique, elle doit faire apparaître les éléments suivants :

- Le prénom et le nom du gestionnaire de certificat ;
- L'adresse e-mail du gestionnaire de certificat ;
- La raison de la révocation ;
- Le code de révocation (attribué lors de la délivrance du certificat).

La demande électronique peut être effectuée par une personne habilitée munie d'un certificat Certigna ID PRIS *** Pro (opérateur d'AED ou le cas échéant un MC). La demande sera alors signée électroniquement avec ce certificat Certigna ID PRIS Pro ***. Dans ce cas, l'information 'code de révocation' peut être absente du formulaire.

Chapitre 4

Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Le demandeur de certificat peut ne pas appartenir officiellement à l'entité mais être délégué par celle-ci. Il faut dans tous les cas le consentement d'un représentant légal de l'entité, ou celui d'un MC dûment mandaté pour cette entité, qui mandate le demandeur (le futur gestionnaire de certificat).

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 gestionnaire à partir des éléments fournis par son entité, soit par son entité et signé par le futur gestionnaire. 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 gestionnaire, ce dernier doit fournir une adresse e-mail qui permet à l'AE de prendre contact pour toute question relative à son enregistrement. Le MC doit également fournir une adresse e-mail lors de son enregistrement, pour que l'AE puisse prendre contact avec ce dernier pour toute question relative à l'enregistrement des gestionnaires de certificat.

Avant de rentrer en relation contractuelle, l'AC Certigna SSL informe le gestionnaire de certificat des termes et conditions au regard de l'utilisation du certificat. Ces conditions sont décrites dans les Conditions Générales d'Utilisation (CGU) annexées au formulaire de demande et également décrites dans la présente PC.

En cas d'envoi par courrier électronique du dossier de demande, le formulaire de demande ainsi que les Conditions Générales d'Utilisation doivent être imprimés pour être complétés par le demandeur (signature, paraphe, etc.), puis scannés pour être joints au dossier transmis.

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 du(des) FQDN ;
- Validation de l'identité des signataires de la demande (gestionnaire, représentant légal) ;
- Validation de l'identité de l'entité ;
- Validation du dossier (complétude du dossier et cohérence des justificatifs présentés) ;
- Assurance que le futur gestionnaire a pris connaissance des modalités applicables pour l'utilisation du certificat.

L'identité du futur gestionnaire 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 une AED, cette dernière retransmet la demande à l'AE après avoir effectué les opérations ci-dessus.

L'AE s'assure que le type de certificat demandé correspond au mandat des opérateurs 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 gestionnaire de certificat, validation du dossier, assurance de la prise de connaissance des conditions générales).

L'AE s'assure alors que le type de certificat demandé 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).

Le traitement d'une demande pourra être déclenché dès la réception du dossier papier ou de sa version dématérialisée transmis :

- soit par le futur gestionnaire de certificat ;
- soit par le représentant légal ;
- ou le cas échéant par le MC.

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 gestionnaire de certificat, 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 électronique (CSR) n'est pas cohérente avec le dossier de demande (des informations telles que l'identité, l'adresse e-mail du futur gestionnaire de certificat, le(les) FQDN, ou le nom de l'entité sont différentes).
- La demande ne correspond pas au mandat du MC.

En cas d'acceptation par l'AE, après génération du certificat par l'AC, l'AE envoie un mail au gestionnaire de certificat contenant un lien permettant d'accéder à la page d'importation du certificat.

En cas de transmission par un opérateur d'AED ou le cas échéant un MC, l'opérateur d'AE vérifie la signature électronique du dossier de demande transmis sous forme dématérialisée ainsi que l'habilitation du demandeur :

- Si le demandeur n'est pas le gestionnaire de certificat, le demandeur doit être enregistré comme opérateur d'AED ou MC dans la base de l'AE ;
- L'AC Certigna SSL est inscrite dans le périmètre d'intervention du demandeur : la base de l'AE indique les AC pour lesquelles les opérateurs d'AED ou les MC peuvent exercer leur rôle.
- Dans le cas d'un MC, l'opérateur d'AE vérifie l'appartenance du MC et du futur gestionnaire de certificat à la même entité.

4.2.3 Durée d'établissement du certificat

A compter de la réception du dossier d'enregistrement complet (format papier ou électronique) et de la demande électronique (CSR), le certificat est établi dans un délai de cinq jours ouvrés. L'AE conserve ensuite les éléments constitutifs du dossier. L'établissement du certificat est soumis, pour rappel, à la condition qu'une CSR ait été émise en parallèle par le gestionnaire de certificat (demande en ligne).

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 gestionnaire de certificat. Le bi-clé est généré par un module cryptographique logiciel du gestionnaire de certificat. La partie publique du bi-clé est transmise dans la CSR à l'AE.

Avant de procéder à la génération du certificat, l'AC Certigna SSL vérifie que les données devant figurer obligatoirement (champs et extensions) dans ce dernier sont renseignées avec des valeurs cohérentes.

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 gestionnaire (transmission par mail). Le gestionnaire de certificat installe le certificat grâce à l'outil Certigna-Factory (applet téléchargée depuis le site <http://www.certigna.fr>). C'est Certigna-Factory qui notifie l'AE de la bonne délivrance du certificat, par envoi d'un accusé de réception signé par le gestionnaire de certificat. Cet accusé spécifie également l'acceptation ou le rejet du certificat (cf. 4.4.1. Acceptation du certificat).

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

C'est à l'installation du certificat avec Certigna-Factory et par l'intermédiaire de cet outil que le gestionnaire de certificat choisit d'accepter ou non le certificat. La notification d'acceptation ou de refus est transmise avec l'accusé de réception à l'AE signé électroniquement (avec la clé privée associée au certificat).

En cas d'échec de l'envoi, un formulaire (disponible sur <http://www.certigna.fr>) peut être téléchargé, imprimé, complété et envoyé par courrier. Toutefois, l'acceptation est tacite dans un délai de 7 jours à compter de l'envoi du certificat par l'AE. En cas de détection d'incohérence entre les informations figurant dans l'accord contractuel et le contenu du certificat, le gestionnaire de certificat doit refuser le certificat, ce qui aura pour conséquence sa révocation par l'AE.

4.4.2 Publication du certificat

Aucune publication n'est effectuée après l'acceptation du certificat par le gestionnaire de certificat.

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 gestionnaire de certificat.

4.5 Usages du bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le gestionnaire de certificat

L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service d'établissement d'une session sécurisée SSL/TLS : authentification du serveur, échange de la clé de session (cf chapitre 1.4.1.). Les gestionnaires de certificat doivent respecter strictement les usages autorisés des bi-clés et des certificats au niveau des serveurs. Dans le cas contraire,

leur responsabilité pourrait être engagée.

L'usage autorisé du bi-clé et du certificat associé est indiqué dans le certificat lui-même, via l'extension Key Usage qui inclut les valeurs digitalSignature et keyEncipherment.

Faisant partie du dossier d'enregistrement, les Conditions Générales d'Utilisation sont portées à la connaissance du gestionnaire de certificat ou du MC par l'AC avant d'entrer en relation contractuelle. Elles sont consultables préalablement à toute demande de certificat en ligne. Elles sont accessibles sur le site <http://www.certigna.fr>. Les conditions acceptées et signées par le gestionnaire de certificat lors de la demande de certificat restent applicables pendant toute la durée de vie du certificat, ou le cas échéant jusqu'à l'acceptation et la signature par le gestionnaire de certificat de nouvelles conditions générales émises et portées à sa connaissance par l'AC via le site <http://www.certigna.fr>. Les nouvelles conditions signées doivent être transmises par le gestionnaire de certificat à l'AC pour être applicables.

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 un bi-clé précédemment émis. Le renouvellement passe par la génération d'un nouveau bi-clé et une nouvelle demande de certificat (cf. chapitre 4.1). Le gestionnaire de certificat s'engage, en acceptant les Conditions Générales d'Utilisation, à utiliser exclusivement l'outil Certigna-Factory version SSL pour générer sa demande de certificat (demande initiale ou renouvellement), et par conséquent à générer un nouveau bi-clé à chaque demande.

4.7 Délivrance d'un nouveau certificat suite au changement du bi-clé

4.7.1 Causes possibles de changement d'un bi-clé

Les bi-clés doivent être périodiquement renouvelés afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des serveurs, et les certificats correspondants, sont renouvelés au minimum tous les trois ans (cf. période de validité du certificat d'un à trois ans).

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 gestionnaire de certificat (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 désignation d'un gestionnaire de certificat (avec acceptation de ce dernier) pour ce certificat reste obligatoire.

La génération de la CSR reste toujours sous la responsabilité du gestionnaire de certificat. L'importation du nouveau certificat est également effectué sous la responsabilité du gestionnaire de certificat.

4.8 Modification du certificat

La modification de certificats Certigna SSL n'est pas autorisée. En cas de nécessité de changement d'informations présentes dans le certificat (principalement les informations du champ 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 de serveurs

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

- 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, modification d'un FQDN), ceci avant l'expiration normale du certificat ;
- Le gestionnaire de certificat n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le gestionnaire de certificat, l'entité, le cas échéant l'opérateur d'AED ou le MC, 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 gestionnaire de certificat, le représentant légal de l'entité à laquelle il appartient, le cas échéant l'opérateur d'AED ou le MC, 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, la cessation d'activité ou l'interdiction de l'exercer de l'entité de rattachement du serveur ;
- 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 de serveurs

Les personnes ou entités qui peuvent demander la révocation d'un certificat Certigna SSL sont les suivantes :

- Le gestionnaire de certificat ;
- L'AC ;
- L'AE ou les AED ;
- Un représentant légal de l'entité à laquelle est rattaché le serveur ;
- Le cas échéant le MC.

Le gestionnaire de certificat est informé, en particulier par le biais des Conditions Générales d'Utilisation qu'il a acceptées, des personnes susceptibles d'effectuer une demande de révocation pour le certificat dont il a la responsabilité.

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 serveur

La demande de révocation est effectuée auprès de l'AE.

Les informations suivantes doivent figurer dans la demande de révocation de certificat (formulaire transmis par courrier ou en ligne) :

- Le nom de l'autorité qui a émis le certificat (Certigna SSL) ;
 - L'identité du gestionnaire de certificat ;
 - L'adresse mail du gestionnaire de certificat ;
 - Le FQDN principal du serveur ;
 - Le numéro de série du certificat ;
 - La raison de la révocation ;
- Et, pour les demandes envoyées par courrier si le gestionnaire de certificat n'est pas le demandeur :*
- Le prénom et le nom du demandeur ;
 - La qualité du demandeur (un responsable légal, le cas échéant un opérateur d'AED ou le MC) ;

- Le numéro de téléphone du demandeur.

Si la demande est transmise par courrier, cette dernière doit être signée par le demandeur (la signature est vérifiée par l'AE avec celle du dossier de demande de certificat).

Si la demande est effectuée en ligne, l'habilitation de la personne à effectuer cette demande est vérifiée (fourniture du code de révocation et/ou signature électronique du formulaire). En l'occurrence la personne à l'origine de la demande peut être :

- Le gestionnaire de certificat lui-même ;
- Le cas échéant un MC ;
- Un opérateur d'AED.

Les étapes sont les suivantes :

- Le demandeur de la révocation transmet sa demande à l'AE, par courrier ou en ligne (sur <http://www.certigna.fr>) ;
- 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 ;
- Dans tous les cas, le gestionnaire de certificat est informé de la révocation par e-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 Certigna Racine décide de révoquer le certificat d'AC intermédiaire Certigna SSL (suite à la compromission de la clé privée de l'AC Certigna SSL ou de l'AC Certigna Racine), cette dernière informe par e-mail l'ensemble des gestionnaires de certificat 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 (auxquelles sont rattachés les serveurs) et le cas échéant de leur MC.

4.9.4 Délai accordé au gestionnaire de certificat pour formuler la demande de révocation

Dès que le gestionnaire de certificat 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 serveur

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 dont le demandeur a pu être authentifié et son habilitation vérifiée, est de 72 heures après réception par l'AE.

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 Certigna SSL 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 durée de validité de la LCR est de 24 heures. La fréquence d'établissement de la LCR est de 2 par jour (émission toutes les 12 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 60 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 SSL dispose d'un répondeur OCSP disponible aux adresses suivantes : <http://ssl.ocsp.certigna.fr> et <http://ssl.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.

4.9.10 Exigences spécifiques en cas de compromission de la clé privée

Les gestionnaires de certificat 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 gestionnaire de certificat s'oblige à interrompre immédiatement et définitivement l'usage du certificat serveur et de la clé privée qui lui est associée. Pour rappel, cet engagement est pris lors de la signature des conditions générales d'utilisation.

4.9.11 Suspension de certificat

Les certificats émis par l'AC Certigna SSL 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 (jusqu'à et y compris l'AC Certigna Racine), c'est à dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR/LAR et l'état du certificat de l'AC Certigna Racine.

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 dans un annuaire (accessible en protocole LDAP V3) et sur le site Web de publication (accessible avec le protocole HTTP).

4.10.2 Disponibilité de la fonction

Dhimyotis garantit la disponibilité de la fonction d'information sur l'état des certificats les jours ouvrés. Dans la pratique, cette fonction est accessible 24h/24, 7j/7.

4.11 Fin de la relation entre le gestionnaire de certificat et l'AC

En cas de fin de relation contractuelle ou réglementaire entre l'AC Certigna SSL et l'entité de rattachement du serveur avant la fin de validité du certificat, pour une raison ou pour une autre, le certificat est révoqué. De plus, l'AC Certigna SSL révoque tout certificat pour lequel il n'y a plus de gestionnaire de certificat explicitement identifié.

4.12 Séquestre de clé et recouvrement

Le séquestre des clés privées des serveurs est interdit par la présente PC. Les clés d'AC ne sont en aucun cas séquestrées.

Chapitre 5

Mesures de sécurité non techniques

RAPPEL (cf. chapitre 1.3.1) - 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 composants 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 Comité de Direction de l'AC Certigna

L'AC Certigna dispose d'un comité de direction qui approuve la politique de certification, et en assume la responsabilité.

5.2.2 Comité de Sécurité de l'AC Certigna

L'AC Certigna dispose d'un comité de sécurité qui vérifie que les pratiques de sécurité décrites dans la DPC sont appliquées correctement.

5.2.3 Rôles de confiance

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

1. **Officier de sécurité** – L'officier 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.
2. **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.
3. **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.
4. **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.
5. **Contrôleur** - Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.

Un sixième rôle, lié au partage du secret de l'AC, est également défini :

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 propre 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.

5.2.4 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 ».

5.2.5 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 Certigna SSL 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.).

5.2.6 Rôle exigeant une séparation des attributions

Concernant les rôles de confiance, les cumuls suivants sont interdits au sein de l'IGC :

- officier de sécurité et administrateur système ;
- contrôleur et tout autre rôle ;
- administrateur système et opérateur.

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 l'officier 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, formation 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 Certigna SSL 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 (Autorité d'Enregistrement, Autorité de Certification).

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 ;
- Événements 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 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 porteurs).

Des événements spécifiques aux différentes fonctions de l'IGC sont également journalisés :

- Événements liés aux clés de signature et aux certificats d'AC (génération, sauvegarde et récupération, révocation, destruction,...) ;
- 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 gestionnaires de certificat et, selon les cas, acceptations / rejets explicites par les gestionnaires de certificat ;
- Publication et mise à jour des informations liées à l'AC (PC/DPC, certificats d'AC, conditions générales d'utilisation, etc.)
- Réception d'une demande de révocation ;

- Validation / rejet d'une demande de révocation ;
- Génération puis publication des LCR.

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 Certigna SSL 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 chaque 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 une fois toutes les deux 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 une

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.

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 5 ans, comptés au maximum à partir de l'acceptation du certificat par le gestionnaire de certificat. 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 gestionnaire de certificat responsable à un instant "t" du serveur désigné dans le certificat émis par l'AC dans le certificat émis par l'AC.

Certificats et LCR / LAR émis par l'AC Les certificats de clés de serveurs et d'AC, ainsi que les LCR / LAR produites (respectivement par l'AC Certigna SSL et AC Certigna Racine), sont archivés pendant au moins cinq ans après leur expiration.

Journaux d'événements Les journaux d'événements traités au chapitre 5.4 sont archivés pendant cinq 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 Certigna SSL . 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 Certigna SSL 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 Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela, la période de validité 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'un nouveau bi-clé d'AC est généré, 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.

Pour rappel :

Suivant le système d'exploitation et/ou le navigateur utilisé par l'utilisateur le nouveau certificat de l'AC Certigna Racine peut être automatiquement installé dans les magasins de certificats des autorités de confiance grâce aux mécanismes de mise à jour (pour les éditeurs ayant reconnu

l'autorité Certigna comme autorité de confiance).

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

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 gestionnaires de certificat et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;
- 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). En outre, l'AC respecte au minimum les engagements suivants :

- elle informe les entités suivantes de la compromission : tous les gestionnaires de certificat, 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 Racine, 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 Racine.

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.

5.7.5 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.

5.7.6 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 gestionnaire de certificat 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.

5.7.7 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 gestionnaires de certificat, 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.

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.

Chapitre 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 du bi-clé de l'AC Certigna SSL .

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 de partage de Shamir n parmi m .

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 gestionnaire de certificat

Le bi-clé d'un serveur est généré exclusivement par un dispositif logiciel (applet « Certigna-Factory ») fourni par l'AC, et sous le contrôle du gestionnaire de certificat.

6.1.2 Transmission de la clé privée à son propriétaire

La clé privée est générée exclusivement par le gestionnaire de certificat (poste de travail ou matériel de type HSM).

6.1.3 Transmission de la clé publique à l'AC

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 intermédiaire Certigna SSL est diffusée dans un certificat lui-même signé par l'AC Certigna Racine. La clé publique de l'AC Certigna Racine 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).

Rappel :

Suivant le système d'exploitation et/ou le navigateur utilisé par l'utilisateur le certificat de l'AC Certigna Racine peut être automatiquement installé dans les magasins de certificats des autorités de confiance grâce aux mécanismes de mise à jour (pour les éditeurs ayant reconnu l'autorité Certigna comme autorité de confiance).

6.1.5 Tailles des clés

Clés d'AC

– AC Certigna Racine

Le bi-clé d'AC est de type RSA 2048 bits

L'algorithme de hachage est de type SHA-1 (160 bits)

- AC Certigna SSL
 - Le bi-clé d'AC est de type RSA 2048 bits
 - L'algorithme de hachage est de type SHA-1 (160 bits)

Clés serveurs

Les bi-clés des serveurs sont de type RSA 2048 bits
L'algorithme de hachage est de type SHA-1 (160 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 au bi-clé (cf. caractéristiques du module TrustWay CryptoBox).

Clés serveurs

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

6.1.7 Objectifs d'usage de la clé

Clés d'AC

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

Clés serveurs

L'utilisation de la clé privée du serveur et du certificat associé est exclusivement limitée au service d'établissement d'une session sécurisée SSL/TLS(cf. chapitre 1.4.1).

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

Le module cryptographique utilisé par l'AC Certigna Racine et l'AC Certigna SSL pour la génération et la mise en œuvre de leurs clés de signature est la TrustWay CryptoBox S507 de la société BULL qualifiée au niveau renforcée conformément à l'ordonnance n° 2005-1516 du 8 décembre 2005.

Dispositifs de protection des clés privées des serveurs

Les gestionnaires de certificat s'engagent à mettre tous les moyens en œuvre pour protéger efficacement les clés privées sur leurs serveurs. Concrètement cela peut se traduire par la mise en place de :

- une protection physique des serveurs avec des accès contrôlés ;
- des procédures d'authentification sur les serveurs ;
- des droits d'accès ;
- un module cryptographique (type HSM).

6.2.2 Contrôle de la clé privée par plusieurs personnes

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

La génération du 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 Certigna SSL 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 quatre 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 en aucun cas séquestrées.

Clés serveurs

Les clés privées des serveurs sont exploitées exclusivement à des fins de *Authentication Serveur* et ne font par conséquent pas l'objet de séquestre sur l'AC.

6.2.4 Copie de secours de la clé privée

Clés d'AC

Les clés d'AC font l'objet d'une copie de secours hors du module cryptographique. Cette copie est chiffrée par Triple-DES et protégée en intégrité et authenticité avec un calcul de MAC. Le chiffrement de la clé (wrapping) est réalisé au sein du module cryptographique.

La clé de chiffrement de longueur 168 bits est obtenue par diversification d'une clé de base avec un secret d'initialisation partagé entre deux opérateurs. 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.

Le module cryptographique est certifié Critères Communs au niveau EAL4 augmenté et, est par conséquent en conformité avec les règles définies dans le document « Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 1.11 », en particulier pour la méthode de chiffrement des clés exportées. A aucun moment, les clés privées d'AC sont en clair en dehors du module cryptographique. La cible de sécurité a été déclarée conforme au profil de protection [CWA14167-2], Cryptographic Module for CSP Signing Operations with Backup – Protection Profile (CMCSOB-PP).

Clés serveurs

Les clés privées des serveurs ne font l'objet d'aucune copie de secours par l'AC.

6.2.5 Archivage de la clé privée

Clés d'AC

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

Clés serveurs

Les clés privées de serveurs ne sont en aucun cas archivées.

Pour les clés privées générées sur HSM, il est techniquement impossible d'effectuer une copie de ces clés hors HSM.

6.2.6 Transfert de la clé privée avec le module cryptographique

Pour rappel, les clés privées des serveurs sont générées sous la responsabilité des gestionnaire de certificat.

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.

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 (officier sécurité, et un opérateur habilité à administrer le module cryptographique).

Clés serveurs

Le gestionnaire de certificat génère lui-même les données d'activation de son certificat (mot de passe pour utiliser son certificat).

6.2.9 Méthode de désactivation de la clé privée

Clés d'AC

Le module cryptographique (carte PCI intégrée dans le boîtier 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 du boîtier.

Clés serveurs

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

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 serveurs

Le gestionnaire de certificat 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.

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 : 1, 2 ou 3 ans en fonction du contrat souscrit.

Pour l'IGC Certigna, la durée de validité du certificat de l'AC Certigna Racine est de 20 ans, et celle du certificat de l'AC Certigna SSL est de 10 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

La clé privée du serveur n'étant pas générée par l'AC, aucune exigence n'est formulée.

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 l'officier de 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

Le gestionnaire de certificat gère lui-même son équipement informatique et, à ce titre, génère de manière autonome sous sa seule responsabilité son bi-clé et ses données d'activation (par exemple, mot de passe nécessaire pour utiliser sa clé privée).

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

Le niveau de sécurité des systèmes informatiques est adapté à l'exploitation de l'IGC au regard de la norme ETSI TS 102 042.

Le boîtier BULL TrustWay CryptoBox exploité par l'IGC est qualifiée au niveau renforcée conformément à l'ordonnance n° 2005-1516 du 8 décembre 2005. Le boîtier répond aux exigences de sécurité du profil de protection CWA 14167-2 version 0.28 du 27 octobre 2003, certifié par l'ANSSI sous la référence [PP/0308].

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 Certigna Racine ou de l'AC Certigna SSL 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 Certigna SSL 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

Le niveau de sécurité du cycle de vie des systèmes est adapté à l'exploitation de l'IGC au regard de la ETSI TS 102 042 V2.1.2.

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.

6.7.1 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).

Chapitre 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 des certificats émis par l'AC Certigna Racine

Les certificats émis par l'AC Certigna Racine, en particulier le certificat de l'autorité Certigna SSL , contiennent les champs de base et les extensions suivantes :

Champs de base

Champ	Description
Version	V3
Serial Number	Numéro de série unique
Signature	Identifiant de l'algorithme de signature de l'AC SHA-1 160 bits RSA 2048 bits
Issuer	DN={ } countryName : C=FR organizationName : O=Dhimyotis commonName : CN=Certigna
Validity	Dates et heures d'activation et d'expiration du Certificat
Subject	DN={ } serialNumber : Numéro de série unique countryName : C=FR organizationName : O=Dhimyotis organizationUnitName : OU=0002 481463081 commonName : CN= Nom de l'AC intermédiaire
Subject Public Key Info	RSA 2048 bits

Extensions

Champ	C	Description
Authority Key Identifier	N	Identifiant de la clé publique de l'autorité Certigna
Subject Key Identifier	N	Identifiant de la clé publique de l'autorité intermédiaire
Key Usage	O	Signature de certificat Signature de la liste de révocation hors connexion Signature de la liste de révocation
CRL Distribution Points	N	URL=http ://crl.certigna.fr/certigna.crl URL=http ://crl.dhimyotis.com/certigna.crl
Basic Constraints	N	SubjectType=CertAuthority PathLengthConstraint=aucune
netscape-cert-type	N	S/MIME, signature
netscape-revocation-url	N	URL=http ://crl.certigna.fr/certigna.crl

7.2 Profil des certificats émis par l'AC Certigna SSL

Les certificats émis par l'AC Certigna SSL contiennent les champs de base et les extensions suivantes :

Champs de base

Champ	Description
Version	V3
Serial Number	Numéro de série unique
Signature	Identifiant de l'algorithme de signature de l'AC SHA-1 160 bits RSA 2048 bits
Issuer	DN={ } serialNumber : Numéro de série unique countryName : C=FR organizationName : O=Dhimyotis organizationUnitName : OU=0002 481463081 commonName : CN=Certigna SSL
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 commonName : CN=FQDN principal du serveur informatique organizationName : O=Nom de l'entité à laquelle appartient le serveur informatique organizationalUnitName : OU=ICD(*) + identifiant de l'entité à laquelle appartient le serveur informatique enregistré conformément à la législation et aux réglementations en vigueur
Subject Public Key Info	RSA 2048 bits

(*) cf chapitre 3.1.2 ("Nécessité d'utilisation de noms explicites")

Extensions

Champ	C	Description
Authority Key Identifier	N	Identifiant de la clé publique de l'autorité Certigna SSL
Subject Key Identifier	N	Identifiant de la clé publique du serveur
Key Usage	O	digitalSignature, keyEncipherment
Extended Key Usage	N	serverAuth, msSGC, nsSGC
Subject Alternative Name	N	dNSName : DNSName=FQDN principal du serveur informatique optionnellement : DNSName=FQDN secondaire (1 occurrence par FQDN secondaire)
Certificate Policies	N	0.4.0.2042.1.3 1.2.250.1.177.1.1.1.7 : CPS=http://www.certigna.fr/PC
CRL Distribution Points	N	URL=http://crl.certigna.fr/certignassl.crl URL=http://crl.dhimyotis.com/certignassl.crl URL=ldap://ldap.certigna.fr/cn=Certigna%20SSL, OU=IGC, DC=certigna, DC=fr?certificateRevocationList;binary URL=ldap://ldap.dhimyotis.com/cn=Certigna%20SSL, OU=IGC, DC=certigna, DC=fr?certificateRevocationList;binary
Authority Information Access	N	URL=http://ssl.ocsp.certigna.fr URL=http://ssl.ocsp.dhimyotis.com
Basic Constraints	N	SubjectType=EndEntity PathLengthConstraint=0
netscape-cert-type	N	SSL Server
netscape-revocation-url	N	URL=http://crl.certigna.fr/certignassl.crl

7.3 Profil des LCR

Champs de base

Champ	Description
Version	V2
Signature	Identifiant de l'algorithme de signature de l'AC SHA-1 160 bits RSA 2048 bits
Issuer	DN={ } serialNumber : Numéro de série unique countryName : C=FR organizationName : O=Dhimyotis organizationUnitName : OU=0002 481463081 commonName : CN=Certigna SSL
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 la clé publique de l'autorité Certigna SSL
CRL Number	N	Contient le n° de série de la LCR

Chapitre 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 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'AE déléguées ou des mandataires de certification au même titre que les audits effectués sur son IGC. Elle s'assure entre autres que ces opérateurs d'AE déléguées 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 par an, 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 : « réussite », « échec », « à confirmer ».

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

- En cas d' « échec », et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.
- En cas de résultat « à confirmer », l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être réparées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de « réussite », l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

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'autorité de certification AC Certigna SSL .

Chapitre 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 gestionnaire de certificat est facturée selon les tarifs définis dans le contrat d'abonnement.

9.1.2 Tarifs pour accéder aux certificats

La présente PC ne prévoit pas de tarifs pour accéder aux certificats.

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

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

En cas de non-conformité du dossier de demande de certificat, l'AC pourra rejeter la demande et le paiement sera alors restitué dans un délai de 1 mois à dater du rejet final de la demande.

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 serveurs ;
- Les données d'activation associées aux clés privées d'AC et des gestionnaires de certificat ;
- Tous les secrets de l'IGC ;
- Les journaux d'événements des composantes de l'IGC ;
- Les dossiers d'enregistrement des gestionnaires de certificat ;
- 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 porteurs à des tiers dans le cadre de procédures légales. Elle donne également accès à ces informations au gestionnaire de certificat, et le cas échéant à l'opérateur d'AED ou le MC en relation avec le gestionnaire de certificat.

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 n^o 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 gestionnaires de certificat 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.

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 gestionnaires de certificat, 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

Les informations que tout gestionnaire de certificat remet à l'AC sont intégralement protégées contre la divulgation sans le consentement de celui-ci, une décision judiciaire ou autre autorisation légale.

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci dessous).

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.

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

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 le gestionnaire de certificat correspondant 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 gestionnaires de certificat 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 gestionnaire de certificat 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 document de référence ETSI TS 102 042, 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 gestionnaires de certificat 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 Obligations communes aux composantes de l'IGC

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.

9.6.3 Service d'enregistrement

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

9.6.4 Gestionnaires de certificat

Dans le cadre du contrat d'abonnement, le gestionnaire de certificat garantit à l'autorité Certigna SSL :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- Protection de la clé privée du serveur dont il a la responsabilité par des moyens appropriés à son environnement pour s'assurer du contrôle exclusif de la clé privée associée au certificat ;
- Protéger ses données d'activation et, le cas échéant, les mettre en œuvre ;
- Protéger l'accès à la base de certificats du serveur ;

- Respecter les conditions d'utilisation de la clé privée du serveur et du certificat correspondant ;
- Informer l'AC de toute modification concernant les informations contenues dans le certificat serveur ;
- Faire, sans délai, une demande de révocation du certificat serveur dont il est responsable auprès de l'AE(ou le cas échéant du MC de son entité) et d'arrêter immédiatement et définitivement l'utilisation du certificat SSL EV, en cas de :
 - compromission ou de suspicion de compromission de la clé privée correspondante ;
 - données contenues dans le certificat devenues incorrectes ou inexactes.
- Cesser d'utiliser le certificat SSL EV immédiatement et définitivement à la fin de validité ou à la révocation de ce dernier.

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

Ces informations s'appliquent également aux opérateurs d'AED et aux MC.

9.6.5 Utilisateurs de certificats

Les tiers utilisateurs doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application ;
- Pour chaque certificat de la chaîne de certification, du certificat du serveur jusqu'à l'AC Certigna Racine, 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.

9.6.6 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 gestionnaires de certificat, ni d'un dommage causé par un fait extérieur, notamment en cas de :

- Perte de profits ;
- Perte de données ;
- Dommage indirect consécutivement à l'utilisation ou en relation avec l'utilisation de certificat ;
- Fraude ou faute intentionnelle du gestionnaire de certificat ou de l'entité ;

- Utilisation d'un certificat pour une autre application que les applications définies au chapitre 1.4.1 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 norme ETSI TS 102 042 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 de la norme ETSI TS 102 042 et des éventuels documents complémentaires à cette dernière.

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 l’AAP de cette PC par rapport à la norme ETSI TS 102 042. La DPC n’est applicable qu’après approbation de l’AAP.

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

Lorsque la modification de la PC est de nature typographique ou lorsque la modification de la PC porte sur le niveau de qualité et de sécurité des fonctions de l’AC et de l’AE sans perte de conformité d’un certificat émis avec la PC qu’il supporte, les OID de la PC et de la DPC correspondante ne sont pas modifiés.

Lorsque la modification de la PC entraîne la perte de conformité d’un certificat avec la PC qu’il supporte, les OID de la PC et de la DPC sont modifiés et notifiés.

9.13 Dispositions concernant la résolution de conflits

Il est rappelé que les conditions d’utilisation des certificats émis par l’AC Certigna SSL 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 gestionnaires de certificat 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.

Chapitre 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 EAL3 des Critères Communs pour le niveau LCP.

Le module cryptographique utilisé par l'AC est le module TrustWay CryptoBox S507 qualifié au niveau renforcé. Il répond aux exigences du chapitre 10.1.

La carte cryptographique Bull Trustway Crypto PCI a été certifiée dans sa version 76675628-220 S507 - RSA4096 (ANSSI-CC-2010/09) selon les Critères Communs le 26 Mars 2010, au niveau d'assurance EAL4 augmenté des composants d'assurance suivants : ALC FLR.3 (correction

d'anomalies), AVA_VLA.4 (tests de vulnérabilité) , AVA_CCA.1 et ADV_IMP.2 (fourniture de l'ensemble du code).

Les mécanismes cryptographiques ont fait l'objet d'une cotation par l'ANSSI. Ils sont compatibles avec le niveau de résistance visé.

La carte cryptographique Bull Trustway Crypto PCI (version 76675628-220 S507) a reçu une qualification au niveau renforcé le 16 avril 2010 [n° 927/ANSSI/SR/RGL].

Elle est également conforme au profil de protection (PP) « CWA14167-2 Cryptographic Module for CSP signing Operations with backup », version 0.28 du 27/10/2003 certifié par l'ANSSI, relatif aux modules cryptographiques pour les opérations de signature des prestataires de service de certification (qui s'inscrit dans l'application du décret précédemment cité).