

## Déclaration des Pratiques de Certification

**FR03**

*(Cachet Serveur visible 2D-DOC)*

**OID = 1.2.250.1.177.2.2.2.1**

Réf. 2015-202

Version 1.2

# SOMMAIRE

<b>SOMMAIRE</b> .....	<b>2</b>
<b>SUIVI DES MODIFICATIONS</b> .....	<b>8</b>
<b>1. INTRODUCTION</b> .....	<b>9</b>
1.1. PRESENTATION GENERALE.....	9
1.2. IDENTIFICATION DU DOCUMENT .....	9
1.3. DEFINITIONS ET ACRONYMES .....	9
1.3.1. <i>Acronymes</i> .....	9
1.3.2. <i>Définitions</i> .....	10
1.4. ENTITES INTERVENANT DANS L'IGC .....	13
1.4.1. <i>Autorité de certification</i> .....	13
1.4.2. <i>Autorité d'enregistrement</i> .....	13
1.4.3. <i>Responsable de certificats électroniques de services applicatifs</i> .....	14
1.4.4. <i>Utilisateurs de certificats</i> .....	14
1.4.5. <i>Autres participants</i> .....	14
1.5. USAGE DES CERTIFICATS .....	15
1.5.1. <i>Domaines d'utilisation applicables</i> .....	15
1.5.2. <i>Domaines d'utilisation interdits</i> .....	16
1.6. GESTION DE LA PC .....	16
1.6.1. <i>Entité gérant la PC</i> .....	16
1.6.2. <i>Point de contact</i> .....	16
1.6.3. <i>Entité déterminant la conformité de la DPC avec la PC</i> .....	16
1.6.4. <i>Procédures d'approbation de la conformité de la DPC</i> .....	16
<b>2. RESPONSABILITE CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS</b> .....	<b>17</b>
2.1. ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS .....	17
2.2. INFORMATIONS DEVANT ETRE PUBLIEES .....	17
2.2.1. <i>Publication de la documentation</i> .....	17
2.2.2. <i>Publication de la LCR</i> .....	18
2.2.3. <i>Publication de la LAR</i> .....	18
2.3. DELAIS ET FREQUENCES DE PUBLICATION .....	18
2.3.1. <i>Publication de la documentation</i> .....	18
2.3.2. <i>Publication des certificats d'AC</i> .....	18
2.3.3. <i>Publication de la LCR</i> .....	19
2.3.4. <i>Publication de la LAR</i> .....	19
2.4. CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES.....	19
<b>3. IDENTIFICATION ET AUTHENTIFICATION</b> .....	<b>20</b>
3.1. NOMMAGE.....	20
3.1.1. <i>Types de noms</i> .....	20
3.1.2. <i>Nécessité d'utilisation de noms explicites</i> .....	20
3.1.3. <i>Anonymisation ou pseudonymisation des porteurs</i> .....	20
3.1.4. <i>Règles d'interprétation des différentes formes de noms</i> .....	20
3.1.5. <i>Unicité des noms</i> .....	20
3.1.6. <i>Identification, authentification et rôle des marques déposées</i> .....	21

3.2. VALIDATION INITIALE DE L'IDENTITE.....	21
3.2.1. Méthode pour prouver la possession de la clé privée.....	21
3.2.2. Validation de l'identité d'un organisme.....	21
3.2.3. Validation de l'identité d'un individu.....	21
3.2.4. Informations non vérifiées du RCCS et du service applicatif.....	26
3.2.5. Validation de l'autorité du demandeur.....	26
3.3. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES .....	26
3.3.1. Identification et validation pour un renouvellement courant.....	26
3.3.2. Identification et validation pour un renouvellement après révocation.....	27
3.4. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION .....	27
<b>4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS</b>	<b>28</b>
.....	
4.1. DEMANDE DE CERTIFICAT.....	28
4.1.1. Origine d'une demande de certificat.....	28
4.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat....	28
4.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT .....	28
4.2.1. Exécution des processus d'identification et de validation de la demande .....	28
4.2.2. Acceptation ou rejet de la demande .....	29
4.2.3. Durée d'établissement du certificat.....	29
4.3. DELIVRANCE DU CERTIFICAT.....	29
4.3.1. Actions de l'AC concernant la délivrance du certificat.....	29
4.3.2. Notification par l'AC de la délivrance du certificat.....	30
4.4. ACCEPTATION DU CERTIFICAT .....	30
4.4.1. Démarche d'acceptation du certificat .....	30
4.4.2. Publication du certificat.....	30
4.4.3. Notification par l'AC aux autres entités de la délivrance du certificat.....	30
4.5. USAGES DE LA BI-CLE ET DU CERTIFICAT.....	31
4.5.1. Utilisation de la clé privée et du certificat par le RCCS.....	31
4.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat .....	31
4.6. RENOUVELLEMENT D'UN CERTIFICAT .....	31
4.7. DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE AU CHANGEMENT DU BI-CLE.....	32
4.7.1. Causes possibles de changement d'un bi-clé.....	32
4.7.2. Origine d'une demande d'un nouveau certificat.....	32
4.8. MODIFICATION DU CERTIFICAT.....	32
4.9. REVOCATION ET SUSPENSION DES CERTIFICATS.....	32
4.9.1. Causes possibles d'une révocation.....	32
4.9.2. Origine d'une demande de révocation .....	33
4.9.3. Procédure de traitement d'une demande de révocation.....	33
4.9.4. Délai accordé au RCCS pour formuler la demande de révocation .....	35
4.9.5. Délai de traitement par l'AC d'une demande de révocation .....	35
4.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats.....	35
4.9.7. Fréquence d'établissement des LCR .....	35
4.9.8. Délai maximum de publication d'une LCR .....	35
4.9.9. Exigences sur la vérification en ligne de la révocation et de l'état des certificats	36
4.9.10. Autres moyens disponibles d'information sur les révocations.....	36
4.9.11. Exigences spécifiques en cas de compromission de la clé privée .....	36
4.9.12. Suspension de certificat.....	36
4.10. FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS.....	36
4.10.1. Caractéristiques opérationnelles .....	36

4.10.2. Disponibilité de la fonction .....	37
4.11. FIN DE LA RELATION ENTRE LE RCCS ET L'AC.....	37
4.12. SEQUESTRE DE CLE ET RECOUVREMENT .....	37
<b>5. MESURES DE SECURITE NON TECHNIQUES .....</b>	<b>38</b>
5.1. MESURES DE SECURITE PHYSIQUE .....	38
5.1.1. Situation géographique et construction des sites.....	38
5.1.2. Accès physique .....	38
5.1.3. Alimentation électrique et climatisation .....	39
5.1.4. Vulnérabilité aux dégâts des eaux.....	39
5.1.5. Prévention et protection incendie .....	39
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 SECURITE PROCEDURALES .....	41
5.2.1. Rôles de confiance.....	41
5.2.2. Nombre de personnes requises par tâche .....	42
5.2.3. Identification et authentification pour chaque rôle.....	42
5.2.4. Rôle exigeant une séparation des attributions .....	43
5.3. MESURES DE SECURITE VIS-A-VIS DU PERSONNEL .....	43
5.3.1. Qualifications, compétences et habilitations requises .....	43
5.3.2. Procédures de vérification des antécédents .....	44
5.3.3. Exigences en matière de formation initiale.....	44
5.3.4. Exigences et fréquence en matière de formation continue.....	44
5.3.5. Fréquence et séquence de rotation entre différentes attributions.....	45
5.3.6. Sanctions en cas d'actions non autorisées .....	45
5.3.7. Exigences vis-à-vis du personnel des prestataires externes.....	46
5.3.8. Documentation fournie au personnel.....	46
5.4. PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT .....	47
5.4.1. Type d'événements à enregistrer .....	47
5.4.2. Fréquence de traitement des journaux d'événements .....	48
5.4.3. Période de conservation des journaux d'événements.....	48
5.4.4. Protection des journaux d'événements .....	48
5.4.5. Procédure de sauvegarde des journaux d'événements.....	49
5.4.6. Système de collecte des journaux d'événements.....	49
5.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement ..	49
5.4.8. Evaluation des vulnérabilités .....	49
5.5. ARCHIVAGE DES DONNEES .....	50
5.5.1. Types de données à archiver .....	50
5.5.2. Période de conservation des archives .....	50
5.5.3. Protection des archives .....	51
5.5.4. Procédure de sauvegarde des archives .....	51
5.5.5. Exigences d'horodatage des données .....	51
5.5.6. Système de collecte des archives .....	51
5.5.7. Procédures de récupération et de vérification des archives .....	51
5.6. RENOUELEMENT D'UNE CLE DE COMPOSANTE DE L'IGC .....	52
5.6.1. Clé d'AC .....	52
5.6.2. Clés des autres composantes.....	52
5.7. REPRISE SUITE A COMPROMISSION ET SINISTRE .....	52
5.7.1. Procédures de remontée et de traitement des incidents et des compromissions....	52

5.7.2. Procédures de reprise en cas de corruption des ressources informatiques.....	53
5.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante .....	53
5.7.4. Capacité de continuité d'activité suite à un sinistre.....	54
5.8. FIN DE VIE DE L'IGC .....	54
<b>6. MESURES DE SECURITE TECHNIQUES.....</b>	<b>57</b>
6.1. GENERATION ET INSTALLATION DE BI-CLES.....	57
6.1.1. Génération des bi-clés.....	57
6.1.2. Transmission de la clé privée à son propriétaire.....	58
6.1.3. Transmission de la clé publique à l'AC.....	58
6.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats .....	59
6.1.5. Taille des clés.....	59
6.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité.....	59
6.1.7. Objectifs d'usage de la clé.....	60
6.2. MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES .....	60
6.2.1. Standards et mesures de sécurité pour les modules cryptographiques.....	60
6.2.2. Contrôle de la clé privée par plusieurs personnes.....	60
6.2.3. Séquestre de la clé privée.....	61
6.2.4. Copie de secours de la clé privée.....	62
6.2.5. Archivage de la clé privée .....	62
6.2.6. Transfert de la clé privée avec le module cryptographique.....	62
6.2.7. Stockage de la clé privée dans un module cryptographique.....	63
6.2.8. Méthode d'activation de la clé privée .....	63
6.2.9. Méthode de désactivation de la clé privée .....	63
6.2.10. Méthode de destruction des clés privées .....	64
6.2.11. Niveau d'évaluation sécurité du module cryptographique.....	64
6.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES.....	64
6.3.1. Archivage des clés publiques .....	64
6.3.2. Durées de vie des bi-clés et des certificats.....	64
6.4. DONNEES D'ACTIVATION .....	64
6.4.1. Génération et installation des données d'activation .....	64
6.4.2. Protection des données d'activation.....	65
6.4.3. Autres aspects liés aux données d'activation .....	65
6.5. MESURES DE SECURITE DES SYSTEMES INFORMATIQUES .....	65
6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques.....	65
6.5.2. Niveau d'évaluation sécurité des systèmes informatiques.....	66
6.6. MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE.....	67
6.6.1. Mesures de sécurité liées au développement des systèmes .....	67
6.6.2. Mesures liées à la gestion de la sécurité.....	67
6.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes .....	67
6.7. MESURES DE SECURITE RESEAU .....	67
6.8. HORODATAGE ET SYSTEME DE DATATION .....	68
<b>7. PROFIL DES CERTIFICATS ET DES LCR .....</b>	<b>69</b>
7.1. PROFIL DU CERTIFICAT DE L'AC.....	69
7.2. PROFIL DES CERTIFICATS CACHET SERVEUR .....	70
7.3. PROFIL DES LCR .....	71
7.4. TRAITEMENT DES EXTENSIONS DE CERTIFICATS PAR LES APPLICATIONS.....	71

<b>8. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS.....</b>	<b>73</b>
8.1. FREQUENCES ET/OU CIRCONSTANCES DES EVALUATIONS .....	73
8.2. IDENTITES/QUALIFICATIONS DES EVALUATEURS .....	73
8.3. RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES.....	74
8.4. SUJETS COUVERTS PAR LES EVALUATIONS.....	74
8.5. ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS .....	74
8.6. COMMUNICATION DES RESULTATS .....	75
<b>9. AUTRES PROBLEMATIQUES METIERS ET LEGALES.....</b>	<b>76</b>
9.1. TARIFS.....	76
9.1.1. <i>Tarifs pour la fourniture ou le renouvellement de certificats</i> .....	76
9.1.2. <i>Tarifs pour accéder aux certificats</i> .....	76
9.1.3. <i>Tarifs pour accéder aux informations d'état et de révocation des certificats</i> .....	76
9.1.4. <i>Tarifs pour d'autres services</i> .....	76
9.1.5. <i>Politique de remboursement</i> .....	76
9.2. RESPONSABILITE FINANCIERE.....	76
9.2.1. <i>Couverture par les assurances</i> .....	76
9.2.2. <i>Autres ressources</i> .....	76
9.2.3. <i>Couverture et garantie concernant les entités utilisatrices</i> .....	76
9.3. CONFIDENTIALITE DES DONNEES PROFESSIONNELLES .....	77
9.3.1. <i>Périmètre des informations confidentielles</i> .....	77
9.3.2. <i>Informations hors du périmètre des informations confidentielles</i> .....	77
9.3.3. <i>Responsabilités en termes de protection des informations confidentielles</i> .....	77
9.4. PROTECTION DES DONNEES PERSONNELLES .....	78
9.4.1. <i>Politique de protection des données personnelles</i> .....	78
9.4.2. <i>Informations à caractère personnel</i> .....	78
9.4.3. <i>Informations à caractère non personnel</i> .....	78
9.4.4. <i>Responsabilité en termes de protection des données personnelles</i> .....	78
9.4.5. <i>Notification et consentement d'utilisation des données personnelles</i> .....	78
9.4.6. <i>Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives</i> .....	79
9.4.7. <i>Autres circonstances de divulgation d'informations personnelles</i> .....	79
9.5. DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE.....	79
9.6. INTERPRETATIONS CONTRACTUELLES ET GARANTIES .....	79
9.6.1. <i>Autorités de Certification</i> .....	80
9.6.2. <i>Service d'enregistrement</i> .....	80
9.6.3. <i>RCCS</i> .....	81
9.6.4. <i>Utilisateurs de certificats</i> .....	81
9.6.5. <i>Autres participants</i> .....	81
9.7. LIMITE DE GARANTIE .....	81
9.8. LIMITE DE RESPONSABILITE.....	81
9.9. INDEMNITES .....	82
9.10. DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC.....	82
9.10.1. <i>Durée de validité</i> .....	82
9.10.2. <i>Fin anticipée de validité</i> .....	82
9.10.3. <i>Effets de la fin de validité et clauses restant applicables</i> .....	82
9.11. NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS .....	82
9.12. AMENDEMENTS A LA PC .....	83
9.12.1. <i>Procédures d'amendements</i> .....	83
9.12.2. <i>Mécanisme et période d'information sur les amendements</i> .....	83

9.12.3. Circonstances selon lesquelles l'OID doit être changé.....	83
9.13. DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS .....	83
9.14. JURIDICTIONS COMPETENTES .....	83
9.15. CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS .....	84
9.16. DISPOSITIONS DIVERSES .....	84
9.16.1. Accord global.....	84
9.16.2. Transfert d'activités.....	84
9.16.3. Conséquences d'une clause non valide .....	84
9.16.4. Application et renonciation.....	84
9.16.5. Force majeure .....	84
9.17. AUTRES DISPOSITIONS .....	84
<b>10. ANNEXE 1 : EXIGENCE DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC.....</b>	<b>85</b>
10.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE.....	85
10.2. EXIGENCES SUR LA QUALIFICATION.....	85
<b>11. ANNEXE 2 : EXIGENCES DE SECURITE DU DISPOSITIF DE CREATION DE CACHET SERVEUR.....</b>	<b>86</b>
11.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE.....	86
11.2. EXIGENCES SUR LA QUALIFICATION.....	86
<b>12. ANNEXE 3 : DOCUMENTS DE REFERENCE .....</b>	<b>87</b>

## SUIVI DES MODIFICATIONS

<b>Date</b>	<b>Version</b>	<b>Auteur</b>	<b>Evolution du document</b>
11/03/2015	1.0	Y. LEPLARD	Création
27/04/2015	1.1	R. DELVAL	Archivage des réponses OCSP
01/08/2016	1.2	J. ALLEMANDOU	Précision sur la vérification de l'adresse email (cf. 3.2)



# 1. Introduction

## 1.1. Présentation générale

Dhimyotis s'est doté d'une Autorité de Certification (AC) de type Cachet Serveur pour délivrer des certificats destinés à être utilisés dans le processus 2D-DOC tel que défini par l'Agence Nationale des Titres Sécurisés (ANTS).

Ces certificats permettent au client de signer selon un mécanisme spécifique des codes barres de type « 2D-DOC » afin de sécuriser des documents papier ou électroniques.

Dans la suite du document le terme 2D-DOC fera référence au processus et à la norme définie par l'ANTS.

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

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

La présente DPC vise la conformité à la PC Type « Certificats électroniques de Services Applicatifs » pour un usage Cachet Serveur et un niveau \*, du Référentiel Général de Sécurité (RGS) élaboré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et aux exigences du CA/BROWSER FORUM.

## 1.2. Identification du document

La présente DPC est dénommée « Description des Pratiques de Certification FR03, Cachet Serveur ».

Elle peut être identifiée par le nom de l'AC : FR03 qui a été délivré par l'ANTS conformément au processus 2D-DOC, ainsi que par son OID : 1.2.250.1.177.2.2.2.1.

## 1.3. Définitions et acronymes

### 1.3.1. Acronymes

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

<b>AA</b>	Autorité Administrative
<b>AAP</b>	Autorité d'Approbation des Politiques
<b>AC</b>	Autorité de Certification
<b>AE</b>	Autorité d'Enregistrement
<b>AED</b>	Autorité d'Enregistrement Déléguée
<b>AH</b>	Autorité d'Horodatage
<b>ANSSI</b>	Agence nationale de la sécurité des systèmes d'information
<b>ANTS</b>	Agence Nationale des Titres Sécurisés

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

### 1.3.2. Définitions

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

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

**Applicatif de vérification de cachet** - Il s'agit de l'application mise en oeuvre par l'utilisateur pour vérifier le cachet des données reçues à partir de la clé publique du serveur contenue dans le certificat correspondant.

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

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

**Autorité de Certification** – Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ « issuer » du certificat).

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

**Cachet serveur** – Signature numérique effectuée par un serveur applicatif sur des données dans le but de pouvoir être utilisée soit dans le cadre d'un service d'authentification de l'origine des données, soit dans le cadre d'un service de non répudiation.

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

**Composante** - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptographie et jouant un rôle déterminé dans la mise en oeuvre opérationnelle d'au moins une fonction de l'IGC. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

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

**Dispositif de protection des éléments secrets** - Désigne un dispositif de stockage des éléments secrets remis au RCCS (ex. clé privée, code PIN, ...). Il peut prendre la forme d'une carte à puce, d'une clé USB à capacité cryptographique ou se présenter au format logiciel (ex. fichier PKCS#12).

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

**Infrastructure de Gestion de Clés** - Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une AC, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, ...

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

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

**Politique de certification** - Ensemble de règles, identifié par un nom (OID), définissant

les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les RCCS et les utilisateurs de certificats.

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

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

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

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

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

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

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

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

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

**Utilisateur de certificat** - Entité ou personne physique qui utilise un certificat et qui s'y fie pour vérifier une signature électronique ou une valeur d'authentification provenant d'un porteur de certificat ou chiffrer des données à destination d'un porteur de certificat.

*Nota* - Un agent d'une autorité administrative qui procède à des échanges électroniques avec une autre autorité administrative est, pour cette dernière, un usager.

## 1.4. Entités intervenant dans l'IGC

### 1.4.1. Autorité de certification

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation, ...) et s'appuie pour cela sur une infrastructure technique : une IGC. L'AC est responsable de la mise en application de la PC à l'ensemble de l'IGC qu'elle a mise en place.

Pour les certificats signés en son nom, l'AC assure les fonctions suivantes :

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

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

L'AC s'engage à respecter les obligations décrites dans la présente PC.

Elle s'engage également à ce que les composants de l'IGC, internes ou externes à l'AC, auxquels elles incombent les respectent aussi.

Enfin, les parties de l'AC concernées par la génération des certificats et la gestion des révocations sont indépendantes d'autres organisations en ce qui concerne leurs décisions concernant la mise en place, la fourniture, le maintien et la suspension des services ; en particulier, les cadres dirigeants, leur personnel d'encadrement et leur personnel ayant des rôles de confiance, sont libres de toute pression d'ordre commercial, financier ou autre, qui pourraient 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.

### 1.4.2. Autorité d'enregistrement

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

- La prise en compte et la vérification des informations du futur RCCS et du service applicatif ainsi que leur entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- La prise en compte et la vérification des informations, le cas échéant, du futur mandataire de certification(\*) et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- L'établissement et la transmission de la demande de certificat à l'AC ;
- L'archivage des dossiers de demande de certificat ;
- La conservation et la protection en confidentialité et intégrité des données personnelles d'authentification du RCCS ou du MC ;
- La vérification des demandes de révocation de certificat.

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

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

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

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

### **1.4.3. Responsable de certificats électroniques de services applicatifs**

Dans le cadre de la présente PC, un RCCS ne peut être qu'une personne physique. Il est responsable de l'utilisation du certificat (et de la clé privée associée) dans lequel sont identifiés le service applicatif concerné, et également l'entité pour le compte de laquelle il utilise le certificat et avec laquelle il entretient un lien contractuel/hierarchique/réglementaire.

Le RCCS doit respecter les conditions qui lui incombent et qui sont définies dans la PC et dans les CGU.

Le certificat est rattaché au service applicatif et non au RCCS. En cas de changement de RCCS, 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 RCCS explicitement identifié.

### **1.4.4. Utilisateurs de certificats**

Un utilisateur de certificat de cachet 2D-DOC peut être :

- Un service applicatif qui signe des données électroniques. On parle d'émetteur de 2D-DOC.
- Un usager ou un service applicatif destinataire de données signées par un service applicatif de cachet 2D-DOC et qui utilise un certificat et un applicatif de vérification de cachet afin d'authentifier l'origine de ces données transmises. On parle de consommateur de 2D-DOC.

Les émetteurs de 2D-DOC doivent être référencés par l'ANTS. D'après la norme 2D-DOC, un émetteur référencé correspond à un participant (personne morale signant les 2D-DOC) référencé qui s'appuie sur la solution d'un éditeur (fournisseur de la solution technique) référencé. L'émetteur de 2D-DOC doit désigner au moins un RCCS afin d'obtenir un certificat.

L'ANTS ne contrôle pas les consommateurs de 2D-DOC.

### **1.4.5. Autres participants**

L'AC FR03 s'appuie également sur des AED pour sous-traiter une partie des fonctions de l'AE. Un opérateur d'AED a le pouvoir :

- d'autoriser, d'effectuer une demande de certificat ou de renouvellement de certificat ;
- d'effectuer une demande de révocation de certificat ;

- le cas échéant, d'enregistrer les mandataires de certification au sein des entités émettrices de demandes de certificat.

Il assure pour l'autorité Certigna FR03 , dans le contexte de la délivrance de certificat, la vérification d'identité des futurs RCCS dans les mêmes conditions et avec le même niveau de sécurité que ceux requis pour l'opérateur d'AE. Il est pour cela en relation directe avec l'AE. Les engagements de l'opérateur d'AED à l'égard de l'AC sont précisés dans un contrat écrit avec l'entité responsable de l'opérateur ainsi que dans la lettre d'engagement que doit signer ce dernier. Ces deux documents précisent notamment que l'opérateur d'AED doit effectuer de façon impartiale et scrupuleuse les contrôles d'identité et des éventuels attributs des futurs RCCS et services applicatifs, et respecter les parties de la PC et de la DPC lui incombant.

L'AC Certigna FR03 offre la possibilité à l'entité cliente de désigner un ou plusieurs mandataires de certification (MC). Ce mandataire a, par la loi ou par délégation, le pouvoir :

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

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

Il assure pour l'autorité Certigna FR03, dans le contexte de la délivrance de certificat, la vérification d'identité des futurs RCCS dans les mêmes conditions et avec le même niveau de sécurité que ceux requis pour l'opérateur d'AE. Il est pour cela en relation directe avec l'Autorité d'Enregistrement.

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

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

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

## **1.5. Usage des certificats**

### **1.5.1. Domaines d'utilisation applicables**

#### *Bi-clés et certificats du service applicatif*

Les usages sont la signature électronique de données contenues dans un 2D-DOC et la vérification de la signature électronique.

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

## *Bi-clés et certificats d'AC et de composantes*

L'AC Certigna FR03 dispose d'un seul bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur (Certigna Root CA). Le bi-clé de l'AC Certigna FR03 permet de signer les différents types d'objets qu'elle génère : certificats des services applicatifs, LCR. Les opérateurs de l'IGC disposent de certificats permettant de s'authentifier sur cette IGC. Pour les opérateurs d'AE (les opérateurs d'AED n'étant pas concernés), ce certificat permet de signer les demandes de certificats et de révocation avant leur transmission à l'AC. Ces certificats sont émis par une IGC distincte, interne à Dhimyotis, et dont le niveau de sécurité est adapté à celui requis pour l'AC Certigna FR03.

### **1.5.2. Domaines d'utilisation interdits**

Les usages autres que ceux cités dans le paragraphe précédent sont interdits. L'AC s'engage à respecter ces restrictions et à imposer leur respect par les RCCS et les utilisateurs de certificats. A cette fin, elle publie à destination des RCCS, MC et utilisateurs potentiels des CGU qui peuvent être consultées sur le site <http://www.certigna.fr> avant toute demande de certificat ou toute utilisation d'un certificat cachet serveur visible.

## **1.6. Gestion de la PC**

### **1.6.1. Entité gérant la PC**

Dhimyotis dispose d'un Comité de Sécurité présidé par l'Officier de Sécurité. Ce comité est responsable de l'élaboration, du suivi, de la modification et de la validation de la présente PC. Il statue sur toute modification nécessaire à apporter à la PC à échéance régulière.

### **1.6.2. Point de contact**

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

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

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

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

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

Toute demande de mise à jour de la DPC suit également ce processus.

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



## **2. Responsabilité concernant la mise à disposition des informations**

### **2.1. Entités chargées de la mise à disposition des informations**

L'IGC met à disposition des utilisateurs et des applications utilisatrices des certificats qu'elle émet des informations sur l'état de révocation des certificats en cours de validité émis par l'AC Certigna FR03. Ces informations sont publiées au travers de plusieurs serveurs :

- Serveur Web (2) :
  - <http://crl.certigna.fr/2ddoc.crl>
  - <http://crl.dhimyotis.com/2ddoc.crl>
- Serveur OCSP (2) :
  - <http://2ddoc.ocsp.certigna.fr>
  - <http://2ddoc.ocsp.dhimyotis.com>

Le site Internet <http://www.certigna.fr> est hébergé sur le serveur de publication hébergé sur le site principal de Dhimyotis (Data Center de CIV).

Le site Internet <http://www.dhimyotis.com> est hébergé chez un second prestataire : OVH.

Les adresses [crl.dhimyotis.com](http://crl.dhimyotis.com), et [ocsp.dhimyotis.com](http://ocsp.dhimyotis.com) sont redirigées sur le serveur de publication hébergé sur le site secondaire (datacenter IBM).

### **2.2. Informations devant être publiées**

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

- La PC;
- Les Conditions Générales d'Utilisation des services de certification Certigna FR03;
- Les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, . . . ) ;
- Le certificat d'AC Certigna Root CA et le certificat d'AC intermédiaire Certigna FR03 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 RCCS ou les utilisateurs de certificats non spécialistes du domaine, l'AC publie en dehors des PC et DPC des CGU que le futur RCCS est dans l'obligation de lire et d'accepter lors de toute demande de certificat (demandes initiales et suivantes, en cas de renouvellement) auprès de l'AE.

#### **2.2.1. Publication de la documentation**

*Publication de la PC, des conditions générales et des formulaires*

La PC, les conditions générales d'utilisation des services de certification Certigna FR03 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 RCCS et utilisateurs de certificats, et sur leur demande, sa DPC pour rendre possible l'évaluation de la conformité avec sa politique de certification. Les détails relatifs à ses pratiques ne sont toutefois pas rendus publics.

Les éléments confidentiels, les noms des documents internes relatifs aux procédures confidentielles mises en œuvre ne sont pas mentionnés dans la DPC.

### *Publication des certificats d'AC*

Les RCCS et les utilisateurs de certificat peuvent accéder aux certificats d'AC qui sont publiés aux adresses :

- <http://www.certigna.fr/autorites>
- <http://www.dhimyotis.com/autorites>

## **2.2.2. Publication de la LCR**

La liste des certificats révoqués est publiée sous format électronique aux adresses décrites dans le chapitre 2.1 ci-dessus. Ces adresses sont également indiquées dans les certificats émis par l'AC Certigna FR03.

## **2.2.3. Publication de la LAR**

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

## **2.3. Délais et fréquences de publication**

### **2.3.1. Publication de la documentation**

La PC, les CGU des services de certification Certigna FR03 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.

Afin de garantir cette disponibilité et une reprise rapide en cas de sinistre, deux sites redondants ont été mis en place (un site principal chez CIV et un site de secours chez IBM).

Afin de détecter et de corriger dans les meilleurs délais tout incident survenant lors de l'exploitation du site principal, les mesures suivantes ont été mises en place :

- Installation et exploitation d'un logiciel de supervision (Nagios) permettant de surveiller tous les éléments constitutifs de la plate-forme technique (serveurs, équipement, processus) et d'émettre en temps réel des alertes (e-mail, SMS) en cas de détection d'incident (surveillance en parallèle du site principal et du site de secours) ;
  - Développement et mise en place de scripts permettant d'automatiser/simplifier le basculement sur le site de secours (et le retour sur le site principal) ;
  - Instauration d'astreintes pendant les heures non ouvrées (avec attribution d'un portable professionnel dédié aux réceptions d'alertes) ;
  - Souscription d'un service de surveillance de sécurité 24 heures sur 24 ;
  - Création de liens VPN sécurisés permettant une prise en main de la plate-forme à distance.
- La description des procédures permettant de garantir la disponibilité et une reprise fait partie intégrante du PCA (Plan de Continuité d'Activité) qui doit être accessible aux exploitants de l'IGC. Une formation est dispensée aux exploitants pour la mise en oeuvre du PCA.
- En complément, des tests de bascule sont effectués périodiquement dans le cadre du plan de secours afin de s'assurer de la bonne configuration et de la disponibilité du site de secours. Ces tests sont effectués une à deux fois par an. Le résultat de ces tests est consigné en précisant les éventuels dysfonctionnements et ce, afin de corriger si nécessaire les procédures et les scripts. Ces rapports sont consultables par le cabinet réalisant les audits périodiques.

### **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 à minima si possible tous les 6 mois et à minima une fois par an, et à chaque nouvelle révocation.

## **2.4. Contrôle d'accès aux informations publiées**

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

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

Les opérateurs d'AE et d'AC s'authentifient sur les composantes respectives avec un certificat dont la clé privée associée est stockée sur un token. Un rôle spécifique est associé par mappage au certificat lors de son émission sur l'IGC (opérateur d'AE ou opérateur d'AC). Ce rôle est contrôlé lors de l'authentification avec certificat sur l'interface du composant. La mise en oeuvre de la clé privée (authentification réciproque SSL) nécessite l'authentification du porteur (saisie du code PIN et vérification par le token).

L'attribution d'un token et d'un certificat à un opérateur est rigoureusement contrôlée par des procédures formalisées (notamment signature procès verbaux d'attribution conservés par le responsable de sécurité).

## **3. Identification et Authentification**

### **3.1. Nommage**

#### **3.1.1. Types de noms**

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

#### **3.1.2. Nécessité d'utilisation de noms explicites**

Le DN du certificat permet d'identifier le service applicatif.

Il est construit à partir de l'identité du serveur. Cette identité comprend l'identité de l'entité ainsi que la fonction du service offert par le serveur.

Le DN a la forme suivante :

```
{  
  C = Pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée,  
  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.  
  CN = Nom du certificat, conforme à la norme 2D-DOC  
}
```

La norme 2D-DOC définit les règles suivantes :

- Les noms sont codés sur 4 caractères alphanumériques majuscules.
- Le nom FR03 de l'AC a été choisi par l'ANTS.
- Le nom des certificats cachet émis par l'AC FR03 est composé d'un code client sur les 3 premiers caractères et du numéro d'ordre chronologique du certificat cachet (de 0 à 9 puis de A à Z).

Le champ « Subject Alt Name » peut être utilisé pour rendre plus explicite le nom des certificats (en indiquant le type de document signé par le cachet).

#### **3.1.3. Anonymisation ou pseudonymisation des porteurs**

Sans objet.

#### **3.1.4. Règles d'interprétation des différentes formes de noms**

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

#### **3.1.5. Unicité des noms**

L'ANTS est garante de l'unicité des noms des AC qu'elle référence dans le cadre de la norme 2D-DOC.

La combinaison du pays, du nom du certificat, ainsi que de l'identité de l'entité (nom et identifiant) identifie de manière univoque les cachets serveurs émis.

### **3.1.6. Identification, authentification et rôle des marques déposées**

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

## **3.2. Validation initiale de l'identité**

L'enregistrement d'un RCCS 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.

Lors de la demande de certificat, l'adresse email du RC est vérifiée au travers de l'envoi de plusieurs emails qui permettent au RC d'accéder à son compte client Certigna et à certaines données d'activation lui permettant ainsi de récupérer et d'utiliser le certificat du serveur.

Un contrôle strict des dossiers de demande transmis par une tierce personne doit permettre de s'assurer que cette dernière est bien enregistrée comme opérateur d'AE déléguée, ou comme mandataire de certification pour le compte de l'entité à laquelle appartient le futur RCCS. Dans les deux cas (demande effectuée auprès de l'AE et demande effectuée via un mandataire de certification), un contrôle de l'individu est effectué sur la base des données transmises (dossier de demande de certificat, le cas échéant le dossier d'enregistrement de l'opérateur d'AED ou du mandataire de certification).

Les audits périodiques doivent prendre en compte des vérifications par échantillonnage des dossiers traités, afin de s'assurer du respect des procédures.

### **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 RCCS avant de certifier la clé publique. Pour ceci, L'AE génère le bi-clé dans un module cryptographique qualifié au minimum au niveau standard, ou bien le RCCS génère lui même son bi-clé sur un dispositif de sécurité matériel certifié au minimum au niveau 2 selon la norme [FIPS 140-2], 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).

L'AE vérifie au préalable la validité de la signature lors du traitement des demandes de certificat reçues. Ce traitement est automatisé et ne requiert par conséquent aucune intervention humaine. Toute erreur de signature, due notamment à la non-possession de la clé privée associée à la clé publique à certifier, est systématiquement détectée et provoque le rejet de la demande.

### **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 RCCS correspondant. Le cas échéant, ce dernier devra démontrer que la marque déposée apparaissant dans l'identité du serveur appartient bien à l'entité qu'il représente.

Un RCCS peut être amené à changer en cours de validité du certificat serveur correspondant.

Dans ce cas, tout nouveau RCCS doit également faire l'objet d'une procédure d'enregistrement.

Le RCCS 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 RCCS, et du serveur informatique correspondant, peut se faire soit directement auprès de l'AE, soit via un mandataire de certification de l'entité. Dans ce dernier cas, le MC doit être préalablement enregistré par l'AE.

### *Enregistrement d'un RCCS sans MC pour un certificat à émettre*

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

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

- La demande de certificat cachet 2D-DOC (formulaire disponible sur le site de Certigna <http://www.certigna.fr>), datée de moins de trois mois, remplie et co-signée par un représentant légal de l'entité et par le RCCS comportant notamment :

- L'acceptation des termes et conditions (conditions générales d'utilisation) ;
- Le type de documents à signer par le cachet ;
- Les coordonnées d'un représentant légal de l'entité (nom, entreprise, adresse, téléphone, e-mail) ;
- Les coordonnées du futur RCCS (nom, entreprise, adresse, téléphone, e-mail).

- Un mandat signé, et daté de moins de trois mois, par un représentant légal de l'entité désignant le cas échéant le futur RCCS comme étant habilité à être RCCS pour le serveur informatique auquel le certificat doit être délivré. Ce mandat doit être signé pour acceptation par le futur RCCS ;

- Des informations d'identification de l'entité, qui doit être référencée par l'ANTS (au titre de « participant »).

*Pour une entreprise :*

- Tout document attestant de la qualité du représentant légal (par exemple, un exemplaire des statuts de l'entreprise, en cours de validité, portant signature de ses représentants) ;
- Toute pièce, valide au moment de l'enregistrement, portant le numéro SIREN de l'entreprise (extrait KBIS ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements) ou, à défaut, une autre pièce valide attestant l'identification unique de l'entreprise qui figurera dans le certificat.

*Pour une administration :*

- Une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative.

- La photocopie d'une pièce d'identité officielle (comportant une photo d'identité) en cours de validité au moment de l'enregistrement du futur RCCS, certifiée conforme par le futur RCCS (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 ce dernier (date, de moins de 3 mois, et signature précédées de la mention "copie certifiée conforme à l'original").

- Pour les certificats utilisés sur les justificatifs de domicile : l'avis de participation attestant que la personne morale, porteuse du certificat, fait partie la liste des participants du dispositif 2D-doc autorisés par le Ministère de l'intérieur.

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

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

Les opérateurs d'AE et d'AED sont sensibilisés sur les fraudes qui peuvent intervenir sur la délivrance de documents ou copies de documents officiels (documents falsifiés). Une attention particulière doit être apportée aux contrôles de validité des pièces fournies (date de validité des pièces d'identité, âge des demandes, etc.). Ces aspects sont développés lors de la formation initiale prévue pour les opérateurs d'AE et détaillés dans le plan de formation du personnel de l'IGC Certigna [REF24].

Les audits périodiques doivent prendre en compte des vérifications par échantillonnage des dossiers traités, afin de s'assurer du respect des procédures. Ces audits peuvent être menés par le cabinet d'audit externe mais également par le responsable de sécurité.

#### *Enregistrement d'un nouveau RCCS sans MC pour un certificat déjà émis*

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

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

- Un mandat daté de moins de trois mois, désignant le futur RCCS comme étant habilité à être le nouveau RCCS pour le serveur informatique auquel le certificat a été délivré, en remplacement de l'ancien RCCS. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RCCS ;
- 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.
- La photocopie d'une pièce d'identité officielle (comportant une photo d'identité) en cours de validité au moment de l'enregistrement du futur RCCS, 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 ce dernier (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) ;

L'authentification du futur RCCS s'effectue par l'envoi du dossier par courrier postal ou sous



forme dématérialisée (dossier scanné puis transmis par courrier électronique).

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

Les opérateurs d'AE et d'AED sont sensibilisés sur les fraudes qui peuvent intervenir sur la délivrance de documents ou copies de documents officiels (documents falsifiés). Une attention particulière doit être apportée aux contrôles de validité des pièces fournies (date de validité des pièces d'identité, âge des demandes, etc.). Ces aspects sont développés lors de la formation initiale prévue pour les opérateurs d'AE et détaillés dans le plan de formation du personnel de l'IGC Certigna [REF24].

Les audits périodiques doivent prendre en compte des vérifications par échantillonnage des dossiers traités, afin de s'assurer du respect des procédures. Ces audits peuvent être menés par le cabinet d'audit externe mais également par le responsable de sécurité.

#### *Enregistrement du mandataire de certification (MC)*

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

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

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

- Une demande écrite signée, datée de moins de 3 mois, par un représentant légal de l'entité ;
- Un mandat signé, daté de moins de 3 mois, par un représentant légal de l'entreprise désignant le mandataire. Ce mandat est également signé par le mandataire de certification pour acceptation ;
- Un engagement signé, daté de moins de 3 mois, du mandataire de certification à :
  - Effectuer de façon impartiale et scrupuleuse les contrôles d'identité des futurs RCCS 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 , qui doit être référencée par l'ANTS (au titre de « participant ». :

#### *Pour une entreprise :*

- Tout document attestant de la qualité du représentant légal (par exemple, un exemplaire des statuts de l'entreprise, en cours de validité, portant signature de ses représentants) ;
- Toute pièce, valide au moment de l'enregistrement, portant le numéro SIREN de l'entreprise (extrait KBIS ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements) ou, à défaut, une autre pièce valide attestant l'identification unique de l'entreprise qui figurera dans le certificat.

#### *Pour une administration :*

- Une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative.



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

L'authentification du mandataire est réalisée lors d'un face à face physique. Lors de ce face-à-face, un certificat de même niveau ou supérieur peut être remis au mandataire. Ce certificat permettra de transmettre sous forme dématérialisée les dossiers de demande de certificat ou les demandes de révocation. Si le mandataire n'est pas équipé d'un certificat de même niveau ou supérieur, les dossiers ne pourront être envoyés sous forme dématérialisée. Dans ce cas, chaque dossier ne sera validé qu'après réception des documents originaux par courrier.

Les opérateurs d'AE et d'AED sont sensibilisés sur les fraudes qui peuvent intervenir sur la délivrance de documents ou copies de documents officiels (documents falsifiés). Une attention particulière doit être apportée aux contrôles de validité des pièces fournies (date de validité des pièces d'identité, âge des demandes, etc.). Ces aspects sont développés lors de la formation initiale prévue pour les opérateurs d'AE et détaillés dans le plan de formation du personnel de l'IGC Certigna [REF24].

Les audits périodiques doivent prendre en compte des vérifications par échantillonnage des dossiers traités, afin de s'assurer du respect des procédures. Ces audits peuvent être menés par le cabinet d'audit externe mais également par le responsable de sécurité.

#### *Enregistrement d'un RCCS via un MC*

L'enregistrement d'un RCCS via un MC nécessite la validation par le MC de l'identité "personne physique" du futur RCCS 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 RCCS et comportant l'identité et la fonction du serveur concerné par cette demande ;
- Un mandat daté de moins de trois mois, désignant le futur RCCS comme étant habilité à être RCCS 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 RCCS.
- La photocopie d'une pièce d'identité officielle (comportant une photo d'identité) en cours de validité au moment de l'enregistrement du futur RCCS, certifiée conforme par le MC (date, de moins de 3 mois, et signature précédées de la mention "copie certifiée conforme à l'original"). Cette photocopie est également signée par le RCCS ;
- L'acceptation des termes et conditions (conditions générales d'utilisation) ;
- Pour les certificats utilisés sur les justificatifs de domicile : l'avis de participation attestant que la personne morale, porteuse du certificat, fait partie la liste des participants du dispositif 2D-doc autorisés par le Ministère de l'intérieur.

Le dossier est envoyé par courrier à l'AE pour conservation, et éventuellement sous forme électronique signée avec le certificat du MC.

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

Les MC doivent être sensibilisés au même titre que les opérateurs d'AE sur les fraudes qui peuvent intervenir sur la délivrance de documents ou copies de documents officiels (documents falsifiés). Une attention particulière doit être apportée aux contrôles de validité des pièces fournies (date de validité des pièces d'identité, âge des demandes, etc.). Ces aspects sont développés lors de la formation initiale prévue pour les MC opérant pour l'entité à laquelle ils appartiennent.

Les audits périodiques doivent prendre en compte des vérifications par échantillonnage des dossiers traités, afin de s'assurer du respect des procédures. Ces audits peuvent être menés par le cabinet d'audit externe mais également par le responsable de sécurité.

#### *Enregistrement d'un nouveau RCCS via un MC pour un certificat déjà émis*

En cas de changement de RCCS pour un certificat serveur en cours de validité, le nouveau RCCS doit faire l'objet d'une procédure d'enregistrement en remplacement de l'ancien RCCS. 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 RCCS, 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 RCCS comme étant habilité à être le nouveau RCCS pour le serveur informatique auquel le certificat doit être délivré, en remplacement de l'ancien RCCS. Ce mandat doit être signé par le MC et co-signé, pour acceptation, par le futur RCCS.

Le dossier est envoyé par courrier à l'AE pour conservation, et éventuellement sous forme électronique signée avec le certificat du MC.

#### **3.2.4. Informations non vérifiées du RCCS et du service applicatif**

Sans objet.

#### **3.2.5. Validation de l'autorité du demandeur**

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

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

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

Le logiciel OpenCA dispose de la capacité à détecter une demande de certificat avec une clé publique qui aurait déjà été certifiée.

#### **3.3.1. Identification et validation pour un renouvellement courant**

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

### 3.3.2. Identification et validation pour un renouvellement après révocation

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

### 3.4. Identification et validation d'une demande de révocation

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

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

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 RCCS ;
- L'adresse e-mail du RCCS ;
- L'identité et la fonction du serveur ;
- La raison de la révocation.

Si le RCCS n'est pas le demandeur :

- Le prénom et le nom du demandeur ;
- La qualité du demandeur (responsable légal, opérateur d'AED, MC);
- Le numéro de téléphone du demandeur.

Le formulaire papier peut également être transmis sous format électronique.

La demande électronique peut être effectuée par une personne habilitée munie d'un certificat de même niveau ou supérieur (un opérateur d'AED ou le cas échéant un MC). La demande sera alors signée électroniquement avec ce certificat de même niveau ou supérieur.

Le traitement de demande de révocation est détaillé dans la procédure opérationnelle de demande de révocation [REF07]. En cas de demande de révocation transmise par courrier, l'opérateur d'AE traitant ces demandes, doit vérifier la signature du demandeur (comparaison de cette signature avec celle présente dans le dossier de demande de certificat) ainsi que son autorité par rapport au certificat à révoquer. En l'occurrence, l'opérateur d'AE doit s'assurer que le signataire de la demande est le RCCS, un représentant légal (nom mentionné, par exemple, dans l'exemplaire des statuts de l'entité transmis avec les demandes de certificat ou dans le dossier d'enregistrement du mandataire de certification), un mandataire de certification (désigné par le dossier d'enregistrement), ou un opérateur d'AED.

Comme pour les demandes de certificats, les audits périodiques pourront prendre en compte des vérifications par échantillonnage des demandes de révocation traitées par l'AE, afin de s'assurer du respect des procédures. Ces audits peuvent être menés par le cabinet d'audit externe mais également par le responsable de sécurité.

## **4. Exigences opérationnelles sur le cycle de vie des certificats**

### **4.1. Demande de certificat**

#### **4.1.1. Origine d'une demande de certificat**

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

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

L'adresse mail du RCCS, et le cas échéant du MC, est enregistrée dans les bases de données de l'AE. Ces adresses sont utilisées pour transmettre les messages de service lors du traitement des demandes de certificat ou de révocation, ou pour des demandes complémentaires effectuées par les opérateurs d'AE traitant ces demandes.

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

### **4.2. Traitement d'une demande de certificat**

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

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

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

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

**REMARQUE :** Lors de la saisie du formulaire en ligne, le processus de demande de certificat impose de valider explicitement la prise de connaissance et l'acceptation des conditions générales d'utilisation.

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

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

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

#### **4.2.2. Acceptation ou rejet de la demande**

La demande de certificat s'effectue, pour rappel, en deux étapes distinctes :

- L'envoi de la demande électronique (CSR) ;
- L'acquisition de la demande (réception du dossier papier de demande signé ou éventuellement de sa version dématérialisée).

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

La justification d'un éventuel refus est effectuée par l'AE en précisant la cause :

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

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

#### **4.2.3. Durée d'établissement du certificat**

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

### **4.3. Délivrance du certificat**

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

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

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).

Les opérations de validation de demande sur l'AE et de génération de certificat sur l'AC sont détaillées dans la procédure opérationnelle de demande de certificat [REF04].

Les échanges entre l'AE et l'AC sont effectués de manière sécurisée, de l'AE vers l'AC par signature avec le certificat d'opérateur AE.

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

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

Le traitement des accusés de réception est décrit dans la procédure opérationnelle de demande de certificat [REF04].

### **4.4. Acceptation du certificat**

#### **4.4.1. Démarche d'acceptation du certificat**

L'acceptation peut être réalisée de deux façons.

Soit lors de l'installation du certificat le RCCS choisit d'accepter ou non le certificat depuis son espace client. La notification d'acceptation ou de refus est transmise automatiquement à l'AC.

Soit le RCCS notifie l'acceptation ou non du certificat en complétant un formulaire papier qui sera envoyé par courrier ou remis lors d'un face à face.

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

#### **4.4.2. Publication du certificat**

Tous les certificats émis par l'AC Certigna FR03 sont publiés dans un annuaire après l'acceptation du certificat par le RCCS. Le RCCS est informé de cette publication.

#### **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 RCCS.

## 4.5. Usages de la bi-clé et du certificat

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

L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service de cachet de données émises par le serveur (cf chapitre 1.4.1.). Les RCCS 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.

Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du RCCS 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 par le RCCS 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 RCCS 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 RCCS 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 RCCS s'engage, en acceptant les Conditions Générales d'Utilisation, à générer un nouveau bi-clé à chaque demande.

Le logiciel IGC mis en oeuvre dispose de la capacité à détecter une demande de certificat avec une clé publique qui aurait déjà été certifiée. Toute demande de certification d'une clé publique ayant déjà fait l'objet d'une signature se solde par un échec avec un message explicite au niveau du module de gestion des demandes de certificats de l'AE.

Ce contrôle sous-entend qu'il existe une base intègre des certificats émis depuis la mise en place de l'AC. Les sauvegardes en temps réel de NetApp (fonction SnapMirror Sync) permettent de garantir l'intégrité de cette base en cas de bascule sur le site de secours ou de restauration du site principal.

En cas de défaillance de la fonction SnapMirror Sync, une procédure manuelle de secours est prévue dans la procédure opérationnelle de sauvegarde [REF44].

Cette procédure consiste en :

- La sauvegarde des bases sur le site en exploitation ;
- La réplication manuelle sur le second site (copie complète de la base) après rétablissement de la fonction SnapMirror Sync.



## 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 moins tous les trois ans (cf. période de validité chapitre 6.3.2).

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

### 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 RCCS (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 service applicatif qui lui est rattaché.

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

## 4.8. Modification du certificat

La modification de certificats de l'autorité FR03 n'est pas autorisée. En cas de nécessité de changement d'informations présentes dans le certificat (principalement le DN), un nouveau certificat doit être délivré après révocation de l'ancien.

## 4.9. Révocation et suspension des certificats

### 4.9.1. Causes possibles d'une révocation

#### *Certificats de cachet serveur*

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

- 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 de l'identité ou de la fonction du serveur), ceci avant l'expiration normale du certificat ;
- Le RCCS n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le RCCS, l'entité, le cas échéant le MC ou l'opérateur d'AED, n'a pas respecté ses obligations découlant de la PC;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- La clé privée du serveur est suspectée de compromission, est compromise, est perdue ou volée (ou éventuellement les données d'activation associées à la clé privée) ;
- Le RCCS, le représentant légal de l'entité à laquelle il appartient, le cas échéant le MC, ou l'opérateur d'AED demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du serveur et/ou de son support) ;



- L'arrêt définitif du serveur ou la cessation d'activité de l'entité du RCCS de rattachement du serveur ;
- Le certificat de signature de l'AC FR03 est révoqué (ce qui entraîne la révocation de tous les certificats en cours de validité signés par la clé privée correspondante) ;
- Pour des raisons techniques (échec de l'envoi du certificat, . . . ).

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

#### *Certificats d'une composante de l'IGC*

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

- Suspicion de compromission, compromission, perte ou vol de la clé privée ;
- 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 cachet serveur*

Les personnes ou entités qui peuvent demander la révocation d'un certificat de cachet serveur sont les suivantes :

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

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

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

Pour une demande effectuée depuis l'espace client, l'utilisateur s'authentifie avec son compte client et sélectionne le certificat à révoquer.

Pour une demande par courrier, les informations suivantes doivent figurer dans la demande de révocation de certificat (formulaire à télécharger sur le site internet) :

- L'identité du RCCS ;
- L'adresse mail du RCCS ;
- L'identité et la fonction du serveur ;
- La raison de la révocation ;

Si le RCCS n'est pas le demandeur :

- Le prénom et le nom du demandeur ;
- La qualité du demandeur (responsable légal, le cas échéant opérateur d'AED ou 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 (Authentification avec son compte utilisateur). En l'occurrence la personne à l'origine de la demande peut être :

- Le porteur lui-même ;
- Le cas échéant un MC;
- Un opérateur d'AED ;
- Le responsable légal de l'entité.

Les étapes sont les suivantes :

- Le demandeur de la révocation transmet sa demande à l'AE, par courrier ou en ligne ;
- L'AE authentifie et valide la demande de révocation selon les exigences décrites au chapitre 3.4 ;
- Le numéro de série du certificat est inscrit dans la LCR;
- Dans tous les cas, le RCCS 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.

Le mécanisme de révocation est décrit dans la procédure opérationnelle de demande de révocation [REF07].

### *Certificats d'une composante de l'IGC*

Dans le cas où l'AC Certigna Root CA décide de révoquer le certificat d'AC intermédiaire FR03 (suite à la compromission de la clé privée de l'AC FR03 ou de l'AC Certigna Root CA), cette dernière informe par e-mail l'ensemble des RCCS que leurs certificats ne sont plus valides car l'un des certificats de la chaîne de certification n'est plus valide. Cette information sera relayée également directement auprès des entités et le cas échéant de leur MC.

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

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

La procédure est détaillée dans la procédure opérationnelle de gestion des clés cryptographiques d'AC [REF39] et dans la procédure opérationnelle de gestion des certificats de composante [REF48].

#### **4.9.4. Délai accordé au RCCS pour formuler la demande de révocation**

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

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

##### *Certificats de cachet 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 est de 72 heures. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

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

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

Le personnel Certigna responsable de la maintenance s'engage à appliquer le PCA en respectant notamment les procédures décrites suite à un incident ou sinistre.

##### *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.

L'organisation et les moyens mis en oeuvre en cas de révocation d'un certificat d'une composante de l'IGC sont décrits dans la procédure opérationnelle de gestion des clés cryptographiques d'AC [REF39] et dans la procédure opérationnelle de gestion des certificats de composante [REF48].

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

L'utilisateur d'un certificat serveur de l'autorité FR03 est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée (LCR ou OCSP) est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.

#### **4.9.7. Fréquence d'établissement des LCR**

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

#### **4.9.8. Délai maximum de publication d'une LCR**

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

#### **4.9.9. Exigences sur la vérification en ligne de la révocation et de l'état des certificats**

L'AC Certigna FR03 dispose d'un répondeur OCSP disponible aux adresses suivantes : <http://2ddoc.ocsp.certigna.fr> et <http://2ddoc.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 la PC.

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

#### **4.9.10. Autres moyens disponibles d'information sur les révocations**

Sans objet

#### **4.9.11. Exigences spécifiques en cas de compromission de la clé privée**

Les RCCS 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 RCCS 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 l'acceptation des CGU.

Les dispositions prises sont explicitées dans la procédure opérationnelle de gestion des clés cryptographiques d'AC [REF39] et la procédure opérationnelle de gestion des certificats de composante [REF48].

#### **4.9.12. Suspension de certificat**

Les certificats émis par l'AC Certigna FR03 ne peuvent pas être suspendus.

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

#### **4.10.1. Caractéristiques opérationnelles**

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

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

La publication de ces informations est décrite dans la procédure opérationnelle de publication [REF09].

#### **4.10.2. Disponibilité de la fonction**

La fonction d'information sur l'état des certificats est disponible 24 heures sur 24, 7 jours sur 7. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4 heures (jours ouvrés) et une durée maximale totale d'indisponibilité par mois de 32 heures (jours ouvrés).

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

Le personnel Certigna responsable de la maintenance s'engage à appliquer le PCA en respectant notamment les procédures décrites suite à une détection d'incident par le moniteur de supervision. Si besoin est, le site secondaire doit prendre le relais du site principal dans le délai le plus bref possible. Dhimyotis peut éventuellement s'appuyer sur les astreintes mises en place pour les autres AC de niveau d'exigence supérieure (c'est-à-dire \*\*\*) pour les périodes non ouvrées, en sachant toutefois qu'une disponibilité pour ces périodes n'est pas requise par la PC.

#### **4.11. Fin de la relation entre le RCCS et l'AC**

En cas de fin de relation contractuelle ou réglementaire entre l'AC Certigna FR03 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.

#### **4.12. Séquestre de clé et recouvrement**

Le séquestre des clés privées est interdit.

## **5. Mesures de sécurité non techniques**

RAPPEL - L'AC a mené une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en oeuvre. 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**

L'AC est hébergée sur deux sites distincts redondants :

- Un site principal sécurisé, situé chez CIV : ce site abrite les composants de l'IGC nécessaires à son exploitation (gestion des demandes de certificats/révocations, génération des certificats/LCR, serveur de publication) ;
- Un site secondaire sécurisé, situé chez IBM : ce site est la réplique du site principal ;

Une réplique des données (base de données IGC, LCR) est effectuée entre les deux sites. Une consolidation des logs est effectuée sur les deux sites.

En cas de défaillance d'un composant du site principal, une alerte est envoyée par le superviseur aux responsables d'exploitation. Ces derniers sont de plus à même de détecter en temps réel les incidents grâce à l'interface de supervision (défaillance d'un serveur ou d'un équipement de télécommunication, processus arrêté). Suivant la gravité de l'incident un basculement sur le site secondaire peut être déclenché (le site secondaire devient site principal jusqu'à la remise en route du site concerné par l'incident). Les deux sites sont connectés à Internet au travers de liens xDSL. La liaison inter-site est effectuée par VPN IPSec (authentification des pairs par certificat numérique).

#### **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 oeuvre 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.

Plus particulièrement, les aménagements suivants ont été effectués :

- Sur le site principal CIV :

- Mise en place d'un espace grillagé hébergeant l'infrastructure informatique protégeant l'exploitation des serveurs et équipements hébergés (un périphérique clavier-écran est intégré dans la baie) ;
- Local hébergeant la baie protégé par un contrôle d'accès physique avec journalisation des accès ;
- Locaux de CIV protégés par une alarme (détecteur d'ouverture et détecteur volumétrique) ;
- Vidéo-surveillance de l'accès principal.

- Sur le site de secours (IBM) :

- Mise en place d'un espace grillagé hébergeant l'infrastructure informatique protégeant l'exploitation des serveurs et équipements hébergés (un périphérique clavier-écran est intégré dans la baie) ;
- Local hébergeant la baie protégé par un contrôle d'accès physique avec journalisation des accès ;
- Vidéo surveillance de l'espace grillagé ;
- Local hébergeant la baie situé dans un périmètre protégé par un contrôle d'accès physique avec journalisation des accès ;
- Locaux d'IBM protégés par une alarme (détecteur d'ouverture et détecteur volumétrique).

Sur le site principal, les prestataires de Dhimyotis intervenant notamment pour des opérations de maintenance dans la salle sécurisée sont surveillés durant le temps de leur intervention grâce à la caméra IP. Cet aménagement évite un déplacement sur site du personnel habilité et permettent une intervention immédiate en cas d'urgence.

Les modalités d'intervention des sociétés CIV et IBM dans les locaux loués à Dhimyotis font l'objet d'un document remis à CIV et IBM [REF60]. Il définit entre autres les personnes habilitées à entrer dans les locaux ainsi que les conditions d'accès.

### **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.

Le site principal est équipé de :

- Un onduleur ;
- Un système de climatisation.

Le site de secours est équipé de :

- Un onduleur ;
- Un système de climatisation.

### **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.

Le site principal est équipé de :

- Un système de détection d'incendie ;
- Un système d'extinction d'incendie.



Le site de secours est équipé de :

- Un système de détection d'incendie ;
- Un système d'extinction d'incendie.

Le PCA décrit les procédures à suivre en cas de sinistre de type incendie afin d'assurer la continuité de service en cohérence avec les garanties de disponibilité décrites dans la PC et la DPC.

### **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.

Les informations sur supports papier (dossiers envoyés par les clients) sont conservées dans les locaux de Dhimyotis dans des armoires fermées à clé.

L'analyse de risque, mise à jour régulièrement, met en évidence la nécessité de sauvegarder les informations nécessitant un haut degré de disponibilité. Cette haute disponibilité est offerte par le mirroring mis en place avec les serveurs de sauvegarde NetApp (et utilitaire SnapMirror) ainsi que par les procédures de sauvegarde (robot et logiciel de sauvegarde sur cartouche LTO).

### **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.

En fin de vie, les supports électronique et papier intervenant dans les processus d'exploitation de l'IGC sont détruits physiquement : effacement sécurisé multi-passes pour les supports électroniques réinscriptibles, utilisation du broyeur de documents, de CD-ROM et de cartes. Ces mécanismes sont décrits dans la procédure opérationnelle de fin de vie des supports de données [REF63].

En cas de dysfonctionnement irréversible du boîtier cryptographique empêchant un effacement logique des clés privées (pour permettre un envoi à la maintenance), il est prévu de détruire physiquement la carte PCI (carte supportant le module abritant les clés privées). Cette destruction est effectuée mécaniquement (broyage de la carte) et chimiquement (trempage dans un bain d'acide).

La procédure de destruction de CryptoBox [REF34] s'effectue en présence de plusieurs témoins et fait l'objet d'un procès verbal.

### **5.1.8. Sauvegardes hors site**

L'IGC met en oeuvre 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.



Le mirroring (fonction SnapMirror du NetApp) est effectué au travers d'un tunnel VPN IPSec chiffré garantissant l'intégrité et la confidentialité des données échangées.

La liaison inter-site est doublée (2+1 liens Internet loués auprès de deux fournisseurs d'accès distincts) et garantit une disponibilité de la fonction de mirroring. Deux tunnels sont en effet configurés au niveau des firewalls (2 combinaisons possibles de liaison) avec une route définie prioritairement (correspondant à la liaison via les lignes SDSL). Cette route est également configurée pour qu'après utilisation d'une route secondaire (suite à indisponibilité de la route prioritaire) il y ait repli sur la route prioritaire dès détection de sa disponibilité.

Une supervision des différentes liaisons internet (via le logiciel Nagios) est effectuée afin de s'assurer à tout moment de la disponibilité d'une route secondaire.

## 5.2. Mesures de sécurité procédurales

### 5.2.1. Rôles de confiance

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

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

**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 propres à chaque entité opérant une des composantes de l'IGC sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles déterminent la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilisation des employés.

Ces rôles sont décrits précisément dans des fiches de profil. Des habilitations sont mises en correspondance avec ces profils et sont détaillées dans le descriptif des profils d'accès physique et logique [REF29].

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

### **5.2.2. Nombre de personnes requises par tâche**

Pour des raisons de disponibilité, chaque tâche doit pouvoir être effectuée par au moins deux personnes.

Au minimum, chacune des tâches suivantes est affectée sur deux personnes distinctes :

- Administrateur système ;
- Opérateur.

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

#### **Cérémonie de clés**

Lors de la cérémonie de clés (génération des clés de l'AC), les personnes suivantes sont requises :

- au moins une personne ayant un rôle de confiance au sein de l'IGC pour assurer le contrôle de la cérémonie ;
- plusieurs témoins.

Concrètement, il y a présence des porteurs de secrets (5 au total) à qui sont remises les parts de secret après partage de Shamir. Parmi ces cinq personnes, une au moins dispose d'un rôle de confiance au sein de l'IGC.

Un procès-verbal est rédigé à l'issue de cette procédure et signé par l'ensemble des participants.

#### **Opérateurs de composant**

Pour des questions de disponibilités deux personnes au minimum sont désignées au sein de chaque composante de l'IGC, soit l'AE et l'AC :

- AE : au minimum deux opérateurs assurent les tâches d'enregistrement ;
- AC : le responsable de sécurité est responsable de la génération/révocation des certificats et délègue ses pouvoirs au minimum à deux opérateurs d'AE.

### **5.2.3. Identification et authentification pour chaque rôle**

Chaque attribution de rôle à un membre du personnel de l'IGC est notifiée par écrit. Ce rôle est clairement mentionné et décrit dans sa fiche de poste. Il est accepté explicitement par la personne concernée. L'AC Certigna FR03 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.).

Les rôles de chaque membre de l'IGC sont listés dans un document interne [REF13].

L'employé accepte explicitement les rôles au sein de l'IGC qui sont repris dans la charte de sécurité qu'il doit signer à son entrée dans l'entreprise et de façon périodique (tous les ans).

Ces processus sont décrits dans la procédure de traitement de l'arrivée, départ ou changement de rôle d'un employé [REF58].

Schématiquement, les actions décrites sont les suivantes :

- Vérification des antécédents (fourniture copie bulletin n°3 casier judiciaire par l'employé) ;
- Signature de la charte de sécurité ;
- Attribution des droits d'accès physiques ;
- Attribution des droits d'accès logiques ;
- Emission de certificat(s) nécessaire(s) à l'exécution de son rôle dans l'IGC ;
- Optionnellement attribution de rôle de porteur de secret.

Les acteurs concernés par cette procédure sont :

- L'officier de sécurité ;
- L'administrateur système du réseau d'entreprise ;
- Le gestionnaire du système de contrôle d'accès physique (Mifare) ;
- L'administrateur système de l'IGC.

Des contrôles des procès verbaux d'attribution/restitution des éléments sensibles nécessaires à l'exécution du rôle de l'employé au sein de l'IGC sont effectués lors des audits périodiques effectués par le cabinet externe. Ces documents sont détenus par le responsable de la sécurité.

#### **5.2.4. Rôle exigeant une séparation des attributions**

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

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

Des mesures sont mises en place pour contrôler qu'il n'y a aucun cumul non autorisé de rôles de confiance :

- audit réguliers des journaux pour identification des acteurs des opérations sensibles.

Ces audits sont réalisés par un cabinet d'audit externe afin de s'assurer de l'impartialité des contrôles et sont intégrés par conséquent dans le programme d'audit de ce dernier (cf. 8. Audit de conformité et autres évaluations).

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

#### **5.3.1. Qualifications, compétences et habilitations requises**

Toutes les personnes amenées à travailler au sein de composantes de l'IGC doivent signer la charte de sécurité interne. Cette charte comporte notamment une clause de confidentialité qui s'applique tant à l'égard des tiers que des utilisateurs. Elle liste les rôles de chaque employé au sein de l'IGC. Elle est co-signée par l'employé et le responsable de sécurité. L'adéquation des compétences des personnels intervenant dans l'IGC est vérifiée par rapport à ses attributions sur les composantes de cette dernière.

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

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

La signature de la charte de sécurité par chaque employé de l'IGC est intégrée dans la procédure d'entrée (cf. 5.2.3. Identification et authentification pour chaque rôle).

Une sensibilisation du personnel est effectuée sur la sécurisation de la mise en oeuvre des composantes de l'IGC. Le responsable de sécurité est garant de la diffusion de ces informations auprès du personnel de l'IGC. Lors de toute évolution de l'IGC impliquant une modification des règles ou procédures de sécurité applicables, un relais d'information est effectué par le responsable de sécurité vers les membres de l'IGC (note d'information, formation, etc.).

Les personnes assurant des rôles sensibles et stratégiques au sein de l'IGC disposent d'expertise reconnue dans les technologies des certificats numériques. La perception et la connaissance des règles de sécurité sont régulièrement évaluées au sein du personnel de l'IGC. Elles le sont au cours des audits périodiques effectués par le cabinet externe et sont intégrés par conséquent dans le programme d'audit de ce dernier (cf. 8. Audit de conformité et autres évaluations).

Les intervenants de ce cabinet d'audit disposent des compétences dans le domaine du management de la sécurité de l'information et à ce titre peuvent effectuer des interventions ponctuelles pour former et/ou assister les personnes concernées par les problèmes de sécurité au sein de l'IGC. Ces prestations sont proposées à l'initiative du cabinet d'audit à l'issue de ses audits périodiques.

### **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.

Un plan de formation est défini pour tout le personnel opérant au sein de l'IGC :

- Formation initiale pour tout nouvel employé. Cette formation couvre entre autres les aspects suivants :

- Principes de cryptographie ;
- La cryptographie à clé publique (algorithmes asymétriques) ;
- Application aux certificats numériques ;
- Les IGC (architectures, composants, fonctionnement) ;
- Autres services (séquestre, horodatage, OCSP, serveur de publication) ;
- Présentation technique de l'IGC Certigna (logiciel OpenCA).

- Formation personnalisée présentant les procédures à mettre en oeuvre dans le cadre de l'exploitation de la (des) composante(s) de l'IGC :

- Certifications ETSI TS 102042 et RGS des AC;
- Politique de Certification et Déclaration des Pratiques de Certification associées ;

- Présentation du référentiel documentaire décrivant les procédures mises en place dans le cadre des différentes DPC;

- Notion de disponibilité : présentation du plan de secours, du plan de continuité d'activité ;

- Préparation aux tests du plan de continuité d'activité ;

- Présentation du programme d'audit annuel : rôle des différents acteurs.

L'enregistrement d'opérateurs d'AE déléguée et éventuellement de mandataires de certification au sein de l'IGC Certigna peut également donner lieu à une formation concernant leur rôle au sein de l'IGC Certigna.

Les aspects liés à la communication interne et à la formation sont abordés au cours des comités de direction/sécurité mensuels et font partie à ce titre de l'ordre du jour traité lors de ces réunions (point récurrent).

Le contenu des formations internes est décrit dans le plan de formation du personnel [REF24].

En cas d'évolution notoire dans l'IGC (sur le plan organisationnel ou technique) le comité de direction décide de la nécessité et/ou de la pertinence de communiquer au sein du personnel de l'IGC les informations liées à l'exploitation de l'IGC et le cas échéant de la formation à mettre en place préalablement à cette exploitation.

### **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 FR03 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.

L'intervention d'un externe (prestataire ou stagiaire) au sein de l'IGC Certigna doit suivre la procédure de traitement de l'arrivée, départ ou changement de rôle d'un externe [REF59].

Schématiquement, les actions qui sont listées sont les suivantes :

- Signature de la charte de sécurité ;
- Attribution des droits d'accès physiques ;
- Attribution des droits d'accès logique ;
- Attribution de biens sensibles.

Les acteurs concernés par cette procédure sont :

- L'officier de sécurité ;
- L'administrateur système du réseau d'entreprise.

Des contrôles des procès verbaux d'attribution/restitution des éléments sensibles nécessaires à l'exécution de la prestation de la personne externe au sein de l'IGC sont effectués lors des audits périodiques effectués par le cabinet externe. Ces documents sont détenus par le responsable de la sécurité.

### 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 oeuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, l'AC lui remet les politiques de sécurité l'impactant.

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

Les procédures de référence pour les opérateurs des composantes de l'IGC sont les suivants :

- La procédure opérationnelle de demande de certificat [REF04] ;
- La procédure opérationnelle de demande de révocation [REF07] ;
- La politique de gestion des mots de passe [REF55] ;
- La procédure opérationnelle d'enregistrement des MC [REF08] ;
- La procédure opérationnelle d'enregistrement des opérateurs d'AED [REF62] ;
- La procédure opérationnelle de publication [REF09] ;
- La procédure opérationnelle d'archivage [REF10] ;

auxquels s'ajoutent les documents de politique de sécurité :

- La politique de sûreté [REF42] ;
- La politique de classification et de manipulation des informations [REF30].

## 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.

On distingue trois familles d'événements :

- Les événements concernant les modifications de la plate-forme technique : ces événements sont consignés dans la main courante (données manuscrites). Les conditions de mise à jour de la plate-forme sont décrites dans la procédure opérationnelle de mise à jour de la plate-forme technique [REF21].
- Les incidents d'exploitation de l'IGC : ces incidents sont enregistrés sous forme de fiches. Ces fiches comportent différentes rubriques (prise en compte, traitement, etc.) qui sont complétées par les administrateurs systèmes prenant en charge leur résolution ;
- Les événements d'exploitation de l'IGC : ces événements sont enregistrés par les différents composants/systèmes dans des fichiers de trace (données électroniques).

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

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

- Événements liés aux clés de signature et aux certificats d'AC ou aux données d'activation (génération, sauvegarde et récupération, révocation, destruction, destruction des supports,...) ;
- Réception d'une demande de certificat (initiale et renouvellement) ;
- Validation / rejet d'une demande de certificat ;
- Génération des certificats des serveurs ;
- Transmission des certificats aux RCCS et, selon les cas, acceptations / rejets explicites par les RCCS ;



- Publication et mise à jour des informations liées à l'AC (PC/DPC, certificats d'AC, CGU, etc.)
- Réception d'une demande de révocation ;
- Validation / rejet d'une demande de révocation ;
- Génération puis publication des LCR;
- Destruction des supports contenant des renseignements personnels sur les porteurs.

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.

Les cas exceptionnels d'écriture différée concernent l'inscription dans la main courante d'une mise à jour de la configuration de l'IGC non planifiée correspondant par exemple à l'application de patch de sécurité pour assurer l'intégrité et la disponibilité de cette dernière (détection d'une faille de sécurité).

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

- Le type d'événement ;
- La date et heure de l'événement (l'heure exacte des événements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat est enregistrée) ;
- Le nom de l'exécutant ou la référence du système ayant déclenché l'événement (pour imputabilité) ;
- Le résultat de l'événement (réussite ou échec).

En fonction du type d'événement, on trouve également les champs suivants :

- Le destinataire de l'opération ;
- Le nom du demandeur de l'opération ou la référence du système ayant effectué la demande ;
- Le nom des personnes présentes (pour les opérations nécessitant plusieurs personnes);
- La cause de l'événement ;
- Toute information caractérisant l'événement (par exemple : n° de série du certificat émis ou révoqué).

#### **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 FR03 sont autorisés à traiter ces fichiers.

L'accès en écriture à ces fichiers est protégé (gestion des droits). Les journaux sont sur les machines de l'IGC dont l'accès nécessite une authentification logique. Les machines sont situées dans des salles sécurisées (site principal et site secondaire) dont l'accès est contrôlé physiquement (de type Mifare).



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.

Une consolidation des journaux d'événements (du site principal et du site secondaire) est effectuée sur les deux sites par le processus de mirroring du NetApp (SnapMirror). Cette sauvegarde est réalisée à intervalle régulier (une fois par jour).

#### **5.4.6. Système de collecte des journaux d'événements**

Les journaux d'événements sont stockés sur le NetApp (qtree dédié pour chaque site). La consolidation obtenue est accessible par le personnel Certigna en local (site secondaire) ou à distance (site principal au travers du VPN établi entre les deux sites). La protection de la confidentialité et de l'intégrité des journaux d'événements est assurée par le contrôle d'accès logique (restriction d'accès aux membres de l'AC FR03) ainsi que par l'utilisation de la compression (fichiers tar.gz).

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

Sans objet.

#### **5.4.8. Evaluation des vulnérabilités**

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

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

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

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

Le programme d'audit annuel (cabinet d'audit externe) intègre la vérification des contrôles des journaux d'événements avec notamment relecture sur échantillonnage. Les contrôles des journaux d'événements sont enregistrés dans une main courante, facilitant ainsi le rôle de l'auditeur externe.

## 5.5. Archivage des données

### 5.5.1. Types de données à archiver

L'AC archive :

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

### 5.5.2. Période de conservation des archives

#### *Dossiers de demande de certificat*

Tout dossier de demande de certificat accepté est archivé aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable, en particulier à l'article 6-II du décret d'application n°2001-272 du 30 mars 2001. En l'occurrence, il est archivé pendant au moins sept ans, comptés au maximum à partir de l'acceptation du certificat par le RCCS. 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 RCCS responsable à un instant "t" du serveur désigné dans le certificat émis par l'AC dans le certificat émis par l'AC.

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

Les certificats de clés de serveurs et d'AC, ainsi que les LCR / LAR produites (respectivement par l'AC Certigna FR03 et AC Certigna Root CA), sont archivés pendant au moins cinq ans après leur expiration.

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

#### *Journaux d'événements*

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

Les archives listées sont conservées en double exemplaire (exceptées les dossiers papier de demande de certificat) grâce au processus de mirroring entre les deux sites, ce qui assure la protection et la disponibilité des informations. Les archives sont stockées dans des répertoires indiquant de manière explicite la date de sauvegarde. Les archives électroniques sont effacées (processus périodique) une fois leur période de conservation passée. Les dossiers de demande papier sont physiquement détruits (utilisation du broyeur de document). Au-delà des 11 premières années d'exploitation de l'AC FR03, une procédure manuelle annuelle d'effacement des archives est exécutée : effacement des archives de la première année d'exploitation au bout de 11 années d'exploitation, puis effacement des archives de la seconde année l'année suivante, etc. L'effacement concerne tous les types d'archives (certificats et LCR/LAR émises par l'AC, journaux d'événements). La durée minimale de conservation est respectée (5 ans + durée maximale de validité des certificats des particuliers, 5 ans = 10 ans). Cette procédure est effectuée sur les deux sites (sur chaque serveur NetApp).

### **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 FR03. 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.

Le mirroring est effectué avec l'outil SnapMirror de NetApp. Pour pallier l'impossibilité de mirroring entre les deux sites (indisponibilité du second site par exemple), des sauvegardes quotidiennes sur cartouche sont réalisées afin de garantir l'existence d'une copie des données enregistrées.

### **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 FR03 autorisés à traiter ces fichiers dans un délai maximal de deux jours ouvrés. Les données concernant les contractants peuvent être récupérées à leur demande.

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

### 5.6.1. Clé d'AC

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

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

Dès qu'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.

La gestion du cycle de vie des clés d'AC de l'IGC Certigna est documentée dans [REF51].

### 5.6.2. Clés des autres composantes

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

## 5.7. Reprise suite à compromission et sinistre

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

Ces procédures sont formalisées dans le cadre de la mise en place du PCA (Plan de Continuité d'Activité). En particulier pour les risques majeurs identifiés, ce plan aborde le traitement immédiat dans le cas de contraintes fortes de disponibilité de service exigées par la PC. L'exploitation d'un moniteur de supervision garantit une détection et une prise en compte en temps réel des incidents sur le site principal comme sur le site de secours.

### 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.).

Dans le cas d'un tel événement, l'AC avertit les comités de direction et de sécurité de Certigna.

Un plan de crise est déclenché. Après s'être assuré que l'incident est réel, le comité de direction pilote et coordonne les actions à effectuer, soit par ordre prioritaire :

- Révoquer immédiatement le certificat d'AC, générer la liste de révocation sur l'AC Certigna Root CA et la publier (adresses spécifiées dans le chapitre 2.1) ;
- Diffuser l'information auprès des RCCS responsables de certificats en cours de validité : envoi d'un e-mail aux adresses fournies dans les dossiers de demandes de certificat ;
- Relayer l'information sur le site de Certigna ;
- Informer directement et sans délai le point de contact identifié sur le site :

<https://www.references.gouv.fr> ;

- Analyser l'origine de l'incident et déterminer le cas échéant l'action corrective : en particulier, il est nécessaire de déterminer si l'incident est dû à une erreur humaine, un manquement aux procédures sécuritaires en vigueur, un acte de malveillance interne ou externe, etc. Cet aspect est pris en charge par le comité de sécurité ;

- Mettre en place une organisation spécifique et planifier des renouvellements de certificats rendus invalides par la révocation du certificat d'AC..

La compromission d'une clé d'AC étant considérée comme un sinistre majeur, sa résolution est logiquement décrite dans le Plan de Continuité d'Activité. Dans tous les cas d'incident, une fiche d'incident général doit être remplie en utilisant le formulaire de déclaration type. Cette fiche est ensuite remise au responsable sécurité qui après analyse de l'origine créera la fiche d'incident et de suivi ad-hoc. Cette procédure est décrite dans la procédure opérationnelle de gestion des incidents [REF35].

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 RCCS 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.

Schématiquement, une évaluation de la gravité de l'incident permet de déterminer si l'état initial de la composante peut être restauré ou non dans un délai compatible avec les exigences de disponibilité exprimées dans la présente DPC. Le cas échéant (délai non compatible avec les exigences), une bascule sur le site secondaire est effectuée. Cette procédure est amplement détaillée dans le PCA.

### **5.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante**

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité d'activité de la composante en tant que sinistre (cf. chapitre 5.7.2). Dans le cas de compromission d'une clé d'AC, le certificat correspondant sera immédiatement révoqué (cf. chapitre 4.9). De même, tous les certificats serveurs en cours de validité émis par cette AC seront révoqués. En outre, l'AC respecte au minimum les engagements suivants :

- elle informe les entités suivantes de la compromission : tous les RCCS, MC et les autres entités avec lesquelles l'AC a passé des accords ou a d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autres AC. En complément, cette information est mise à disposition des autres tiers utilisateurs ;
- elle indique notamment que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

Remarque :

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

Ces aspects sont décrits dans la procédure opérationnelle de gestion des clés cryptographiques d'AC [REF39]. Le scénario (sinistre) de compromission de clés privées d'une composante de l'IGC a été intégré dans le plan de continuité de l'IGC (fiche de sinistre/incident n°3) et doit faire, à ce titre, partie du plan de test du PCA.

#### **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.

Le PCA est testé périodiquement (test à blanc et test réel) et dès qu'une modification majeure lui est apportée, notamment suite à une modification de l'architecture ou de la configuration de l'IGC. L'objectif de ces tests est de s'assurer que le PCA répond aux exigences en termes de disponibilité de la PC. L'AC est responsable de l'évolution du PCA en cas de non-conformité par rapport à la PC : elle prend les mesures organisationnelles, techniques ou humaines nécessaires pour assurer cette conformité.

### **5.8. Fin de vie de l'IGC**

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

Le transfert d'activité est défini comme :

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

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

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

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

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

C'est le comité de direction qui pilote le transfert ou la cessation d'activité. Il s'assure à ce titre le suivi et la coordination des différentes tâches listées. Ceci est détaillé dans la procédure de transfert d'activité ou de cessation d'activité [REF03] et la procédure d'arrêt du module cryptographique d'une AC et de l'IGC Certigna [REF06]. Le comité de direction s'assure de la continuité de service des services de publication et de révocation en maintenant en exploitation les composantes concernées sur les deux sites et ce jusqu'au transfert effectif de l'activité (cas du transfert) ou jusqu'à la fin de validité des certificats de serveurs émis (cas de la cessation d'activité).

### *Cessation d'activité affectant l'AC*

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

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

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

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

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

C'est le comité de direction qui pilote la cessation d'activité. Il s'assure à ce titre le suivi et la coordination des différentes tâches listées. Ceci est décrit dans la procédure opérationnelle de transfert ou de cessation d'activité [REF03] et la procédure d'arrêt du module cryptographique d'une AC et de l'IGC Certigna [REF06].



## 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 FR03.

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 conforme au chapitre 10.

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

La cérémonie se déroule suivant un script préalablement défini :

- Elle se déroule sous le contrôle d'au moins une personne ayant un rôle de confiance au sein de l'IGC et en présence de plusieurs témoins ;
- Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

La génération des clés de signature d'AC s'accompagne de la génération de parts de secrets. Les parts de secret d'IGC sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC. Ces secrets sont des parties de la clé privée de l'AC décomposée suivant un schéma à seuil de Shamir (3 parties parmi 5 sont nécessaires pour reconstituer la clé privée).

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

La génération et la restauration des clés d'AC sont décrites dans la procédure de cérémonie de clé [REF16] et la procédure de restauration de clés [REF18]. Elles incluent notamment les différents procès verbaux de conformité de leur déroulement par rapport aux exigences de la PC.

En cas de départ d'un employé porteur de parts de secret, ses parts de secret sont restituées au responsable sécurité qui les transmet à un employé promu porteur de parts. Un nouveau partage peut être effectué en cas de suspicion de fraude (enveloppe contenant la part d'un secret descellée) à l'issue duquel l'ancien partage (l'ensemble des parts) est détruit. Un employé ne peut en aucun cas détenir plusieurs parts d'un même secret. Lors du départ de l'employé, son remplaçant (nouvel arrivant ou employé déjà en place) « hérite » de son coffre de banque. Un transfert de nom est effectué auprès de la banque ayant en charge la gestion des coffres. Une fois attribuées, les parts de secret sont rapidement placées par leurs porteurs dans leurs coffres respectifs.

La(les) cérémonie(s) de clés est(sont) effectuée(s) sur le site de Villeneuve d'Ascq. Les clés sont ensuite reconstituées et injectées dans le boîtier cryptographique du site de CIV à partir des partages obtenus lors de la cérémonie initiale. Le module cryptographique répond aux exigences du chapitre 10. Annexe 1 : exigence de sécurité du module cryptographique de l'AC.

#### *Clés générées par le RCCS*

Le RCCS s'engage à générer la clé privée dans un dispositif de création de cachet conforme aux exigences du chapitre 11.

Le RCCS s'engage de manière contractuelle, en acceptant les conditions générales d'utilisation, à respecter les exigences quant au dispositif qu'il utilise pour générer et stocker sa clé privée, si ce dernier n'est pas fourni par l'AE.

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

#### *Clés générées par l'AC*

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

La génération des clés des porteurs sur un support physique est effectuée dans un environnement sécurisé. Le bi-clé du porteur est généré par l'AE directement dans le dispositif d'authentification et de signature qui lui est destiné. La gestion du support et du code PIN associé sont assurés par deux rôles de confiance de l'AC. Le bi-clé et le code PIN ne sont jamais détenus en même temps par une même personne. Le code PIN est transmis par téléphone (ou en cas d'échec, par mail) au RCCS.

### **6.1.2. Transmission de la clé privée à son propriétaire**

La clé privée est générée par l'AE ou le RCCS et est transmise de manière sécurisée.

Pour un certificat logiciel, la clé privée est protégée par une donnée d'activation transmise au porteur qu'il changera lors de l'acceptation du certificat.

Si la clé privée est générée sur le support physique, l'AE en garantira la confidentialité et l'intégrité jusqu'à la remise du support au RCCS.

### **6.1.3. Transmission de la clé publique à l'AC**

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

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

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

La clé publique de l'AC intermédiaire FR03 est diffusée dans un certificat lui-même signé par l'AC Certigna Root CA. La clé publique de l'AC Certigna Root CA est diffusée dans un certificat auto-signé.

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

#### **6.1.5. Taille des clés**

##### *Clés d'AC*

- AC Certigna Root CA

Le bi-clé d'AC est de type RSA 4096 bits

L'algorithme de hachage est de type SHA-256 (256 bits)

- AC FR03

Le bi-clé d'AC est de type RSA 4096 bits

L'algorithme de hachage est de type SHA-256 (256 bits)

##### *Clés serveurs*

Les bi-clés des serveurs sont de type courbe elliptique NIST P-256 (256 bits)

L'algorithme de hachage est de type SHA-256 (256 bits)

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

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

##### *Clés d'AC*

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant au bi-clé (cf. caractéristiques du module TrustWay Protecchio).

##### *Clés serveurs*

L'équipement de génération de bi-clés employé par le RCCS 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 FR03 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 de cachet des données émises par ce serveur (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*

Les modules cryptographiques utilisés par l'AC Certigna Root CA et l'AC FR03 pour la génération et la mise en œuvre de leurs clés de signature sont respectivement la TrustWay CryptoBox et la Trustway Proteccio de la société BULL.

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

#### *Dispositifs de protection des clés privées des serveurs*

Le module cryptographique logiciel ou matériel utilisé pour la création de cachets, la protection et la mise en œuvre des clés privées des serveurs doit être conforme aux exigences du chapitre 11.

Le RCCS doit garantir contractuellement la conformité du dispositif mis en œuvre sur le serveur.

### 6.2.2. Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'AC FR03 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 FR03 est assuré par du personnel de confiance (porteurs de secrets d'AC) et via un outil mettant en œuvre le partage des secrets (systèmes où  $n$  exploitants parmi  $m$  doivent s'authentifier, avec  $n$  au moins égal à 2).

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

Le module cryptographique (HSM) est une ressource cryptographique partagée entre les différentes autorités constitutives de l'IGC Certigna. Les exigences de sécurité exprimées dans

les PC/DPC des différentes AC, concernant la gestion des secrets, sont identiques et correspondent au niveau de sécurité le plus élevé au sein de l'IGC Certigna (soit le niveau \*\*\* du RGS).

L'exportation d'un secret hors du module cryptographique est uniquement réalisée dans l'objectif de le sauvegarder, cette sauvegarde ayant lieu sous forme de partage. Cette exportation (sous forme chiffrée) nécessite la présence de l'officier de sécurité et d'un administrateur du module cryptographique.

La procédure de partage de secret est effectuée dans les différents cas suivants :

- Cérémonie de clé (création initiale / renouvellement d'un bi-clé d'AC)
- Suspicion de fraude (descellement d'une ou plusieurs enveloppes contenant une part de secret)

Le partage est effectué entre cinq personnes distinctes ayant un rôle de confiance dans l'IGC. La reconstitution du secret nécessite la réunion de 3 porteurs minimum.

Ce partage est consigné pour ces différents cas dans des documents internes. Le déroulement de ces procédures donne lieu à la génération d'un procès verbal conservé par le responsable de la sécurité. Les procédures concernées sont la cérémonie de clés [REF16] et la procédure de traitement d'arrivée, départ ou changement de rôle d'un employé [REF58].

Remarque :

La reconstitution du secret hors module cryptographique ne fournit pas d'information pertinente puisque le secret est reconstitué sous forme chiffrée et nécessite la connaissance d'une clé qui est elle-même partagée entre plusieurs personnes.

L'importation d'un secret dans le module cryptographique est uniquement réalisée dans le cadre d'une restauration. Cette importation (sous forme chiffrée) nécessite la présence de l'officier de sécurité et d'un administrateur du module cryptographique.

La procédure de reconstitution de secret est effectuée dans les différents cas suivants :

- Configuration initiale du module cryptographique du second ;
- Configuration initiale du module cryptographique de backup dans le cas du remplacement d'un module défaillant (nécessitant une maintenance ou une destruction) ;
- Perte de la configuration d'un module cryptographique en exploitation, nécessitant une restauration de tous les secrets.

L'importation/exportation de secrets sont contrôlées au final par deux personnes distinctes :

- Un administrateur du module cryptographique ;
- Le responsable de la sécurité détenant dans le coffre d'entreprise les cartes administrateur du module cryptographique.

Seuls les administrateurs détiennent les codes PIN des cartes.

### **6.2.3. Séquestre de la clé privée**

#### *Clés d'AC*

Les clés privées d'AC ne sont jamais séquestrées.

#### *Clés serveurs*

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

## 6.2.4. Copie de secours de la clé privée

### *Clé d'AC*

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

Le partage du secret et l'effacement sécurisé font partie de la procédure de cérémonie de clé [REF16]. Cette procédure est effectuée devant plusieurs témoins avec signature d'un procès verbal.

Les clés privées d'AC sont partagées selon le principe de partage de Shamir (n parts parmi m sont nécessaires pour reconstituer la clé privée). Les parts de secrets sont remises à des porteurs de secrets distincts. La reconstitution d'une clé hors module cryptographique n'est pas possible.

Sauf en cas de restauration ou de destruction, les parts de secret sont stockées dans des coffres de banque personnels. Lors de la reconstitution d'une clé privée, des mécanismes de contrôle permet de vérifier l'intégrité de la clé obtenue.

### *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

### *Clé d'AC*

La clé privée de l'AC FR03 n'est en aucun cas archivée.

L'exportation de la clé privée nécessite l'intervention de deux personnes (cf. 6.2.8. Méthode d'activation de la clé privée). Cette mesure garantit qu'une personne seule n'est en aucun cas apte à récupérer le clé privée de l'AC.

### *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 de l'opérateur d'AE, d'AED, du MC ou du RCCS.

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

### 6.2.7. Stockage de la clé privée dans un module cryptographique

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

La procédure de cérémonie de clé [REF16] garantit que les clés privées d'AC sont effectivement générées dans le module cryptographique et qu'à l'issue de cette cérémonie il n'existe plus de copie en clair ou chiffrée sur les disques des serveurs après le partage.

### 6.2.8. Méthode d'activation de la clé privée

#### *Clés d'AC*

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

La génération ou la restauration de la clé privée dans l'enceinte du module cryptographique nécessite l'authentification de l'administrateur du module par le biais d'une carte à puce 'administrateur'.

Le responsable sécurité est détenteur de cette carte, tandis que l'administrateur est le détenteur du code PIN qui lui est associé. Lorsqu'ils ne sont pas exploités, carte et code PIN doivent être placés dans le coffre personnel de leur détenteur respectif. Deux administrateurs sont désignés par le responsable sécurité (il existe deux cartes 'administrateur' distinctes).

Les administrateurs du module cryptographique peuvent, à l'aide de leur carte à puce, générer ou détruire des bi-clés, réaliser des sauvegardes des bi-clés.

#### *Clés serveurs*

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

### 6.2.9. Méthode de désactivation de la clé privée

#### *Clés d'AC*

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

L'exportation (sous forme chiffrée exclusivement) ou l'effacement des clés privées d'AC ne peut s'effectuer que sous le contrôle de deux personnes ayant un rôle de confiance (administrateur de la CryptoBox et responsable de sécurité). Ces opérations nécessitent l'authentification de l'administrateur à l'aide la carte 'administrateur' (saisie et soumission du code PIN), carte fournie par le responsable sécurité le temps nécessaire à effectuer ces opérations.

#### *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.

Des détails sont donnés dans la procédure de destruction de clé [REF17]. En l'occurrence, les CD et les supports papiers sont passés au broyeur. La destruction est effectuée en présence de plusieurs témoins pouvant attester de sa conformité par rapport à la procédure décrite.

### *Clés serveurs*

Le RCCS 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 10. Les dispositifs de protection des cachets sont évalués au niveau précisé au chapitre 11.

## 6.3. Autres aspects de la gestion des bi-clés

### 6.3.1. Archivage des clés publiques

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

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

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

Pour l'IGC Certigna, la durée de validité du certificat de l'AC Certigna Root CA est de 20 ans, et celle du certificat de l'AC FR03 est de 18 ans.

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

## 6.4. Données d'activation

### 6.4.1. Génération et installation des données d'activation

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

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



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

La génération et l'installation des données d'activation font intervenir, pour rappel, deux personnes distinctes :

- Le responsable sécurité (détenteur de la carte d'administration) ;
- L'administrateur du module cryptographique (détenteur du code PIN associé à la carte).

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

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

### **6.4.2. Protection des données d'activation**

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

Les données d'activation ne sont en aucune manière conservées sous forme électronique ou manuscrite. Il s'agit pour rappel d'une carte 'administrateur' et du code PIN associé, détenus respectivement par le responsable sécurité et l'administrateur du module cryptographique. En cas de panne matérielle ou d'oubli des données d'activation, il existe une seconde carte 'administrateur' dont le code PIN est détenu par le second administrateur.

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

Si le bi-clé est généré par l'AE, elle génère également les données d'activation qui sont envoyés par SMS (ou, en cas d'échec, par mail) au porteur, ces données d'activation ne sont pas sauvegardées par l'AE et sont modifiées par le porteur lors de l'acceptation du certificat. Une fois les données d'activation transmises au porteur, l'AE ne peut plus les renvoyer. Si le RCCS génère lui-même son bi-clé, il génère de manière autonome et sous sa seule responsabilité ses données d'activation.

### **6.4.3. Autres aspects liés aux données d'activation**

Sans objet.

## **6.5. Mesures de sécurité des systèmes informatiques**

### **6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques**

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

- Identification et authentification forte des utilisateurs pour l'accès au système (contrôle d'accès physique pour entrer dans la salle + contrôle logique par identifiant / mot de passe ou par certificat pour accéder au système) ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;

- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) ;
- Protection contre les virus informatiques et toutes formes de logiciel compromettant ou non autorisé et mises à jour des logiciels à l'aide du firewall ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Protection du réseau contre toute intrusion d'une personne non autorisée à l'aide du firewall ;
- Communication sécurisée inter-site (tunnel VPN IPSec) ;
- Fonctions d'audit (non-répudiation et nature des actions effectuées).

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

La charte de sécurité du personnel de l'IGC [REF15] décrit les mesures de sécurité applicables aux mots de passe attribués aux utilisateurs des équipements informatiques. Cette charte est remise à tout nouvel employé et signée par ce dernier et ce, en conformité avec la procédure de traitement d'arrivée, départ ou changement de rôle d'un employé [REF58]. Elle doit être également remise à tout intervenant externe, prestataire externe ou stagiaire, selon la procédure de traitement d'arrivée, départ ou changement de rôle d'un externe [REF59].

D'autre part, les règles de gestion des mots de passe et des codes (qualité et fréquence de changement) sont décrites dans la politique de gestion des mots de passe [REF55] destinée aux administrateurs système et réseau, gestionnaire du système de contrôle d'accès physique et responsable de sécurité.

La configuration des firewalls (firewalls du site principal et firewalls du site de secours) est amplement documentée [REF05]. Sont présentés entre autres :

- L'architecture physique et logique du réseau ;
- La description des interfaces des firewalls (équipements connectés et plan d'adressage) ;
- Les règles de routage ;
- Les flux ;
- La liaison sécurisée inter-site avec les tunnels VPN IPSec.

La procédure de mise à jour des logiciels anti-virus est également documentée [REF02].

Le logiciel de supervision (Nagios) mis en place permet une surveillance active des composants de la plate-forme technique des deux sites d'exploitation. L'objectif est de détecter tout incident ou sinistre et d'émettre en temps réel des alertes.

L'application et le respect des procédures sont de la responsabilité du responsable de sécurité.

A cette fin, des audits internes réguliers sont effectués :

- Audit de la configuration et audit des traces générées par les firewalls ;
- Audit des logs générés par les composants de l'IGC.

## 6.5.2. Niveau d'évaluation sécurité des systèmes informatiques

Sans objet.

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

### **6.6.1. Mesures de sécurité liées au développement des systèmes**

Conformément à l'analyse de risque menée, lors de la conception de tout nouveau projet de développement, une analyse sur le plan de la sécurité est réalisée et doit être approuvée par le Comité de Sécurité de l'AC. Cet aspect est précisé dans le guide de développement d'applications [REF27].

La configuration des systèmes de l'AC Certigna Root CA ou de l'AC FR03 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 FR03 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.

La description du contexte d'évolution de l'IGC est détaillée dans les procédures de mise à jour de la plate-forme technique [REF21]. Ces dernières sont applicables quelque soit la nature de la mise à jour (logiciel ou matériel). Les développements des modules liés à l'exploitation des composantes de l'IGC sont effectués en respectant les règles et consignes édictées dans le guide de développement d'applications [REF27]. Toute modification de la plate-forme technique est soumise à approbation du comité de sécurité et est, le cas échéant, consignée dans la main courante et ce, à des fins de traçabilité.

### **6.6.2. Mesures liées à la gestion de la sécurité**

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

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

Sans objet.

## **6.7. Mesures de sécurité réseau**

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement souhaité par l'AC. Le réseau est équipé notamment de deux firewalls (mis en cluster) intégrant un système de détection des intrusions IPS (avec émission d'alertes).

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

Les équipements réseaux (routeurs, firewalls, switch, etc.) sont disposés dans des locaux à accès restreint et contrôlé : l'accès physique à ces équipements nécessite une authentification par badge sans contact (MiFare) et des clés/codes pour l'ouverture des baies informatiques. Les composantes informatiques de l'IGC sont intégrées dans des sous-réseaux du réseau informatique de Dhimyotis. Ces sous-réseaux sont isolés dans des DMZ du firewall, ainsi que dans des VLAN. Ils sont inaccessibles par des personnes situées à l'extérieur du réseau de Dhimyotis via les liens WAN. Une liaison inter-site utilise les liens externes pour la réplication et la consolidation, et également pour la supervision et les opérations d'exploitation du site distant. Cette communication est effectuée au travers d'un tunnel VPN IPSec (nécessitant une authentification des pairs par certificat numérique). Ce tunnel garantit l'intégrité et la confidentialité des données échangées. Les schémas du réseau et les règles de firewall sont décrits dans la configuration des firewalls [REF05]. Cette description de la configuration est impérativement mise à jour à chaque modification de la configuration. Cette dernière est périodiquement contrôlée et révisée. La fréquence de revue de la configuration est tenue à jour dans les tableaux de bord de l'IGC, accessibles à l'ensemble du personnel (via un groupware). Les audits internes effectués par le cabinet externe couvrent également ces aspects.

## **6.8. Horodatage et Système de datation**

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

## 7. Profil des certificats et des LCR

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

### 7.1. Profil du certificat de l'AC

#### *Champs de base*

Champ	Description
Version	V3
Serial Number	Numéro de série unique
Signature	Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096
Issuer	DN={ } countryName : C=FR organizationName : O=Dhimyotis organizationUnitName : OU=0002 48146308100036 commonName : CN=Certigna Root CA
Validity	Dates et heures d'activation et d'expiration du Certificat
Subject	DN={ } countryName : C=FR organizationName : O=Dhimyotis organizationUnitName : OU=0002 48146308100036 commonName : CN= FR03
Subject Public Key Info	RSA 4096 bits

#### *Extensions*

Champ	C	Description
Authority Key Identifier	N	Identifiant de la clé publique de l'autorité Certigna Root CA
Subject Key Identifier	N	Identifiant de la clé publique de l'autorité FR03
Key Usage	O	Signature de certificat Signature de la liste de révocation
CRL Distribution Points	N	URL=http ://crl.certigna.fr/certignarootca.crl URL=http ://crl.dhimyotis.com/certignarootca.crl
Basic Constraints	N	cA = TRUE PathLengthConstraint=0

## 7.2. Profil des certificats Cachet Serveur

### Champs de base

Champ	Description
Version	V3
Serial Number	Numéro de série unique
Signature	Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096
Issuer	DN={ } countryName : C=FR organizationName : O=Dhimyotis organizationUnitName : OU=0002 48146308100036 commonName : CN=FR03
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 organizationName : O=Nom de l'entité à laquelle appartient le serveur informatique organizationUnitName : OU=ICD + identifiant de l'entité à laquelle appartient le serveur informatique enregistré conformément à la législation et aux réglementations en vigueur organizationIdentifier : OI=Informations sur le justificatif d'identité de l'entité commonName : CN= XXXY (cf 3.1.2)
Subject Public Key Info	NIST P-256

### Extensions

Champ	C	Description
Authority Key Identifier	N	Identifiant de la clé publique de l'autorité FR03
Subject Key Identifier	N	Identifiant de la clé publique du serveur
Key Usage	O	digitalSignature, nonRepudiation
Extended Key Usage	N	anyExtendedKeyUsage
Certificate Policies	N	1.2.250.1.177.2.2.1.1 : CPS=http://www.certigna.fr/PC
CRL Distribution Points	N	URL=http://crl.certigna.fr/2ddoc.crl URL=http://crl.dhimyotis.com/2ddoc.crl
Authority Information Access		URL=http://2ddoc.ocsp.certigna.fr URL=http://2ddoc.ocsp.dhimyotis.com caIssuers=http://autorite.certigna.fr/2ddoc.der caIssuers=http://autorite.dhimyotis.com/2ddoc.der
Basic Constraints	N	cA = FALSE
Subject Alternative Name	N	Type de document signé

## 7.3. Profil des LCR

### Champs de base

Champ	Description
Version	V2
Signature	Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096
Issuer	DN={ } countryName : C=FR organizationName : O=Dhimyotis organizationUnitName : OU=0002 48146308100036 commonName : CN=FR03
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 FR03
CRL Number	N	Contient le numéro de série de la LCR

## 7.4. Traitement des extensions de certificats par les applications

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

- si l'extension est non-critique, alors :

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

- si l'extension est critique, alors :

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

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

### **authorityKeyIdentifier**

Cette extension 'non critique' identifie la clé publique utilisée pour vérifier la signature sur un certificat. Elle permet de différencier les différentes clés utilisées par l'AC lorsque celle-ci dispose de plusieurs clés de signature.

Le champ authorityKeyIdentifier est obligatoirement renseigné. Il contient un identifiant unique (keyIdentifier). Cet identifiant de clé d'AC a la même valeur que le champ subject-KeyIdentifier du certificat de l'AC.

Les champs authorityCertIssuer et authorityCertSerialNumber ne sont pas renseignés.

### **keyUsage**

Cette extension définit l'utilisation prévue de la clé contenue dans le certificat. L'AC :

- indique l'usage prévu de la clé comme défini au chapitre 7.2.
- gère la criticité comme défini au chapitre 7.2.

### **certificatePolicies**

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

### **cRLDistributionPoints**

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

### **SubjectKeyIdentifier**

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

### **AuthorityInformationAccess**

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

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

### **Extended Key Usage**

Cette extension 'non critique' définit l'utilisation avancée de la clé, fixée à 'authentification client' et 'sécurisation de la messagerie'

### **Basic Constraints**

Cette extension 'non critique' indique si le certificat est un certificat d'entité finale ou un certificat d'autorité.



## **8. Audit de conformité et autres évaluations**

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

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

Le cabinet responsable des audits périodiques de surveillance de la certification RGS de l'AC peut être amené à intégrer dans son programme d'audit des audits et interviews auprès des opérateurs d'AED ou des mandataires de certification opérant pour l'AC.

### **8.1. Fréquences et/ou circonstances des évaluations**

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

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

Les audits internes récurrents sont réalisés par un cabinet d'audit externe et suivant les modalités spécifiées dans :

- La procédure d'audit et de contrôle interne [REFPROCAUDIT] qui décrit le mode opératoire à suivre pour la planification, la réalisation et le suivi d'audits et contrôles ;
- Le programme annuel d'audit et de contrôle interne [REFPROGAUDIT] qui décrit les activités d'audit et de contrôle qui se dérouleront chaque année ;
- Les Plans d'audit et de contrôle interne [REFPLANAUDIT] qui décrivent le plan des différentes sessions d'audit et de contrôle qui sont programmées chaque année.

Le programme d'audit défini chaque année est destiné à vérifier, assurer et améliorer la conformité de l'IGC. Il est élaboré et proposé par le cabinet externe responsable de cet audit. Il est soumis à l'approbation du responsable de sécurité et peut être modifié en cours de période.

### **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.

En l'occurrence les intervenants externes disposent d'une certification Lead Auditor ISO/IEC 27001.

### 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, ...).

Le programme d'audit établi par le cabinet externe inclut une procédure d'approbation des DPC.

### 8.5. Actions prises suite aux conclusions des évaluations

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

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

- En cas d' « amélioration », et selon l'importance de l'amélioration, l'équipe d'audit émet des recommandations à l'AC pour améliorer son fonctionnement. Les améliorations sont laissées à l'appréciation de l'AC qui décide ou non des les mettre en place.
- En cas de résultat « remarque » ou « écart mineur », l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de confirmation permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas d' « écart majeur », et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.

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

## **8.6. Communication des résultats**

Les résultats des audits de conformité effectués par le cabinet d'audit (audits récurrents) sont tenus à la disposition de l'organisme en charge de la qualification de l'autorité de certification AC FR03.

## **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 RCCS est facturée selon les tarifs affichés sur le site internet ou sur le formulaire de commande.

#### **9.1.2. Tarifs pour accéder aux certificats**

Sans objet.

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

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

#### **9.1.4. Tarifs pour d'autres services**

D'autres prestations pourront être facturées. Dans ce cas, les tarifs seront portés à la connaissance des personnes auxquelles ils s'appliquent et seront disponibles auprès de l'AC.

#### **9.1.5. Politique de remboursement**

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

## **9.2. Responsabilité financière**

### **9.2.1. Couverture par les assurances**

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

### **9.2.2. Autres ressources**

Sans objet.

### **9.2.3. Couverture et garantie concernant les entités utilisatrices**

Cf. chapitre 9.9.

## **9.3. Confidentialité des données professionnelles**

### **9.3.1. Périmètre des informations confidentielles**

Les informations considérées comme confidentielles sont les suivantes :

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

### **9.3.2. Informations hors du périmètre des informations confidentielles**

Sans objet.

### **9.3.3. Responsabilités en termes de protection des informations confidentielles**

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

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

L'AC applique des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles au 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage. De plus, lorsque ces données sont échangées, l'AC en garantit l'intégrité. L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des porteurs à des tiers dans le cadre de procédures légales. Elle donne également accès à ces informations au RCCS, MC et le cas échéant à l'opérateur d'AED en relation avec le RCCS.

Les aménagements suivants sont en place :

- Application d'une politique de classification et de manipulation des informations [REF30] ;
- Les dossiers d'enregistrement des RCCS, MC, et opérateurs d'AED sont stockés dans une armoire accessible uniquement aux opérateurs d'AE (située dans salle sécurisée) ;
- Les dossiers numérisés des RCCS, MC, et opérateurs d'AED ne sont accessibles que par les opérateurs d'AE et les administrateurs systèmes ;
- Application d'une procédure pour la fin de vie des supports de données [REF63] ;
- Signature de la charte de sécurité par le personnel de l'IGC (incluant notamment une clause de confidentialité) [REF15].

## **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° 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 RCCS un droit de rectification de leurs données personnelles en cas de données inexactes, incomplètes ou équivoques au moment de leur collecte. L'IGC Certigna s'engage donc à les rectifier dès lors qu'elle est informée qu'elles sont erronées.

Toute correction de données peut être demandée par simple envoi de courrier à l'autorité d'enregistrement concernée en précisant :

- Les données initiales transmises lors de l'enregistrement de la demande ;
- Les corrections à apporter ;
- Les éventuels justificatifs (photocopie de pièce d'identité).

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

Les courriers de demande de rectification des données sont traités par les opérateurs d'AE et les opérateurs d'AED. Ce point est traité dans :

- Les procédures opérationnelles à destination des MC [REF50] ;
- La procédure opérationnelle de traitement des demandes de certificat [REF04] ;
- Les procédures opérationnelles à destination des opérateurs d'AE déléguée [REF49].

### **9.4.2. Informations à caractère personnel**

Les informations considérées comme personnelles sont les suivantes :

- Les causes de révocation des certificats des serveurs ;
- Le dossier d'enregistrement des serveurs, des opérateurs d'AED et des MC.

### **9.4.3. Informations à caractère non personnel**

Sans objet.

### **9.4.4. Responsabilité en termes de protection des données personnelles**

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

### **9.4.5. Notification et consentement d'utilisation des données personnelles**

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

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

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

Par le biais de cette réquisition judiciaire, l'enquêteur est susceptible de demander :

- Les coordonnées du RCCS (nom, prénom, adresse mail, etc.) ;
- Les sites ou adresses électroniques en rapport avec l'entité concernée ;
- Les données relatives au(x) certificat(s) de sécurité ;
- Tout élément pouvant faciliter le décryptage par l'enquêteur de données chiffrées par le RCCS : information sur le format utilisé par les utilitaires de chiffrement de Dhimytis, etc.

#### **9.4.7. Autres circonstances de divulgation d'informations personnelles**

Sans objet.

### **9.5. Droits sur la propriété intellectuelle et industrielle**

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

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

### **9.6. Interprétations contractuelles et garanties**

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

- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ;
- N'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent ;
- Respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante) ;
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre 8.) et l'organisme de qualification ;
- Respecter les accords ou contrats qui les lient entre elles ou à l'entité ;
- Documenter leurs procédures internes de fonctionnement ;
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

Plusieurs niveaux de contrôle sont établis :

- Contrôle par le responsable sécurité : il est garant du respect par l'ensemble du personnel opérant sur l'IGC, par les opérateurs d'AED, ainsi que par les mandataires de certification, de la DPC et des procédures édictées ;
- Contrôle par le cabinet d'audit externe indépendant : ce dernier contrôle l'existence des procédures et leur application par différents moyens (audit des journaux d'événements, interviews, etc.).

### 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 RCCS 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 RCCS 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 RCCS 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.

Ces différents aspects font l'objet de contrôle lors des audits opérés par le cabinet externe.

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

Elle a pris les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des RCCS 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.

Ces aspects sécuritaires de l'IGC sont abordés lors des comités de sécurité planifiés mensuellement. Le comité de sécurité statue sur les décisions impactant le niveau de sécurité de l'IGC.

### 9.6.2. Service d'enregistrement

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

Il doit notamment :

- Identifier et valider toute demande initiale de certificat et toute demande de renouvellement courant en respectant les exigences exprimées respectivement en 3.2.3 et en 3.3.1 ;
- Identifier et valider toute demande éventuelle de révocation suivants les exigences exprimées en 3.4 ;
- Conserver la confidentialité des données personnelles traitées.



### 9.6.3. RCCS

Le RCCS a le devoir de :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- Protéger la clé privée du serveur dont il a la responsabilité par des moyens appropriés à son environnement ;
- 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, en cas de compromission ou de suspicion de compromission de la clé privée correspondante.

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

### 9.6.4. Utilisateurs de certificats

Les tiers utilisateurs doivent :

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

### 9.6.5. Autres participants

Sans objet.

## 9.7. Limite de garantie

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

## 9.8. Limite de responsabilité

Il est expressément entendu que Dhimyotis ne saurait être tenue pour responsable, ni d'un dommage résultant d'une faute ou négligence d'un accepteur et/ou des RCCS, ni d'un dommage causé par un fait extérieur, notamment en cas de :

- Utilisation d'un certificat pour une autre application que les applications définies au chapitre 1.5.1 de la présente PC;
- Utilisation d'un certificat pour garantir un autre objet que l'identité du serveur pour lequel le certificat a été émis ;

- Utilisation d'un certificat révoqué ;
- Utilisation d'un certificat au-delà de sa limite de validité ;
- Non-respect par les entités concernées des obligations définies aux chapitres 9.6.3 et 9.6.4 de la présente PC;
- Faits extérieurs à l'émission du certificat tels qu'une défaillance de l'application pour laquelle il peut être utilisé ;
- Force majeure comme définie par les tribunaux français.

## **9.9. Indemnités**

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

## **9.10. Durée et fin anticipée de validité de la PC**

### **9.10.1. Durée de validité**

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

### **9.10.2. Fin anticipée de validité**

La publication d'une nouvelle version de la PC type RGS « Certificats électroniques de services applicatifs » peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC correspondante. Dans ce cas, cette mise en conformité n'imposera pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité. Enfin, la validité de la PC peut arriver à terme prématurément en cas de cessation d'activité de l'AC (cf. chapitre 5.8).

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

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

## **9.11. Notifications individuelles et communications entre les participants**

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

- Faire valider, au plus tard un mois avant le début de l'opération, ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et de ses différentes composantes ;
- En informer, au plus tard un mois après la fin de l'opération, l'organisme de qualification.

## **9.12. Amendements à la PC**

### **9.12.1. Procédures d'amendements**

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

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

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

### **9.12.2. Mécanisme et période d'information sur les amendements**

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

### **9.12.3. Circonstances selon lesquelles l'OID doit être changé**

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

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

## **9.13. Dispositions concernant la résolution de conflits**

Il est rappelé que les conditions d'utilisation des certificats émis par l'AC FR03 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 RCCS 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 DPC est soumise au droit français, ainsi qu'à l'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.

## **9.16. Dispositions diverses**

### **9.16.1. Accord global**

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

### **9.16.2. Transfert d'activités**

Cf. chapitre 5.8.

### **9.16.3. Conséquences d'une clause non valide**

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

### **9.16.4. Application et renonciation**

Sans objet.

### **9.16.5. Force majeure**

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

## **9.17. Autres dispositions**

Sans objet.

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

### **10.1. Exigences sur les objectifs de sécurité**

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

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

### **10.2. Exigences sur la qualification**

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

Les modules cryptographiques utilisés par l'AC sont :

- le module TrustWay CryptoBox S507 qualifié au niveau renforcé,
- le module TrustWay Proteccio en cours de qualification au niveau renforcé, et faisant l'objet d'une dérogation par l'ANSSI pour les niveaux \* et \*\*.

Ils répondent aux exigences du chapitre 10.1.

## **11. Annexe 2 : exigences de sécurité du dispositif de création de cachet serveur**

### **11.1. Exigences sur les objectifs de sécurité**

Le dispositif de création de cachet, utilisé par le serveur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer son bi-clé, doit répondre aux exigences de sécurité suivantes:

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

### **11.2. Exigences sur la qualification**

Le dispositif de création de cachet est qualifié au minimum au niveau élémentaire si c'est l'AC qui génère le bi-clé ou certifié au minimum au niveau 2 selon la norme FIPS 140-2 dans le cas où c'est le RCCS qui génère le bi-clé.

## 12. Annexe 3 : documents de référence

- REF02 *"Procédure opérationnelle de mise à jour des logiciels anti-virus "*  
(02\_PO\_Maj\_Logiciels\_AntiVirus)
- REF03 *"Procédure de transfert d'activité ou de cessation d'activité "*  
(03\_PO\_Transfert\_Cessation\_Activite)
- REF04 *"Procédure Opérationnelle - Demande de certificat "*  
(04\_PO\_Demande\_Certificat)
- REF05 *"Configuration des firewalls "*  
(05\_Configuration\_Firewall)
- REF06 *"Procédure d'arrêt du module cryptographique d'une AC et de l'IGC Certigna "*  
(06\_PO\_Arret\_HSM\_AC\_IGC)
- REF07 *"Procédure Opérationnelle - Demande de révocation "*  
(07\_PO\_Demande\_Révocation)
- REF08 *"Procédure Opérationnelle - Enregistrement des MC "*  
(08\_PO\_Enregistrement\_MC)
- REF09 *"Procédure Opérationnelle - Service de publication "*  
(09\_PO\_Service\_Publication)
- REF10 *"Procédure Opérationnelle - Service d'archivage "*  
(10\_PO\_Archivage)
- REF13 *"Rôle des intervenants de l'IGC Certigna "*  
(13\_Role\_Intervenants\_IGC)
- REF15 *"Charte de sécurité du personnel de l'IGC "*  
(15\_Charte\_Seurite\_Personnels\_IGC)
- REF16 *"Cérémonie de clé"*  
(16\_Ceremonie\_Cle)
- REF17 *"Destruction de clés"*  
(17\_Destruction\_Cle)
- REF18 *"Restauration de clé"*  
(18\_Restauration\_Cle)
- REF21 *"Procédure Opérationnelle - Mise à Jour de la Plate-Forme Technique "*  
(21\_PO\_Maj\_PlateForme\_Technique)
- REF23 *"Procédure de mise à jour des PC et DPC "*  
(23\_PO\_Maj\_PC\_DPC)
- REF24 *"Formation du personnel de l'IGC Certigna "*  
(24\_Formation\_Personnel\_IGC\_Certigna)
- REF27 *"Guide de Développement d'Applications "*  
(27\_Guide\_Developpement)
- REF29 *"Profils d'accès physique et logique "*  
(29\_Profils\_Acces\_Physique\_Logique)
- REF30 *"Politique de classification et de manipulation des informations "*  
(30\_Politique\_Classification\_Manipulation\_Informations)
- REF34 *"Destruction de CryptoBox "*  
(34\_Destruction\_CryptoBox)
- REF35 *"Procédure opérationnelle de gestion des incidents"*  
(35\_PO\_Gestion\_Incidents)
- REF39 *"Procédure Opérationnelle - Gestion des clés cryptographiques d'AC"*  
(39\_PO\_Gestion\_Cles\_AC)
- REF42 *"Politique de sûreté"*  
(42\_Politique\_Surete)

REF44 "*Procédure Opérationnelle de sauvegarde* "  
 (44\_PO\_Sauvegarde)

REF47 "*Liste des cartes/tokens référencés pour les porteurs de certificats* "  
 (47\_Référence\_Cartes\_Porteurs)

REF48 "*Procédure Opérationnelle \_ Gestion des certificats de composante* "  
 (48\_PO\_Gestion\_Certi\_cats\_Composante)

REF49 "*Procédures Opérationnelles pour les Opérateurs d'AE déléguée*"  
 (49\_PO\_Operateur\_AE\_Deleguee)

REF50 "*Procédures Opérationnelles pour les Mandataires de Certification* "  
 (50\_PO\_Mandataire\_Certification)

REF51 "*Gestion du cycle de vie des clés de l'IGC Certigna* "  
 (51\_Gestion\_CycleVie\_IGC)

REF55 "*Politique de gestion des mots de passe* "  
 (55\_Politique de gestion des mots de passe)

REF58 "*Procédure de traitement de l'arrivée/départ/changement de rôle d'un employé* "  
 (58\_PO\_Traitement\_ArriveeDepartChangement\_Employe)

REF59 "*Procédure de traitement de l'arrivée/départ/changement de rôle d'un externe* "  
 (59\_PO\_Traitement\_ArriveeDepart\_Externe)

REF60 "*Règles d'accès pour CIV au site principal de Certigna* "  
 (60\_Regles\_CIV)

REF62 "*Procédure Opérationnelle - Enregistrement des opérateurs d'AED* "  
 (62\_PO\_Enregistrement\_OpAED)

REF63 "*Procédure Opérationnelle - Fin de vie des supports de données* "  
 (63\_PO\_Fin\_Vie\_Support\_Donnees)

REF64 "*Description des paramètres et algorithmes de signature* "  
 (64\_Parametres\_Algorithmes\_Signature)

REF65 "*Procédure Opérationnelle - Gestion des dispositifs de création de signature* "  
 (65\_PO\_Gestion-Token)

REF66 "*Politique de résolution des conflits* "  
 (66\_Politique\_Resolution\_Conflits)

REFPROCAUDIT "*Procédure d'audit et de contrôle interne* "  
 (\_procedure\_audit\_v1)

REFPROGAUDIT "*Programme annuel d'audit et de contrôle interne* "  
 (\_programme\_audit\_20xx\_20yy\_v1)

REFPLANAUDIT "*Plan d'audit et de contrôle interne* "  
 (xxxxxx\_plan\_audit\_n)

Document(s) ETSI :

ETSI\_TS\_102042 "*( Electronic Signatures and Infrastructures (ESI) ; Policy requirements for certification authorities issuing public key certificates)*"  
 (ts\_102042v020101p)