
Déclaration des Pratiques de Certification

CERTIGNA SERVICES CA

<i>OID :</i>	1.2.250.1.177.2.5.2
<i>Version :</i>	2.0
<i>Edité le :</i>	02/07/2018
<i>Auteurs :</i>	J. Allemandou
<i>Classification :</i>	Publique



SOMMAIRE

HISTORIQUE DU DOCUMENT	8
1. INTRODUCTION.....	10
1.1. PRESENTATION GENERALE.....	10
1.2. IDENTIFICATION DU DOCUMENT	10
1.3. DEFINITIONS ET ACRONYMES	11
1.3.1. Acronymes	11
1.3.2. Définitions	12
1.4. ENTITES INTERVENANT DANS L'IGC	16
1.4.1. Autorité de certification	16
1.4.2. Autorité d'enregistrement.....	16
1.4.3. Responsable de certificats électroniques de services applicatifs	17
1.4.4. Utilisateurs de certificats.....	17
1.4.5. Autres participants.....	18
1.5. USAGE DES CERTIFICATS	19
1.5.1. Domaines d'utilisation applicables.....	19
1.5.2. Domaines d'utilisation interdits	19
1.6. GESTION DE LA PC	20
1.6.1. Entité gérant la PC.....	20
1.6.2. Point de contact	20
1.6.3. Entité déterminant la conformité de la DPC avec la PC	20
1.6.4. Procédures d'approbation de la conformité de la DPC	20
2. RESPONSABILITE CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS	21
2.1. ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS.....	21
2.2. INFORMATIONS DEVANT ETRE PUBLIEES	21
2.2.1. Publication de la documentation	22
2.2.2. Publication de la LCR	22
2.2.3. Publication de la LAR	22
2.3. SIGNALER UN CERTIFICAT MALVEILLANT OU DANGEREUX	22
2.4. DELAIS ET FREQUENCES DE PUBLICATION.....	22
2.4.1. Publication de la documentation	22
2.4.2. Publication des certificats d'AC	23
2.4.3. Publication de la LCR	23
2.4.4. Publication de la LAR	23
2.5. CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES.....	23
3. IDENTIFICATION ET AUTHENTIFICATION	24
3.1. NOMMAGE.....	24
3.1.1. Types de noms	24
3.1.2. Nécessité d'utilisation de noms explicites	24
3.1.3. Anonymisation ou pseudonymisation	24
3.1.4. Règles d'interprétation des différentes formes de noms	24
3.1.5. Unicité des noms	24



3.1.6. Identification, authentification et rôle des marques déposées.....	24
3.2. VALIDATION INITIALE DE L'IDENTITE	25
3.2.1. Méthode pour prouver la possession de la clé privée	25
3.2.2. Validation de l'identité d'un organisme	25
3.2.3. Validation de l'identité d'un individu.....	27
3.2.4. Informations non vérifiées du RC et du service applicatif	34
3.2.5. Validation de l'autorité du demandeur	34
3.2.6. Validation du contrôle du domaine	35
3.2.7. Situation de risque élevé	36
3.2.8. Vérification de certaines sources d'information pour les certificats qualifiés/EV	36
3.3. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUELEMENT DES CLES.....	38
3.3.1. Identification et validation pour un renouvellement courant.....	38
3.3.2. Identification et validation pour un renouvellement après révocation	38
3.4. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION	38
4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	40
4.1. DEMANDE DE CERTIFICAT	40
4.1.1. Origine d'une demande de certificat.....	40
4.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat.....	40
4.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT	40
4.2.1. Exécution des processus d'identification et de validation de la demande	40
4.2.2. Acceptation ou rejet de la demande	41
4.2.3. Durée d'établissement du certificat	43
4.3. DELIVRANCE DU CERTIFICAT	43
4.3.1. Actions de l'AC concernant la délivrance du certificat	43
4.3.2. Notification par l'AC de la délivrance du certificat.....	43
4.4. ACCEPTATION DU CERTIFICAT	43
4.4.1. Démarche d'acceptation du certificat	43
4.4.2. Publication du certificat	43
4.4.3. Notification par l'AC aux autres entités de la délivrance du certificat.....	43
4.5. USAGES DE LA BI-CLE ET DU CERTIFICAT	44
4.5.1. Utilisation de la clé privée et du certificat par le RC	44
4.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat.....	44
4.6. RENOUELEMENT D'UN CERTIFICAT	44
4.7. DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE AU CHANGEMENT DU BI-CLE	44
4.7.1. Causes possibles de changement d'un bi-clé.....	44
4.7.2. Origine d'une demande d'un nouveau certificat	45
4.8. MODIFICATION DU CERTIFICAT.....	45
4.9. REVOCATION ET SUSPENSION DES CERTIFICATS	45
4.9.1. Causes possibles d'une révocation	45
4.9.2. Origine d'une demande de révocation	46
4.9.3. Procédure de traitement d'une demande de révocation	47
4.9.4. Délai accordé au RC pour formuler la demande de révocation	48
4.9.5. Délai de traitement par l'AC d'une demande de révocation	48
4.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats	49
4.9.7. Fréquence d'établissement des LCR	49
4.9.8. Délai maximum de publication d'une LCR.....	49



4.9.9. Exigences sur la vérification en ligne de la révocation et de l'état des certificats	49
4.9.10. Autres moyens disponibles d'information sur les révocations	50
4.9.11. Exigences spécifiques en cas de compromission de la clé privée	50
4.9.12. Suspension de certificat.....	50
4.10. FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS	50
4.10.1. Caractéristiques opérationnelles.....	50
4.10.2. Disponibilité de la fonction.....	50
4.11. FIN DE LA RELATION ENTRE LE RC ET L'AC.....	51
4.12. SEQUESTRE DE CLE ET RECOUVREMENT	51
5. MESURES DE SECURITE NON TECHNIQUES.....	52
5.1. MESURES DE SECURITE PHYSIQUE	52
5.1.1. Situation géographique et construction des sites	52
5.1.2. Accès physique	52
5.1.3. Alimentation électrique et climatisation	52
5.1.4. Vulnérabilité aux dégâts des eaux	53
5.1.5. Prévention et protection incendie	53
5.1.6. Conservation des supports	53
5.1.7. Mise hors service des supports.....	54
5.1.8. Sauvegardes hors site.....	54
5.2. MESURES DE SECURITE PROCEDURALES	54
5.2.1. Rôles de confiance	54
5.2.2. Nombre de personnes requises par tâche	55
5.2.3. Identification et authentification pour chaque rôle	55
5.2.4. Rôle exigeant une séparation des attributions	56
5.3. MESURES DE SECURITE VIS-A-VIS DU PERSONNEL.....	56
5.3.1. Qualifications, compétences et habilitations requises.....	56
5.3.2. Procédures de vérification des antécédents.....	56
5.3.3. Exigences en matière de formation initiale.....	57
5.3.4. Exigences et fréquence en matière de formation continue	57
5.3.5. Fréquence et séquence de rotation entre différentes attributions	57
5.3.6. Sanctions en cas d'actions non autorisées	57
5.3.7. Exigences vis-à-vis du personnel des prestataires externes.....	57
5.3.8. Documentation fournie au personnel	58
5.4. PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT	58
5.4.1. Type d'événements à enregistrer	58
5.4.2. Fréquence de traitement des journaux d'événements.....	59
5.4.3. Période de conservation des journaux d'événements.....	59
5.4.4. Protection des journaux d'événements	59
5.4.5. Procédure de sauvegarde des journaux d'événements.....	60
5.4.6. Système de collecte des journaux d'événements	60
5.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement .	60
5.4.8. Evaluation des vulnérabilités.....	60
5.5. ARCHIVAGE DES DONNEES	60
5.5.1. Types de données à archiver	60
5.5.2. Période de conservation des archives	61
5.5.3. Protection des archives	61



5.5.4. Procédure de sauvegarde des archives	62
5.5.5. Exigences d'horodatage des données	62
5.5.6. Système de collecte des archives.....	62
5.5.7. Procédures de récupération et de vérification des archives.....	62
5.6. RENOUELEMENT D'UNE CLE DE COMPOSANTE DE L'IGC	62
5.6.1. Clé d'AC.....	62
5.6.2. Clés des autres composantes	63
5.7. REPRISE SUITE A COMPROMISSION ET SINISTRE.....	63
5.7.1. Procédures de remontée et de traitement des incidents et des compromissions.....	63
5.7.2. Procédures de reprise en cas de corruption des ressources informatiques	63
5.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante	64
5.7.4. Capacité de continuité d'activité suite à un sinistre.....	64
5.8. FIN DE VIE DE L'IGC.....	64
6. MESURES DE SECURITE TECHNIQUES.....	66
6.1. GENERATION ET INSTALLATION DE BI-CLES.....	66
6.1.1. Génération des bi-clés	66
6.1.2. Transmission de la clé privée à son propriétaire.....	67
6.1.3. Transmission de la clé publique à l'AC.....	67
6.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats	67
6.1.5. Taille des clés.....	67
6.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité.....	68
6.1.7. Objectifs d'usage de la clé	68
6.2. MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES	68
6.2.1. Standards et mesures de sécurité pour les modules cryptographiques.....	68
6.2.2. Contrôle de la clé privée par plusieurs personnes	69
6.2.3. Séquestre de la clé privée	69
6.2.4. Copie de secours de la clé privée	69
6.2.5. Archivage de la clé privée.....	69
6.2.6. Transfert de la clé privée avec le module cryptographique	70
6.2.7. Stockage de la clé privée dans un module cryptographique.....	70
6.2.8. Méthode d'activation de la clé privée	70
6.2.9. Méthode de désactivation de la clé privée.....	70
6.2.10. Méthode de destruction des clés privées	71
6.2.11. Niveau d'évaluation sécurité du module cryptographique	71
6.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES	71
6.3.1. Archivage des clés publiques.....	71
6.3.2. Durées de vie des bi-clés et des certificats	71
6.4. DONNEES D'ACTIVATION	72
6.4.1. Génération et installation des données d'activation	72
6.4.2. Protection des données d'activation	72
6.4.3. Autres aspects liés aux données d'activation	72
6.5. MESURES DE SECURITE DES SYSTEMES INFORMATIQUES	73
6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques	73
6.5.2. Niveau d'évaluation sécurité des systèmes informatiques	73



6.6. MESURES DE SECURITE DES SYSTEMES DURING LEUR CYCLE DE VIE	73
6.6.1. Mesures de sécurité liées au développement des systèmes	73
6.6.2. Mesures liées à la gestion de la sécurité	74
6.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes.....	74
6.7. MESURES DE SECURITE RESEAU	74
6.8. HORODATAGE ET SYSTEME DE DATATION	74
7. PROFILS DES CERTIFICATS ET DES LCR	75
7.1. HIERARCHIE DE CONFIANCE	75
7.2. PROFILS DES CERTIFICATS DES AUTORITES RACINES	75
7.3. PRE-CERTIFICATS	75
8. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS	76
8.1. FREQUENCES ET/OU CIRCONSTANCES DES EVALUATIONS	76
8.2. IDENTITES/QUALIFICATIONS DES EVALUATEURS	76
8.3. RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES	76
8.4. SUJETS COUVERTS PAR LES EVALUATIONS	77
8.5. ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS	77
8.6. COMMUNICATION DES RESULTATS.....	77
9. AUTRES PROBLEMATIQUES METIERS ET LEGALES	78
9.1. TARIFS	78
9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats	78
9.1.2. Tarifs pour accéder aux certificats	78
9.1.3. Tarifs pour accéder aux informations d'état et de révocation des certificats	78
9.1.4. Tarifs pour d'autres services.....	78
9.1.5. Politique de remboursement.....	78
9.2. RESPONSABILITE FINANCIERE	78
9.2.1. Couverture par les assurances	78
9.2.2. Autres ressources	78
9.2.3. Couverture et garantie concernant les entités utilisatrices	78
9.3. CONFIDENTIALITE DES DONNEES PROFESSIONNELLES	79
9.3.1. Périmètre des informations confidentielles.....	79
9.3.2. Informations hors du périmètre des informations confidentielles.....	79
9.3.3. Responsabilités en termes de protection des informations confidentielles.....	79
9.4. PROTECTION DES DONNEES PERSONNELLES	79
9.4.1. Politique de protection des données personnelles	79
9.4.2. Informations à caractère personnel	80
9.4.3. Informations à caractère non personnel	80
9.4.4. Responsabilité en termes de protection des données personnelles.....	80
9.4.5. Notification et consentement d'utilisation des données personnelles.....	80
9.4.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives.....	80
9.4.7. Autres circonstances de divulgation d'informations personnelles.....	81
9.5. DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE	81
9.6. INTERPRETATIONS CONTRACTUELLES ET GARANTIES.....	81
9.6.1. Autorités de Certification	81
9.6.2. Service d'enregistrement.....	82



9.6.3. Responsable du Certificat.....	82
9.6.4. Utilisateurs de certificats.....	83
9.6.5. Autres participants.....	83
9.7. LIMITE DE GARANTIE.....	83
9.8. LIMITE DE RESPONSABILITE.....	83
9.9. INDEMNITES	84
9.10. DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC	84
9.10.1. Durée de validité	84
9.10.2. Fin anticipée de validité.....	84
9.10.3. Effets de la fin de validité et clauses restant applicables.....	84
9.11. NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS.....	85
9.12. AMENDEMENTS A LA PC	85
9.12.1. Procédures d'amendements.....	85
9.12.2. Mécanisme et période d'information sur les amendements.....	85
9.12.3. Circonstances selon lesquelles l'OID doit être changé	85
9.13. DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS	85
9.14. JURIDICTIONS COMPETENTES	86
9.15. CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS.....	86
9.16. DISPOSITIONS DIVERSES	86
9.16.1. Accord global.....	86
9.16.2. Transfert d'activités.....	86
9.16.3. Conséquences d'une clause non valide	86
9.16.4. Application et renonciation	87
9.16.5. Force majeure.....	87
9.17. AUTRES DISPOSITIONS.....	87
10. ANNEXE 1 : EXIGENCE DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC.....	88
10.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE	88
10.2. EXIGENCES SUR LA QUALIFICATION	88
11. ANNEXE 2 : EXIGENCES DE SECURITE DU DISPOSITIF DE D'AUTHENTIFICATION DU SERVEUR	89
11.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE	89
11.2. EXIGENCES SUR LA QUALIFICATION	89



HISTORIQUE DU DOCUMENT

Date	Version	Auteurs	Evolution du document
19/10/2015	1.0	R. DELVAL	Création
08/01/2016	1.1	V. WYON	Précisions sur : - Gestion du multi-domaines, (cf. 3.2), - Ajout de l'OID OV et du champ « localityName » pour répondre aux exigences du CA/Browser Forum (cf.7.2).
01/08/2016	1.2	J. ALLEMANDOU	Précisions sur : - La vérification de l'adresse email (cf. 3.2), - La vérification du FQDN.
16/12/2016	1.3	J. ALLEMANDOU	Révision de la charte graphique et précisions sur : - le niveau de conformité aux spécifications ETSI (cf. 1.1), - le retrait de la mention « Certifié conforme » (cf. 3.2.3), - les modalités de renouvellement courant (cf. 3.3.1), - les modalités d'acceptation du certificat (cf. 4.4.1), - les exigences relatives à l'OCSP Stapling (cf. 4.9.9), - le rôle d'officier d'enregistrement (cf. 5.2.1), - la durée minimale d'archivage (cf. 5.5.2), - les certificats de l'AC émis par 2 AC Racine (cf. 7.1), - les exigences sur la qualification du dispositif (cf. 11.2).
17/04/2017	1.4	J. ALLEMANDOU	Précisions apportées sur : - la version respectée des BR du CAB/Forum (cf. 1.1), - les URL disponibles pour tester les certificats (cf. 2.1), - la base des certificats révoqués ou rejetés (cf. 4.1.1), - la gestion des gTLD (cf. 4.2.2), - le répondeur OCSP et les LCR (cf. 4.9.9), - la valeur de l'exposant public utilisé pour le RSA (cf. 6.1.6), - la conformité à la RFC 5280 (cf. 7), - le format du serialNumber des certificats (cf. 7.2), - le gabarit des certificats OCSP émis par l'AC (cf. 7.2.3), - les audits des dossiers traités (cf. 8.4), - les engagements de l'AC synthétisés (cf. 9.6.1), - les indemnités des fournisseurs de logiciels (cf. 9.9), - la fréquence de révision des PC et DPC (cf. 9.12.1), - la gestion des exigences conflictuelles (cf. 9.16.3).
01/09/2017	1.5	J. ALLEMANDOU	Ajout des engagements relatifs : - au DNS CAA (cf. 4.2.1), - au Certificate Transparency (cf. 7.4). Ajout de l'extension « ExpiredCertsOnCRL » (7.3.2).
12/09/2017	1.6	J. ALLEMANDOU	Précisions apportées sur : - l'email de contact de Certigna (1.6.2), - le formulaire pour signaler un certificat (2.2.4), - les contrôles sur les demandes à haut risque (3.2.6), - les contrôles sur les TLD (4.2.2).
30/09/2017	1.7	J. ALLEMANDOU	Ajout des certificats QCP-w.
01/12/2017	1.8	J. ALLEMANDOU	Précisions apportées sur : - La périodicité de mise à jour de l'ARL (cf. 2.3.4), - Le registre utilisé pour les contrôles (cf. 4.2.1), - L'acceptation de la demande (cf. 4.2.2), - Les causes possibles de révocation (Cf. 4.9.1), - Les accès physiques (cf. 5.1.2), - Durée de vie des certificats de 825 jours maximum (cf. 6.3.2, 7) ; - Le schéma de la hiérarchie d'AC (cf. 7), - La longueur maximale du numéro de série (cf. 7), - La qualification du module cryptographique de l'AC (cf. 10.2),



			- Le changement des numéros de titres (6.2.8 à 6.2.11).
25/01/2018	1.9	J. ALLEMANDOU	Précisions apportées sur la remise des données d'activation (cf. 6.4.3)
02/07/2018	2.0	J. ALLEMANDOU	Ajout de contrôles complémentaires sur le FQDN (cf. 3.2.6) : - Email construit pour le contact du domaine ; - Changement apporté au site web ; - Changement DNS ; Précisions sur : - Les journaux utilisés pour les pré-certificats (cf. 7.3) ; - La politique de protection des données personnelles (cf. 9.4.1).



1. INTRODUCTION

1.1. Présentation générale

Certigna s'est dotée de l'Autorité de Certification (AC) nommée « Certigna Services CA » pour délivrer des certificats destinés à des services applicatifs de type « Authentification client/serveur SSL/TLS ».

La présente Déclaration des Pratiques de Certification (DPC) expose les pratiques que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers en conformité avec sa Politique de Certification (PC) qu'elle s'est engagée à respecter. La Politique de Certification (PC) expose les pratiques que l'AC applique et s'engage à respecter dans le cadre de la fourniture de son service de certification électronique. La PC identifie également les obligations et exigences portant sur les autres intervenants, les utilisateurs de certificat.

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

La présente DPC vise la conformité à :

- La PC Type « Certificats électroniques de Services Applicatifs » pour un usage Authentification client/serveurs SSL/TLS au niveau * du Référentiel Général de Sécurité (RGS) élaboré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ;
- Au règlement européen eIDAS et aux niveaux OVCP de l'ETSI EN 319 411-1 et QCP-w de l'ETSI EN 319 411-2 ;
- Aux exigences des « *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* » et des « *Guidelines for the issuance and management of Extended Validation Certificates* » du CA/BROWSER FORUM, dans leurs versions en vigueur publiées à l'adresse : <http://www.cabforum.org>.

En cas d'incohérence entre cette DPC et les exigences de la PC, ces exigences ont préséance sur cette DPC.

1.2. Identification du document

La présente DPC peut être identifiée par le nom de l'AC « Certigna Services CA » ainsi que par son OID : 1.2.250.1.177.2.5.2.

Elle décrit les dispositions mises en œuvre pour répondre aux engagements formulés dans la Politique de Certification (PC) ayant l'OID suivant : 1.2.250.1.177.2.5.1.

Usage(s)	RGS	ETSI	Type de serveur	OID
Authentification de type serveur TLS/SSL	*	OVCP	Pro (entreprises/administration)	1.2.250.1.177.2.5.1.1.1
Authentification serveur de type client	*	OVCP	Pro (entreprises/administration)	1.2.250.1.177.2.5.1.2.1
Authentification de type serveur TLS/SSL [Qualifié]		EVCP / QCP-w	Pro (entreprises/administration)	1.2.250.1.177.2.5.1.3.1



1.3. Définitions et acronymes

1.3.1. Acronymes

Les acronymes utiles à la bonne compréhension de ce document sont les suivants :

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



1.3.2. Définitions

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

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

Applicatif de vérification de cachet - Il s'agit de l'application mise en œuvre 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.

Autorisation de l'Autorité de Certification (CAA) - Emanant de la RFC 6844, l'enregistrement de ressource DNS permet au propriétaire d'un nom de domaine DNS de désigner les Autorités de Certification autorisées à délivrer des certificats pour ce domaine. La publication des enregistrements de ressources « CAA » permet à une Autorité de Certification publique d'implémenter des contrôles additionnels pour réduire les risques d'émission non autorisée de certificats.

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 œuvre opérationnelle d'au moins une fonction de l'IGC. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

Déclaration des Pratiques de Certification - Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de



la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

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

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

Entité commerciale - Toute entité qui n'est ni une organisation privée, ni une autorité administrative ou une entité non-commerciale. Cette définition couvre par exemple des partenariats généraux, des associations non constituées ainsi que des entreprises individuelles.

Existence légale - Une entité privée, une entité publique, ou une entité commerciale a une existence légale si elle a été formellement validée et n'est pas liquidée, dissolue ou abandonnée.

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

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

Représentant légal : Une personne d'une entité privée, d'une entité publique, ou d'une entité commerciale qui en est soit un propriétaire, un associé, un membre de la direction, le directeur ou un responsable, tel qu'identifié dans sa fiche de poste, ou un employé, un contractant, ou un agent autorisé par l'entité pour gérer l'activité en lien avec la demande, la délivrance et l'utilisation des certificats.

Juridiction d'immatriculation - Dans le contexte d'une entité privée, il s'agit du pays et (le cas échéant) de l'état ou de la région ou de la localité dans lesquels l'existence légale de l'entité a été établie par un dépôt (ou un acte) auprès d'une agence ou d'une entité publique appropriée (exemple : lieu où elle a été immatriculée). Dans le contexte d'une entité publique, le pays et (le cas échéant) l'état ou la région où l'existence de l'entité légale a été créée par la loi.

Juridiction d'enregistrement - Dans le cas d'une entité commerciale, l'état, la région, ou la localité où l'organisation a enregistré sa présence commerciale au travers d'un dépôt effectué par le représentant de l'entreprise.

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.

Organisation privée - toute entité qui n'est pas une entité publique (cotée ou non en bourse) enregistrée dont l'existence a été créée au travers d'un dépôt (ou d'un acte) auprès d'un organisme d'enregistrement des sociétés au niveau de sa juridiction d'immatriculation. En France, cette immatriculation s'effectue au niveau du registre du commerce et des sociétés.

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

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

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

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

Qualification d'un prestataire de services de certification électronique - Le Décret RGS et le règlement eIDAS décrivent 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).



Source Qualifiée d'Informations Fiscales Gouvernementales (QTIS) - Une source d'informations qui contient notamment des informations fiscales relatives à des organisations privées, des entités commerciales ou individuelles.

Source Qualifiée d'Informations Gouvernementales (QGIS) - Une base de données publique mise à jour régulièrement, dont l'objectif est de fournir des données fiables, à la condition qu'elle soit maintenue par une entité gouvernementale, que l'enregistrement des données soit obligatoire et que la déclaration de données fausses ou mensongères soit passible de sanctions pénales ou civiles.

Source Qualifiée d'Informations Indépendantes (QIIS) - Une base de données publique mise à jour régulièrement reconnue comme une source fiable pour certaines informations.

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 serveur de certificat ou chiffrer des données à destination d'un serveur.

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 Politique de Certification. 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 en rapport avec 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 pourrait 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 RC 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 RC 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 du présent document, un RC 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 RC 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 RC.

En cas de changement de RC, 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 RC explicitement identifié.

1.4.4. Utilisateurs de certificats

Authentification de type serveur SSL/TLS

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

Authentification serveur de type client

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

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



1.4.5. Autres participants

Autorité d'enregistrement déléguée

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

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

Il assure pour l'AC, dans le contexte de la délivrance de certificat, la vérification d'identité des futurs RC 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 RC et services applicatifs, et respecter les parties de la PC et de la DPC lui incombant.

Mandataire de certification

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

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

Le mandataire de certification peut être un représentant légal ou toute personne que ce dernier aura formellement désignée. Il assure pour l'AC, dans le contexte de la délivrance de certificat, la vérification d'identité des futurs RC 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 RC 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 RC.



1.5. Usage des certificats

1.5.1. Domaines d'utilisation applicables

Bi-clés et certificats du serveur

Authentification de type serveur SSL/TLS

Authentification du serveur auprès d'autres serveurs ou de personnes, dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS ou IPsec visant à établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés.

L'établissement de la clé de session peut se faire par un mécanisme cryptographique asymétrique, de type RSA (génération de la clé symétrique par le client et chiffrement de cette clé symétrique par la clé publique du serveur) ou de type Diffie-Hellman (obtention de la clé symétrique via un algorithme combinant la clé privée du client et la clé publique du serveur, et inversement).

Authentification serveur de type client

Authentification du serveur auprès d'autres serveurs, dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS ou IPsec visant à établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés.

L'établissement de la clé de session peut se faire par un mécanisme cryptographique asymétrique, de type RSA (génération de la clé symétrique par le client et chiffrement de cette clé symétrique par la clé publique du serveur) ou de type Diffie-Hellman (obtention de la clé symétrique via un algorithme combinant la clé privée du client et la clé publique du serveur, et inversement).

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

Bi-clés et certificats d'AC et de composantes

L'AC dispose d'une seule bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur (AC Racine). La bi-clé de l'AC permet de signer et de vérifier les différents types d'objets qu'elle génère : certificats des serveurs, certificat OCSP de l'AC et 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 l'AC, et dont le niveau de sécurité est adapté à celui requis pour l'AC.

1.5.2. Domaines d'utilisation interdits

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



1.6. Gestion de la PC

1.6.1. Entité gérant la PC

L'AC dispose d'un Comité de Sécurité présidé par le responsable Sécurité.

Ce comité est responsable de l'élaboration, du suivi, de la modification et de la validation de la 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
FRANCE

Contact mail : contact@certigna.fr

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

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

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

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

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. RESPONSABILITE CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS

2.1. Entités chargées de la mise à disposition des informations

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

- Serveurs Web :
 - o <http://crl.certigna.fr/servicesca.crl>
 - o <http://crl.dhimyotis.com/servicesca.crl>
- Serveurs OCSP :
 - o <http://servicesca.ocsp.certigna.fr>
 - o <http://servicesca.ocsp.dhimyotis.com>
- URLs de test des certificats Serveur TLS/SSL non qualifiés :
 - o Certificat valide : <https://valid.servicesca.dhimyotis.com>
 - o Certificat expire : <https://expired.servicesca.dhimyotis.com>
 - o Certificat révoqué : <https://revoked.servicesca.dhimyotis.com>
- URLs de test des certificats Serveur TLS/SSL qualifiés :
 - o Certificat valide : <https://valid.ev-servicesca.dhimyotis.com>
 - o Certificat expire : <https://expired.ev-servicesca.dhimyotis.com>
 - o Certificat révoqué : <https://revoked.ev-servicesca.dhimyotis.com>

Tous les services de publication sont hébergés par l'AC sur plusieurs systèmes d'information afin d'assurer une haute disponibilité.

2.2. Informations devant être publiées

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

- La PC ;
- Les Conditions Générales d'Utilisation liées au service de certification ;
- Les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, ...) ;
- Le certificat d'AC Certigna Root CA et le certificat d'AC intermédiaire en cours de validité ;
- La liste des certificats révoqués (LAR / LCR) ;
- La DPC sur demande expresse auprès de l'AC.

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



2.2.1. Publication de la documentation

Publication de la PC, des conditions générales et des formulaires

La PC, les conditions générales d'utilisation et les différents formulaires nécessaires pour la gestion des certificats sont publiés sous forme électronique à l'adresse <http://www.certigna.fr>. La PC est également publiée à l'adresse <http://www.dhimyotis.com>.

Publication de la DPC

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

Publication des certificats d'AC

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

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

2.2.2. Publication de la LCR

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

2.2.3. Publication de la LAR

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

2.3. Signaler un certificat malveillant ou dangereux

Pour signaler un certificat malveillant ou dangereux (un certificat dont la clé privée est suspectée de compromission, un certificat dont l'usage n'est pas respecté, ou tout autre type de fraude : compromission, détournement d'usage, conduite inappropriée, etc.) ou tout autre problème relatif aux certificats, veuillez utiliser le formulaire de contact disponible à l'adresse suivante <https://www.certigna.fr/contact.xhtml> et sélectionner l'objet « Certificat jugé malveillant ou dangereux ».

2.4. Délais et fréquences de publication

2.4.1. Publication de la documentation

La PC, les CGU 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.

2.4.2. 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, plusieurs sites répliqués ont été mis en place.

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

- Installation et exploitation d'un logiciel de supervision permettant de surveiller tous les éléments constitutifs de la plate-forme technique et d'émettre en temps réel des alertes en cas de détection d'incident ;
- Développement et mise en place de scripts permettant d'automatiser et de simplifier la répartition de charge d'un site à l'autre ;
- Instauration d'astreinte pendant les heures non ouvrées ;
- Souscription d'un service de surveillance de sécurité (24 heures sur 24) ;

2.4.3. Publication de la LCR

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

2.4.4. Publication de la LAR

La LAR est mise à jour au minimum une fois par an, et à chaque nouvelle révocation.

2.5. 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.

L'accès aux systèmes de publication par un opérateur requiert une double authentification : session utilisateur et utilisation d'un certificat utilisateur sur support dédié.



3. IDENTIFICATION ET AUTHENTIFICATION

3.1. Nommage

3.1.1. Types de noms

Dans chaque certificat conforme à la norme X.509, l'AC émettrice (correspondant au champ « issuer ») et le service applicatif (champ « subject ») sont identifiés par un « Distinguished Name » (DN) répondant aux exigences de la norme X.501.

3.1.2. Nécessité d'utilisation de noms explicites

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

Le format du DN est défini au chapitre « 7.2 Profils des certificats et des LCR » de la PC.

3.1.3. Anonymisation ou pseudonymisation

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

3.1.4. Règles d'interprétation des différentes formes de noms

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

3.1.5. Unicité des noms

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

L'attribut « serialNumber », valeur unique attribuée à chaque certificat émis par l'AC et présente dans le DN, assure également l'unicité du DN. Ce champ est constitué à partir d'un numéro aléatoire unique géré par l'AC précédé d'une ou plusieurs lettres indiquant le(s) usage(s) du certificat et son mode de stockage :

- "C" pour « Authentification de client »,
- "S" pour « Authentification de serveur ».

Pour les certificats qualifiés/EV, l'attribut « serialNumber » est constitué du numéro d'immatriculation/d'enregistrement de l'entité.

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

3.1.6. Identification, authentification et rôle des marques déposées

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

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 permet 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 RC.

Dans les deux cas (demande effectuée via une AE déléguée et demande effectuée via un mandataire de certification), un contrôle de l'individu est effectué sur la base des informations communiquées.

3.2.1. Méthode pour prouver la possession de la clé privée

L'AC s'assure de la détention de la clé privée par le RC avant de certifier la clé publique. Pour cela, l'AE ou le RC génère lui-même la bi-clé sur un dispositif conforme aux exigences du chapitre 11, 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

La validation de l'identité d'un organisme repose sur les vérifications suivantes :

- Vérification de l'identité et de l'existence légale et opérationnelle de l'entité ;
- Vérification de l'existence physique de l'entité ;
- Vérification des moyens de communication [*Certificats EV/qualifiés uniquement*] ;
- Vérification des noms de domaine de l'entité.

Vérification de l'identité et de l'existence légale et opérationnelle de l'entité

La vérification que l'entité a légalement l'utilisation exclusive du nom spécifié dans le champ « Organisation » du certificat est effectuée par rapprochement avec des informations récupérées dans des bases de données officielles (QIIS, QGIS, QTIS) confirmant l'existence de l'entité.

Ces bases de données contiennent des informations fiables renseignées par une source de confiance qui a enregistré l'entité. Les informations qui font l'objet d'une vérification durant le processus d'authentification de l'identité de l'entité comprennent le numéro SIREN ou SIRET, le



numéro de déclaration de TVA, le numéro D-U-N-S (Dun & Bradstreet). Les contrôles appliqués sont les suivants :

Pour les **organisations privées**, des contrôles sont opérés dans le QIIS ou le QGIS (ex : annuaire des entreprises de France, greffes des tribunaux de commerce, Dun & Bradstreet) afin de vérifier :

- L'existence légale : l'AE vérifie que l'existence légale de l'entité est reconnue et enregistrée auprès de l'organisme d'immatriculation et d'enregistrement de sa juridiction et qu'elle n'est pas désignée dans les enregistrements comme « inactive », « invalide », « en sommeil » ou équivalent.
- Le nom de l'entité : l'AE vérifie que le nom formel tel qu'enregistré auprès de l'organisme d'immatriculation et d'enregistrement de la juridiction de cette dernière correspond à celui spécifié dans la demande de certificat.
- Le numéro d'enregistrement : un numéro d'enregistrement attribué par l'organisme d'immatriculation et d'enregistrement de la juridiction de l'entité doit être fourni par l'entité. En cas de non attribution de numéro d'enregistrement par cet organisme la date d'enregistrement devra être fournie.
- Le représentant légal : l'AE doit obtenir le nom et l'adresse d'un représentant légal figurant dans la base de l'organisme d'immatriculation et d'enregistrement de la juridiction de l'entité.

Pour les **entités publiques**, des contrôles sont opérés dans le QIIS ou le QGIS afin de vérifier :

- L'existence légale : l'AE vérifie que l'existence légale de l'entité est établie dans la subdivision politique dans laquelle l'entité opère ;
- Le nom de l'entité : l'AE vérifie que le nom formel tel qu'enregistré auprès de l'organisme d'immatriculation et d'enregistrement de la juridiction de cette dernière correspond à celui spécifié dans la demande de certificat ;
- Le numéro d'enregistrement : un numéro d'enregistrement unique attribué par l'organisme d'enregistrement de la juridiction de l'entité doit être fourni par l'entité. En cas de non attribution de numéro d'enregistrement par cet organisme, l'AC intègre de façon claire dans le DN du certificat que l'entité est une entité publique.

Pour les **entités commerciales**, des contrôles sont opérés dans le QIIS ou le QGIS afin de vérifier :

- L'existence légale : l'AE vérifie que l'entité est engagée en affaire sous le nom spécifié dans la demande de certificat ;
- Le nom de l'entité : l'AE vérifie que le nom formel tel qu'enregistré auprès de l'organisme d'immatriculation et d'enregistrement de la juridiction de cette dernière correspond à celui spécifié dans la demande de certificat.
- Le numéro d'enregistrement : un numéro d'enregistrement attribué par l'organisme d'immatriculation et d'enregistrement de la juridiction de l'entité doit être fourni par l'entité. En cas de non attribution de numéro d'enregistrement par cet organisme la date d'enregistrement devra être fournie.
- Le représentant légal : l'AE vérifie l'identité du représentant légal identifié pour l'entité.

Pour les **entités non-commerciales**, des contrôles sont opérés dans le QIIS ou le QGIS afin de vérifier :

- L'existence légale : l'AE vérifie que l'entité est légalement reconnue comme une organisation internationale ;



- Le nom de l'entité : l'AE vérifie que le nom formel tel qu'enregistré auprès de l'organisme d'immatriculation et d'enregistrement de la juridiction de cette dernière correspond à celui spécifié dans la demande de certificat ;
- Le numéro d'enregistrement : un numéro d'enregistrement unique attribué par l'organisme d'enregistrement de la juridiction de l'entité doit être fourni par l'entité. En cas de non attribution de numéro d'enregistrement par cet organisme, l'AC intègre de façon claire dans le DN du certificat que l'entité est une organisation internationale.

Vérification de l'existence physique de l'entité

L'AE vérifie que l'adresse physique fournie est bien une adresse où l'entité ou une société mère/filiale réalise des opérations (pas une boîte aux lettres ou boîte postale) et qui constitue l'adresse de l'entité :

- Pour une entité dont l'activité est dans le même pays que sa juridiction d'immatriculation ou d'enregistrement, une vérification de la présence de l'adresse fournie dans le QGIS, le QIIS ou le QTIS est réalisée par l'AE.
- Pour une entité dont l'activité n'est pas dans le même pays que sa juridiction d'immatriculation ou d'enregistrement, l'AE s'appuie sur un courrier professionnel vérifié qui indique le lieu d'activité de l'entité et que les activités sont réalisées à cet endroit.

Vérification des moyens de communication de l'entité

Lors de la demande de certificat, l'adresse email du demandeur est contrôlée via l'envoi d'un lien d'activation. Pour les certificats EV/qualifiés, le numéro de téléphone communiqué dans la demande est mis en cohérence avec celui disponible au travers des annuaires téléphoniques publiques et du site internet officiel de l'entité le cas échéant. Un appel est réalisé par l'AE afin de vérifier le numéro de téléphone de l'entité et la capacité à joindre le demandeur via ce canal et afin d'avoir sa confirmation sur la légitimité de la demande de certificat.

Vérification de l'existence opérationnelle de l'entité

L'AE vérifie que l'entité a une existence opérationnelle en contrôlant le QIIS ou le QTIS afin de s'assurer que l'entité y figure bien.

Vérification du nom de domaine

Pour chaque FQDN listé dans le certificat, l'AE contrôle que, au moment où le certificat est émis, soit l'entité est le propriétaire du nom de domaine, soit elle a obtenu une autorisation pour utiliser le FQDN en utilisant la procédure décrite au chapitre

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 RC 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.

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



Un RC peut être amené à changer en cours de validité du certificat serveur correspondant. Dans ce cas, tout nouveau RC doit également faire l'objet d'une procédure d'enregistrement.

Le RC est soit le responsable légal de l'entité, soit une personne physique désignée formellement par ce dernier.

L'enregistrement d'un RC, 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.

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 est apportée aux contrôles de validité des pièces fournies (date de validité des pièces d'identité, date des demandes, etc.). Ces aspects sont développés lors de la formation initiale prévue pour les opérateurs d'AE et détaillés dans le programme de formation défini dans le document « [Suivi du personnel](#) ».

Les contrôles périodiques prennent en compte des vérifications par échantillonnage des dossiers traités, afin de s'assurer du respect des procédures. Ces contrôles sont menés par les personnes dans des rôles de contrôleurs ou de responsables de sécurité.

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

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

Le dossier de demande de certificat est à compléter depuis les formulaires disponibles sur le site de Certigna. Une fois complétés, les éléments suivants doivent être transmis à l'AE :

Formulaire de demande du certificat

<i>Objet</i>	Désignation d'un représentant légal de l'entité et de ses coordonnées
	Désignation du futur RC habilité et de ses coordonnées
	Désignation de l'identité de l'entité
	Désignation des CGU applicables
<i>Date</i>	Signé il y a moins de 3 mois
<i>Signature</i>	Signé par un représentant légal de l'entité pour habilitier le futur RC Signé par le futur RC pour accepter le rôle de RC et les CGU

Pièce d'identité officielle du RC

<i>Objet</i>	La photocopie d'un document officiel d'identité en cours de validité du futur RC ou d'une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintient un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent.
<i>Date</i>	Pièce valide au moment de l'enregistrement



Pièce d'identité officielle du Représentant légal

<i>Objet</i>	La photocopie d'un document officiel d'identité en cours de validité du représentant légal ou d'une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintient un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent.
<i>Date</i>	Pièce valide au moment de l'enregistrement

Justificatif attestant de la qualité du Représentant légal

<i>Objet</i>	Pour une entreprise , tout document attestant de la qualité du représentant légal de l'entité reconnu à l'échelle nationale. <i>Ex : un exemplaire des statuts de l'entreprise, en cours de validité, portant signature de ses représentants.</i> Pour une administration , fournir une pièce portant délégation ou subdélégation de l'autorité responsable de la structure administrative reconnue à l'échelle nationale.
<i>Date</i>	Justificatif valide au moment de l'enregistrement

Justificatif portant le numéro de SIREN de l'entité

<i>Objet</i>	Pour une entreprise , toute pièce portant le numéro SIREN de l'entreprise ou, à défaut, une autre pièce valide attestant l'identification unique de l'entreprise qui figurera dans le certificat. <i>Ex : extrait KBIS ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements</i>
<i>Date</i>	Justificatif valide au moment de l'enregistrement

Niveau qualifié/EV

L'authentification du RC par l'AE est réalisée lors d'un face-à-face physique ou sous forme dématérialisée à condition que la demande soit signée par le RC à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau qualifié et EV, que la signature soit vérifiée et valide au moment de l'enregistrement, et que le certificat sur lequel repose cette signature électronique soit un certificat qualifié au titre du règlement eIDAS.

Niveau *

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

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



Enregistrement d'un nouveau RC sans MC pour un certificat déjà émis

En cas de changement de RC pour un certificat en cours de validité, le nouveau RC fait l'objet d'une procédure d'enregistrement. Le dossier d'enregistrement d'un nouveau RC est à compléter depuis les formulaires disponibles sur le site de Certigna. Le dossier transmis à l'AE doit comprendre les éléments suivants :

Formulaire d'enregistrement d'un nouveau RC

Objet	Désignation d'un représentant légal de l'entité et de ses coordonnées
	Désignation du futur RC habilité et de ses coordonnées
	Désignation des CGU applicables
Date	Signé il y a moins de 3 mois
Signature	Signé par un représentant légal de l'entité pour habilitier le futur RC Signé par le futur RC pour accepter le rôle de RC et les CGU

Pièce d'identité officielle du RC

Objet	La photocopie d'un document officiel d'identité en cours de validité du futur RC ou d'une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintient un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent.
Date	Pièce valide au moment de l'enregistrement

Pièce d'identité officielle du Représentant légal

Objet	La photocopie d'un document officiel d'identité en cours de validité du représentant légal ou d'une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintient un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent.
Date	Pièce valide au moment de l'enregistrement

Justificatif attestant de la qualité du Représentant légal

Objet	Pour une entreprise , tout document attestant de la qualité du représentant légal de l'entité reconnu à l'échelle nationale. <i>Ex : un exemplaire des statuts de l'entreprise, en cours de validité, portant signature de ses représentants.</i> Pour une administration , fournir une pièce portant délégation ou subdélégation de l'autorité responsable de la structure administrative reconnue à l'échelle nationale.
Date	Justificatif valide au moment de l'enregistrement



Niveau Qualifié/EV

L'authentification du RC par l'AE est réalisée lors d'un face-à-face physique ou sous forme dématérialisée à condition que la demande soit signée par le RC à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau qualifié et EV, que la signature soit vérifiée et valide au moment de l'enregistrement, et que le certificat sur lequel repose cette signature électronique soit un certificat qualifié au titre du règlement eIDAS.

Niveau *

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

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

Enregistrement du mandataire de certification (MC)

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

L'enregistrement d'un MC nécessite la validation de l'identité "personne morale" de l'entité pour laquelle le MC interviendra, de l'identité "personne physique" du futur MC, et du rattachement du futur MC à cette entité. Le dossier d'enregistrement d'un mandataire de certification est à compléter depuis les formulaires disponibles sur le site de Certigna. Le dossier transmis à l'AE doit comprendre les éléments suivants :

Formulaire de demande d'enregistrement d'un mandataire

<i>Objet</i>	Désignation d'un représentant légal de l'entité et de ses coordonnées
	Désignation du futur mandataire habilité et de ses coordonnées
	Désignation de l'identité de l'entité
<i>Date</i>	Signé il y a moins de 3 mois
<i>Signature</i>	Signé par un représentant légal de l'entité pour habilitier le futur mandataire Signé par le futur mandataire pour accepter ce rôle

Lettre d'engagement du mandataire

<i>Objet</i>	Désignation du futur mandataire habilité et de ses coordonnées
	Désignation du rôle et des responsabilités du mandataire dont notamment : - Effectuer de façon impartiale et scrupuleuse les contrôles d'identité des futurs RC tels que définis dans la PC ; - Informer l'AE en cas de départ de l'entité.
<i>Date</i>	Signé il y a moins de 3 mois
<i>Signature</i>	Signé par le futur mandataire pour s'engager à respecter ces responsabilités



Pièce d'identité officielle du mandataire

Objet	La photocopie d'un document officiel d'identité en cours de validité du mandataire ou d'une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintient un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent.
Date	Pièce valide au moment de l'enregistrement

Justificatif attestant de la qualité du Représentant légal

Objet	Pour une entreprise , tout document attestant de la qualité du représentant légal de l'entité reconnue à l'échelle nationale. <i>Ex : un exemplaire des statuts de l'entreprise, en cours de validité, portant signature de ses représentants.</i> Pour une administration , fournir une pièce portant délégation ou subdélégation de l'autorité responsable de la structure administrative reconnu à l'échelle nationale.
Date	Justificatif valide au moment de l'enregistrement

Justificatif portant le numéro de SIREN de l'entité

Objet	Pour une entreprise , toute pièce portant le numéro SIREN de l'entreprise ou, à défaut, une autre pièce valide attestant l'identification unique de l'entreprise qui figurera dans le certificat. <i>Ex : extrait KBIS ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements</i>
Date	Justificatif valide au moment de l'enregistrement

Niveau qualifié/EV

L'authentification du MC par l'AE est réalisée lors d'un face-à-face physique ou sous forme dématérialisée à condition que la demande soit signée par le RC à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau qualifié/EV, que la signature soit vérifiée et valide au moment de l'enregistrement, et que le certificat sur lequel repose cette signature électronique soit un certificat qualifié au titre du règlement eIDAS.

Niveau *

L'authentification du futur MC 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 à condition que la demande et les justificatifs soient signés par le MC à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau * et que la signature soit vérifiée et valide au moment de l'enregistrement.

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



Enregistrement d'un RC via un MC

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

Le dossier de demande de certificat est à compléter depuis les formulaires disponibles sur le site de Certigna. Le dossier transmis à l'AE doit comprendre les éléments suivants :

Formulaire d'enregistrement d'un nouveau RC

<i>Objet</i>	Désignation d'un représentant légal de l'entité et de ses coordonnées
	Désignation du futur RC habilité et de ses coordonnées
	Désignation des CGU applicables
<i>Date</i>	Signé il y a moins de 3 mois
<i>Signature</i>	Signé par un représentant légal de l'entité pour habilitier le futur RC
	Signé par le futur RC pour accepter le rôle de RC et les CGU

Pièce d'identité officielle du RC

<i>Objet</i>	La photocopie d'un document officiel d'identité en cours de validité du futur RC ou d'une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintient un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent.
<i>Date</i>	Pièce valide au moment de l'enregistrement

Pièce d'identité officielle du mandataire

<i>Objet</i>	La photocopie d'un document officiel d'identité en cours de validité du mandataire ou d'une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintient un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent.
<i>Date</i>	Pièce valide au moment de l'enregistrement

Niveau qualifié/EV

L'authentification du RC par le MC est réalisée lors d'un face-à-face physique ou sous forme dématérialisée à condition que la demande soit signée par le RC à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau qualifié/EV, que la signature soit vérifiée et valide au moment de l'enregistrement, et que le certificat sur lequel repose cette signature électronique soit un certificat qualifié au titre du règlement eIDAS.

Niveau *

L'authentification du futur RC par le MC est réalisée par l'envoi du dossier soit par courrier postal, soit sous forme dématérialisée (dossier scanné puis transmis par courrier électronique).

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



Enregistrement d'un nouveau RC via un MC pour un certificat déjà émis

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

Le dossier d'enregistrement d'un nouveau RC est à compléter depuis les formulaires disponibles sur le site de Certigna. Le dossier transmis à l'AE doit comprendre les éléments suivants :

Formulaire d'enregistrement d'un nouveau RC

<i>Objet</i>	Désignation du Mandataire de certification de l'entité et de ses coordonnées
	Désignation du futur RC habilité et de ses coordonnées
	Désignation des CGU applicables
<i>Date</i>	Signé il y a moins de 3 mois
<i>Signature</i>	Signé par le Mandataire de certification de l'entité pour habilitier le futur RC Signé par le futur RC pour accepter le rôle de RC et les CGU

Pièce d'identité officielle du RC

<i>Objet</i>	La photocopie d'un document officiel d'identité en cours de validité du futur RC ou d'une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintient un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent.
<i>Date</i>	Pièce valide au moment de l'enregistrement

Niveau qualified/EV

L'authentification du RC par le MC est réalisée lors d'un face-à-face physique ou sous forme dématérialisée à condition que la demande soit signée par le RC à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau qualified/EV, que la signature soit vérifiée et valide au moment de l'enregistrement, et que le certificat sur lequel repose cette signature électronique soit un certificat qualifié au titre du règlement eIDAS.

Niveau *

L'authentification du futur RC par le MC est réalisée par l'envoi du dossier soit par courrier postal, soit sous forme dématérialisée (dossier scanné puis transmis par courrier électronique).

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 RC 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 du représentant légal et du responsable de certificat (directement par l'AE ou par le MC). Pour rappel, le formulaire de demande de certificat est signé par le représentant légal de l'entité et le responsable de certificat, et chacun d'eux doit fournir une copie de sa pièce d'identité afin de permettre à l'AE



de vérifier la signature du formulaire. De plus, comme décrit au chapitre 3.2.2, un appel téléphonique est réalisé par l'AE auprès du représentant légal de l'entité ou de la personne ayant délégation afin de vérifier la légitimité de la demande de certificat.

3.2.6. Validation du contrôle du domaine

En complément de la validation de l'autorisation sur le nom de domaine, l'un des contrôles ci-dessous est implémenté pour chaque FQDN afin de s'assurer de son contrôle par le demandeur et de confirmer la légitimité de la demande de certificat.

Email construit pour le contact du domaine

Un mail est envoyé par CERTIGNA à l'une des adresses créées en utilisant "admin", 'administrator', 'webmaster', 'hostmaster', ou 'postmaster' en préfixe, suivie par un arobase ("@"), suivi par le nom de domaine. Ce mail fournit un lien composé d'une valeur aléatoire et permet d'accéder à une page où le demandeur va confirmer qu'il contrôle ce nom de domaine et que la demande de certificat est légitime.

La valeur aléatoire est unique pour chaque FQDN et reste valide jusqu'à 30 jours après sa création.

Le mail peut être renvoyé mais un lien avec une nouvelle valeur aléatoire sera fourni pour chaque FQDN, rendant invalide le lien fourni précédemment.

Si l'email construit est similaire pour plusieurs FQDNs demandés (Ex : cas des sous-domaines), alors un seul mail est envoyé au contact du domaine avec les liens associés pour confirmer le contrôle de chaque FQDN.

Changement apporté au site web

Un mail est envoyé par CERTIGNA au demandeur avec une pièce jointe contenant une valeur aléatoire. Il s'agit d'un fichier texte que le demandeur doit positionner dans le répertoire "/.wellknown/pki-validation" du site web. Un contrôle automatique via le port 80 (HTTP) ou le port 443 (HTTPS) permet à CERTIGNA de vérifier la présence sur le site web du fichier et de contrôler la valeur aléatoire qu'il contient. La valeur aléatoire contenue dans le fichier n'apparaît pas dans la requête utilisée pour la vérification.

La valeur aléatoire est unique pour chaque FQDN et reste valide jusqu'à 30 jours après sa création.

Le mail peut être renvoyé mais un fichier avec une nouvelle valeur aléatoire sera fourni pour chaque FQDN, rendant invalide le fichier fourni précédemment.

Si plusieurs FQDNs sont concernés par une même demande, un seul mail est envoyé au demandeur contenant les fichiers associés. Le demandeur doit positionner tous les fichiers dans le répertoire afin de permettre le contrôle de chaque FQDN.



Changement DNS

Un mail est envoyé par CERTIGNA au demandeur avec un enregistrement de type DNS CNAME à positionner dans la configuration DNS du site web. Cet enregistrement est composé du nom de domaine préfixé par un label commençant par un underscore (" _") ainsi que d'une valeur aléatoire.

La valeur aléatoire est unique pour chaque FQDN et reste valide jusqu'à 30 jours après sa création.

Le mail peut être renvoyé mais un enregistrement avec une nouvelle valeur aléatoire sera fourni pour chaque FQDN, rendant invalide l'enregistrement fourni précédemment.

Si plusieurs FQDNs sont concernés par une même demande, un seul mail est envoyé au demandeur contenant les enregistrements associés. Le demandeur doit ajouter tous les enregistrements dans la configuration DNS du site web afin de permettre le contrôle de chaque FQDN.

3.2.7. Situation de risque élevé

L'AC développe, maintient, et implémente des procédures documentées qui identifient et imposent des activités de vérification complémentaires pour les demandes de certificats à haut risque préalablement à leur acceptation, de manière à garantir que ces demandes sont vérifiées conformément à ces exigences. En particulier, l'AE réalise des contrôles auprès de bases de données de noms de domaines suspectés d'être utilisés pour des activités de phishing (Ex : APWG, Phishing initiative, etc.) ainsi que dans les bases de données internes de l'AC contenant les certificats révoqués suite à une compromission ou les demandes de certificats suspectés d'être utilisés pour des activités de phishing.

3.2.8. Vérification de certaines sources d'information pour les certificats qualifiés/EV

Autres listes noires ou listes des entités sous surveillance

L'AE vérifie si l'un des signataires (Responsable du Certificat, Représentant Légal) ou l'entité :

- est identifié dans une liste d'interdiction gouvernementale, une liste de personnes interdites, ou une autre liste qui interdit les activités avec cette entité ou ces personnes sous la loi du pays de juridiction des opérations de l'AC ; ou
- est rattaché à une juridiction d'immatriculation, d'enregistrement, ou d'activité, dans un pays avec lequel la loi de juridiction des opérations de l'AC interdit de faire des affaires ;

L'AE rejette systématiquement la demande si l'un des signataires ou l'entité figure dans une de ces listes.



Maison mère/filiale/Affilié

L'AE vérifie la relation entre l'entité et la maison mère, une filiale ou un affilié lorsqu'elle est utilisée dans la demande. La relation entre l'entité et la maison mère, la filiale ou l'affilié est identifié au travers d'un QIIS ou QGIS.

Contrôles croisés et obligation de vigilance

Les dossiers de demandes de certificats qualifiés/EV font l'objet de contrôles croisés de la part de l'AE. Les résultats des processus et procédures de vérification réalisée par l'opérateur d'AE initial, tels que décrits dans les sections précédentes, sont examinés par un second opérateur d'AE qui analyse l'intégralité du dossier de demande de certificat en recherchant toute contradiction ou détail qui nécessiterait un examen approfondi.

Si nécessaire, l'Officier de l'AE demande des compléments d'informations ou des précisions aux parties prenantes, consulte des QIIS, et/ou d'autres sources d'informations pour résoudre les anomalies rencontrées. Si besoin est, les deux opérateurs d'AE se concertent pour statuer, au final, quant à la validité de la demande.

L'AC s'abstient de délivrer un certificat qualifié/EV jusqu'à ce que les informations collectées pour le dossier de demande soient complètes, afin de ne pas diffuser dans le certificat des informations inexactes que l'AC connaîtrait ou qu'une diligence raisonnable permettrait de découvrir. Si les justificatifs ou compléments d'information ne sont pas reçus dans le délai d'un mois, l'AE rejette la demande de certificat et le notifie à l'entité.

Les documents constituant le dossier de demande doivent être fournis exclusivement en langue française ou anglaise. Dans le cas où l'abonné est dans l'incapacité de fournir les documentations dans l'une ou l'autre de ces deux langues, l'autorité pourra le cas échéant faire traduire les documents concernés et faire supporter le coût induit à l'abonné.

Validation en face à face

Lors du face-à-face entre le RC et l'opérateur d'AE ou d'AED, les éléments suivants sont contrôlés :

- Le document officiel d'identité en cours de validité du RC comportant une photographie d'identité (carte nationale d'identité, passeport ou carte de séjour).
- Au moins deux autres justificatifs incluant le nom du RC, dont un au moins est produit par un établissement bancaire. Les éléments acceptés par l'AE sont les suivants :
 - Une carte bancaire de crédit avec une date d'expiration et qui n'est pas expirée ;
 - Une carte bancaire de retrait d'un établissement bancaire réglementé contenant une date d'expiration et qui n'est pas expirée ;
 - Un relevé de compte bancaire d'un établissement bancaire réglementé datant de moins de 6 mois ;
 - Une facture originale récente (facture télécom pour une ligne fixe ou une facture EDF/GDF) désignant le nom et l'adresse fixée du RC ;
 - Une copie d'une quittance de loyer datant de moins de 6 mois ;
 - Une facture de taxe locale pour l'année en cours (taxe foncière, taxe d'habitation) ;
 - Un extrait d'acte de naissance.



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

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

Le logiciel PKI 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

Niveau qualifié/EV

Lors du premier renouvellement, l'AC s'assure au minimum :

- que les informations du dossier d'enregistrement initial sont toujours valides et que le certificat à renouveler existe, et est toujours valide ;
- que le demandeur a toujours le contrôle du domaine via l'une des méthodes citées au chapitre 3.2.6.

Niveau *

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

La validation du contrôle du domaine par le demandeur est réalisée via l'une des méthodes citées au chapitre 3.2.6.

Lors du renouvellement suivant, l'AE identifie le RC et le service applicatif selon la même procédure que pour l'enregistrement initial.

3.3.2. Identification et validation pour un renouvellement après révocation

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

3.4. Identification et validation d'une demande de révocation

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

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



Si le RC n'est pas le demandeur :

- Le prénom et le nom du demandeur ;
- La qualité du demandeur (responsable légal, opérateur d'AED, MC) ;
- 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 par l'AE est détaillé dans la « [Procédure opérationnelle de demande de révocation](#) ».

Comme pour les demandes de certificats, les contrôles 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.



4. EXIGENCES OPERATIONNELLES 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 ou d'un MC dûment mandaté pour cette entité, avec un consentement préalable du futur RC.

L'AC maintient une base de données interne de tous les certificats précédemment révoqués et des requêtes de certificats précédemment rejetées en raison d'un phishing suspecté ou d'une autre utilisation ou intention frauduleuse. L'autorité de certification utilise ces informations pour identifier les demandes de certificats suspects ultérieures.

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

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

L'adresse mail du RC, 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 (RC, représentant légal) ;
- Validation de l'autorisation d'émettre un certificat pour les noms de domaines demandés ;
- Validation du contrôle du domaine ;
- Validation du dossier et de la cohérence des justificatifs présentés ;



- Assurance que le futur RC a pris connaissance des modalités applicables pour l'utilisation du certificat.

L'identité du futur RC et du représentant légal est approuvée si les pièces justificatives fournies sont valides à la date de réception. La vérification du FQDN et de l'entité qui en est titulaire est effectuée via l'utilisation de sites de type « WHOIS » (Ex : AFNIC). En complément des méthodes pour la validation du contrôle du domaine (cf. 3.2.6), la vérification du FQDN et de l'entité qui en est titulaire est effectuée via l'utilisation de sites de type « WHOIS » (Ex : AFNIC) et/ou de la fourniture de justificatifs permettant d'attester, dans la mesure du possible, de la propriété du nom de domaine. Un représentant légal de l'entité titulaire du nom de domaine selon ces sites et/ou justificatifs, doit désigner formellement l'entité de rattachement du RC ou le RC dans un document d'autorisation signé par ce représentant (formulaire de demande ou formulaire type fourni par l'AC).

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

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

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

Conformément à la RFC 6844, un contrôle est réalisé par l'autorité d'enregistrement pour chaque nom domaine présent dans l'extension « subjectAltName » du certificat à émettre et dont l'option « DNS CAA » est activée dans l'enregistrement DNS associé. Ce contrôle permet de vérifier que l'AC figure bien parmi les autorités autorisées à délivrer un certificat pour ces domaines. Dans le cas contraire, le demandeur est notifié par mail de la nécessité de mettre à jour les enregistrement DNS concernés afin d'y faire figurer l'AC.

Si le dossier de demande est valide et permet d'obtenir avec certitude l'autorisation d'émettre le certificat par un représentant légal de l'entité propriétaire des noms de domaines, l'AC s'autorise dès lors à émettre le certificat même si elle ne figure pas dans la liste des AC qui y sont autorisées.

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 des formulaires et justificatifs).

Un processus automatique est mis en œuvre, lors de la commande d'un certificat TLS/SSL, pour vérifier que le nom de domaine demandé est de type « *.domain.tld ». Pour consolider ce contrôle, les TLDs validés par l'ICANN sont récupérés automatiquement chaque jour via la liste fournie sur le site <https://publicsuffix.org>.

En complément, la vérification du propriétaire de nom de domaine réalisée par l'AE conduira, dans tous les cas, au rejet de la demande puisqu'il est impossible d'identifier le propriétaire



d'un nom de domaine de type « *.tld ». Les demandes avec un TLD invalide ou sans domaine (Ex : *.co.uk) seront systématiquement rejetées.

L'AC ne délivre pas de certificats contenant un nouveau gTLD en cours d'étude par l'ICANN. Avant de délivrer un certificat contenant un nom interne avec un gTLD que l'ICANN a annoncé comme en cours d'étude pour être opérationnel, l'AC adresse un avertissement à l'organisation dont le gTLD pourra être bientôt traité l'informant que l'AC révoquera immédiatement le certificat sauf si l'organisation enregistre rapidement le nom de domaine.

Lorsqu'un gTLD est délégué via son inclusion dans la base de données « Root zone » de l'IANA, le nom interne devient un nom de domaine, et à ce moment-là, un certificat avec ce gTLD, qui peut avoir respecté ces exigences au moment de l'émission, sera en violation avec ces exigences, à moins que l'AC ait vérifié les droits du demandeur sur le nom de domaine. Les dispositions ci-dessous visent à empêcher une telle violation.

Dans les 30 jours qui suivent l'approbation par l'ICANN d'un nouveau gTLD pour exploitation, comme peut en attester la publication d'un contrat avec l'opérateur gTLD sur [www.ICANN.org], l'AC compare le nouveau gTLD aux enregistrements de certificats valides et cesse d'émettre des certificats contenant un nom de domaine qui contient le nouveau gTLD jusqu'à ce que l'AC ait vérifié préalablement que l'organisation a le contrôle exclusif ou le droit exclusif d'utiliser le nom de domaine conformément à la section 3.2.2.4. Dans les 120 jours qui suivent la publication d'un contrat pour un nouveau gTLD sur [www.icann.org], l'AC révoque chaque certificat contenant un nom de domaine qui inclut le nouveau gTLD à moins que l'organisation soit le titulaire du nom de domaine ou qu'elle puisse démontrer le contrôle sur ce nom de domaine.

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

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

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

Pour les certificats qualifiés/EV, l'acceptation de la demande par l'AE requiert une action d'un opérateur d'AE et d'un Officier d'enregistrement préalablement à la création des certificats.

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



4.2.3. Durée d'établissement du certificat

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

4.3. Délivrance du certificat

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

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

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres 5 et 6 ci-dessous, notamment la séparation des rôles de confiance. (Cf. chapitre 5.2).

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](#) ».

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

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

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

L'acceptation peut être réalisée de deux façons :

- Soit, lors de l'installation du certificat, le RC choisit d'accepter ou non le certificat depuis son espace client. La notification d'acceptation ou de refus est transmise automatiquement à l'AC.
- Soit le RC notifie l'acceptation ou non du certificat en complétant un formulaire papier qui sera envoyé par courrier ou remis lors d'un face à face. Ce cas intervient notamment lors d'une défaillance technique n'ayant pas permis de récupérer la trace d'acceptation.

En cas de détection d'incohérence entre les informations figurant dans l'accord contractuel et le contenu du certificat, le RC doit refuser le certificat, ce qui aura pour conséquence sa révocation.

4.4.2. Publication du certificat

Les certificats émis ne sont pas publiés par l'AC.

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 qui est responsable de la délivrance, au RC, du certificat généré.



4.5. Usages de la bi-clé et du certificat

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

L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service décrit au chapitre 1.5.1. Les RC 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 de la 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 RC 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 RC 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 RC 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 RC 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 une bi-clé précédemment émise. Le renouvellement passe par la génération d'une nouvelle bi-clé et une nouvelle demande de certificat (cf. chapitre 4.1).

Le RC s'engage, en acceptant les Conditions Générales d'Utilisation, à générer une nouvelle bi-clé à chaque demande.

L'IGC détecte automatiquement 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.

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



Par ailleurs, une 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 RC (pas d'existence de processus automatisé). L'entité, via son MC le cas échéant, peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un service applicatif qui lui est rattaché.

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

4.8. Modification du certificat

La modification de certificats de l'AC 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 serveur

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

- Le RC, le représentant légal de l'entité à laquelle il appartient, le cas échéant le MC, ou l'opérateur d'AED demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du serveur et/ou de son support) ;
- Le représentant légal de l'entité à laquelle il appartient informe l'AC que la demande de certificat originale n'était pas autorisée et n'accorde pas d'autorisation rétroactive ;
- Le RC n'a pas respecté les Conditions Générales d'Utilisation du certificat ou l'AC obtient la preuve que l'usage du certificat est détourné ;
- L'AC est informée que le RC a violé une ou plusieurs de ses obligations en vertu des Conditions Générales d'Utilisation ;
- L'AC est informée de toute circonstance indiquant que l'utilisation d'un nom de domaine dans le certificat n'est plus autorisée légalement (Ex : un tribunal ou un arbitre a révoqué le droit d'un titulaire de nom de domaine d'utiliser le nom de domaine, une licence ou un accord de services entre le titulaire et le demandeur est terminée, ou le titulaire n'a pas pu renouveler le nom de domaine) ;
- 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 RC, l'entité, le cas échéant le MC ou l'opérateur d'AED, n'a pas respecté ses obligations découlant de la PC ou de la DPC ;
- L'AC détecte que les informations apparaissant dans le certificat sont inexactes ou trompeuses ;



- L'AC cesse ses activités pour quelque raison que ce soit et n'a pas pris de dispositions pour qu'une autre AC assure le relai en cas de révocation du certificat ;
- Le droit de l'AC pour émettre des certificats sous ces exigences expire ou est révoqué ou est terminé, à moins que l'AC n'ait pris des dispositions pour maintenir la publication des CRL/OCSP ;
- Le certificat de signature de l'AC est révoqué (ce qui entraîne la révocation de tous les certificats en cours de validité signés par la clé privée correspondante) ;
- Le contenu ou le format des certificats présente un risque inacceptable pour les fournisseurs de logiciels applicatifs ou les utilisateurs (Ex : le CA/Browser Forum peut déterminer qu'un algorithme ou une clé de chiffrement/signature obsolète présente un risque inacceptable et que ces certificats doivent être révoqués et remplacés par l'AC sous un délai donné.
- L'arrêt définitif du serveur ou la cessation d'activité de l'entité du RC de rattachement du serveur ;
- 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) ;
- 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 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 serveur

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

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

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



Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

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

4.9.3. Procédure de traitement d'une demande de révocation

Certificat de serveur

La demande de révocation est effectuée auprès de l'AE, 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 de Certigna) :

- L'identité du RC ;
- L'adresse email du RC ;
- L'identité et la fonction du serveur ;
- La raison de la révocation ;

Si le RC n'est pas le demandeur :

- Le prénom et le nom du demandeur ;
- La qualité du demandeur (responsable légal, 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 RC ;
- 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 RC est informé de la révocation par mail ;
- L'opération est enregistrée dans les journaux d'événements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat ;
- L'AC ne publie pas dans la LCR les causes de révocation des certificats.



Le mécanisme de révocation est décrit dans la « [Procédure opérationnelle de demande de révocation](#) ».

Certificats d'une composante de l'IGC

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

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

Le processus est détaillé dans la « [Procédure de gestion des clés cryptographiques](#) » et dans la « [Procédure de gestion des certificats de composante](#) ».

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

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

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

Certificats de 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 24 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 œuvre en cas de révocation d'un certificat d'une composante de l'IGC sont décrits dans la « [Procédure de gestion des clés cryptographiques](#) » et dans la « [Procédure de gestion des certificats de composante](#) ».

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

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

4.9.7. Fréquence d'établissement des LCR

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

4.9.8. Délai maximum de publication d'une LCR

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

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

En complément de la publication des LCR sur les sites en ligne, l'AC met à disposition un répondeur OCSP accessible aux adresses suivantes :

- <http://servicesca.ocsp.certigna.fr>
- <http://servicesca.ocsp.dhimyotis.com>

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.

Les informations fournies par le répondeur OCSP pour les certificats des serveurs sont mises à jour tous les 4 jours au maximum, et les réponses OCSP ont une durée de validité de 7 jours. Les certificats révoqués et expirés sont maintenus dans les CRL et répondeurs OCSP.

Dans le cadre de l'utilisation du service de répondeur OCSP de Certigna, un nombre maximal de 250.000 requêtes OCSP est autorisé par certificat et par jour. En cas de dépassement de ce seuil, Certigna se réserve le droit d'imposer au titulaire du certificat la mise en place du mécanisme d'*OCSP Stapling* sur le serveur sécurisé par le certificat.

En cas de refus de mise en place de l'OCSP stapling, Certigna pourrait être amenée à révoquer le certificat du titulaire et ce afin de maintenir et garantir la disponibilité du répondeur OCSP pour l'ensemble de ses clients.



Nota - Le mécanisme de l'OCSP Stapling consiste à configurer le serveur sécurisé du client afin qu'il assure le rôle de proxy pour l'interrogation OCSP et cela afin de réduire drastiquement le nombre de requêtes transmises au répondeur OCSP de 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

Le RC est tenu 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 de Certigna et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

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

Les mesures mises en œuvre sont cadrées par la « [Procédure de gestion des clés cryptographiques](#) » et dans la « [Procédure de gestion des certificats de composante](#) ».

4.9.12. Suspension de certificat

Les certificats émis par l'AC 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).

Les activités relatives au service de publication sont définies dans la « [Procédure de gestion du service publication](#) ».

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).

L'AC s'assure que les CRLs de la chaîne de confiance des certificats qualifiés/EV peuvent être téléchargées en moins de 3 secondes via une ligne analogique sous des conditions de réseau normales. 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).

La réplication des services sur plusieurs systèmes d'information permet d'assurer automatiquement une continuité des services en cas de sinistre. L'AC s'appuie également sur les astreintes de son personnel aux heures non-ouvrées pour assurer la supervision des alertes de disponibilités de ces fonctions.

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

En cas de fin de relation contractuelle ou réglementaire entre l'AC et 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 œuvre. Cette DPC a été élaborée en fonction de cette analyse des risques. La gestion des risques de sécurité de l'information est décrite dans la « [Procédure de gestion des risques SI](#) » ainsi que dans le formulaire « [Gestion des risques SI](#) ».

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

Les systèmes d'information utilisés pour les fonctions de l'AC sont hébergés dans plusieurs centres de production présentant les mêmes caractéristiques en matière de sécurité. La localisation des sites ne présente pas de risques majeurs.

Les risques sont identifiés dans le document « [Gestion des risques SI](#) ».

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.

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

Les accès physiques aux centres de production sont restreints au travers de mesures de contrôle d'accès physique. Les mesures mises en œuvre sont décrites dans la « [Politique de sûreté](#) ».

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 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.

Les centres de production sont équipés d'onduleurs et de groupes électrogènes. Les mesures mises en œuvre sont décrites dans la « [Politique de sûreté](#) ».



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 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.

Des moyens pour la détection des fuites d'eaux sont positionnés dans les centres de production. Les mesures mises en œuvre sont décrites dans la « [Politique de sûreté](#) ».

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 la 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.

Les salles informatiques des centres de production sont équipées de systèmes d'extinction automatique par gaz inerte. Les mesures mises en œuvre sont décrites dans la « [Politique de sûreté](#) ».

5.1.6. Conservation des supports

Les informations et leurs actifs supports intervenant dans les activités de l'IGC sont identifiés, inventoriés et leurs besoins de sécurité définis en disponibilité, intégrité et confidentialité.

Les actifs sont listés dans le document « [Inventaire des actifs](#) », et les besoins de sécurité dans le formulaire de « [Gestion des risques SI](#) ».

Des mesures sont mises en place pour éviter la compromission et le vol de ces informations. Les supports correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils sont manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.

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

Les mesures mises en œuvre permettent de couvrir les risques identifiés dans le formulaire de « [Gestion des risques SI](#) ».

La « [Politique de sûreté](#) », la « [Procédure de gestion des actifs](#) » et la « [Procédure de gestion des matériels](#) » décrivent plus en détails les dispositions mises en œuvre.



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.

La « [Politique de sûreté](#) », la « [Procédure de gestion des actifs](#) » et la « [Procédure de gestion des matériels](#) » décrivent plus en détails les dispositions mises en œuvre.

5.1.8. Sauvegardes hors site

Des sauvegardes externalisées sont mises en œuvre et organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conformément aux engagements de la PC notamment en matière de disponibilité et de protection en confidentialité et en intégrité des informations sauvegardées.

La « [Procédure de sauvegarde](#) », la « [Procédure de gestion des actifs](#) » et la « [Procédure de gestion des matériels](#) » décrivent plus en détails les dispositions mises en œuvre.

5.2. Mesures de sécurité procédurales

5.2.1. Rôles de confiance

Chaque composante de l'IGC distingue 7 rôles fonctionnels de confiance :

- **Responsable de sécurité** : Le responsable de sécurité est chargé de la mise en œuvre et du contrôle de la politique de sécurité des composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes des composantes. Il est habilité à prendre connaissance des archives et des journaux d'événements. Il est responsable des opérations de génération et de révocation des certificats qui sont implémentées par les Officiers d'enregistrement.
- **Responsable d'application** : Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
- **Administrateur système** : Il est chargé de la mise en route, de la configuration, de l'installation et de la maintenance technique des équipements informatiques de l'AC pour l'enregistrement, la génération des certificats, et la gestion des révocations. Il assure l'administration technique des systèmes et des réseaux de la composante.
- **Opérateur** : Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
- **Contrôleur** : Personne 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.
- **Officier d'enregistrement** : Il est en charge de l'approbation des actions de génération et de révocation des certificats des serveurs et responsables de certificats.



- **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.

Le document « [Rôles, responsabilités et autorités](#) », la « [Procédure de gestion du personnel](#) » et le document de « [Suivi du personnel](#) » décrivent plus en détails les dispositions mises en œuvre.

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.

La « [Politique de sûreté](#) », la « [Procédure de gestion des actifs](#) » et la « [Procédure de gestion des matériels](#) » décrivent plus en détails les dispositions mises en œuvre.

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 ».

Le document « [Rôles, responsabilités et autorités](#) », la « [Procédure de gestion du personnel](#) » et le document de « [Suivi du personnel](#) » décrivent plus en détails les dispositions mises en œuvre.

5.2.3. Identification et authentification pour chaque rôle

Chaque attribution de rôle à un membre du personnel de l'IGC est attribuée et acceptée formellement. L'AC fait vérifier l'identité et les autorisations de tout membre de son personnel avant l'attribution des privilèges relatifs à ses fonctions. L'attribution d'un rôle à un membre du personnel de l'IGC suit 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.).

Le document « [Rôles, responsabilités et autorités](#) », la « [Procédure de gestion du personnel](#) » et le document de « [Suivi du personnel](#) » décrivent plus en détails les dispositions mises en œuvre.



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.

Le document « [Rôles, responsabilités et autorités](#) », la « [Procédure de gestion du personnel](#) » et le document de « [Suivi du personnel](#) » décrivent plus en détails les dispositions mises en œuvre.

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

5.3.1. Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont soumis à une clause de confidentialité vis-à-vis de l'employeur. L'adéquation des compétences professionnelles des personnels intervenant dans l'IGC est vérifiée en cohérence avec les attributions.

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.

Les compétences professionnelles sont déterminées lors du recrutement et chaque année par les responsables sécurité.

Le document « [Rôles, responsabilités et autorités](#) », la « [Procédure de gestion du personnel](#) » et le document de « [Suivi du personnel](#) » décrivent plus en détails les dispositions mises en œuvre.

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. Les employés fournissent une copie du bulletin n°3 de leur casier judiciaire préalablement à leur affectation. Cette vérification est renouvelée périodiquement (au minimum tous les 3 ans). De plus, l'AC s'assure que les personnels ne souffrent pas de conflits d'intérêts préjudiciables à l'impartialité de leurs tâches.

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

Le document « [Rôles, responsabilités et autorités](#) », la « [Procédure de gestion du personnel](#) » et le document de « [Suivi du personnel](#) » décrivent plus en détails les dispositions mises en œuvre.



œuvre.

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.

Le document « [Rôles, responsabilités et autorités](#) », la « [Procédure de gestion du personnel](#) » et le document de « [Suivi du personnel](#) » décrivent plus en détails les dispositions mises en œuvre.

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.

Le document « [Rôles, responsabilités et autorités](#) », la « [Procédure de gestion du personnel](#) » et le document de « [Suivi du personnel](#) » décrivent plus en détails les dispositions mises en œuvre.

5.3.5. Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6. Sanctions en cas d'actions non autorisées

Tout membre du personnel de l'AC agissant en contradiction avec les politiques et les procédures établies 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 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.

Le personnel externe à l'AC est suivi au travers de la « [Procédure de gestion des tiers](#) ». Une appréciation des risques SI liés aux tiers est réalisée et les Besoins/exigences en sécurité sont cartographiées afin d'être suivies au travers du document de « Suivi des tiers » et les accords contractuels associés.



5.3.8. Documentation fournie au personnel

Chaque membre du personnel dispose de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, l'AC lui remet les politiques de sécurité l'impactant. Les opérateurs disposent notamment des manuels d'opérateurs correspondant aux composantes sur lesquelles ils interviennent.

Le document « [Rôles, responsabilités et autorités](#) », la « [Procédure de gestion du personnel](#) » et le document de « [Suivi du personnel](#) » décrivent les mesures mises en œuvre en matière de sensibilisation et formations sur les documentations et le document « [Procédure de gestion documentaire](#) » cadre la gestion de ces documentations.

5.4. Procédures de constitution des données d'audit

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

5.4.1. Type d'événements à enregistrer

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

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Événements liés à la journalisation : actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres événements sont aussi recueillis. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques :

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

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

- 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) ;
- Traces des opérations réalisées pour traiter les demandes de certificats, incluant celles relatives au « DNS CAA » et au « Certificate Transparency » ;



- Validation / rejet d'une demande de certificat ;
- Génération des certificats des serveurs ;
- Transmission des certificats aux RC et, selon les cas, acceptations / rejets explicites par les RC ;
- Publication et mise à jour des informations liées à l'AC (PC/DPC, certificats d'AC, CGU, etc.)
- Réception d'une demande de révocation ;
- Validation / rejet d'une demande de révocation ;
- Génération puis publication des LCR ;
- Destruction des supports contenant des renseignements personnels sur les RC.
- Le processus de journalisation permet un enregistrement en temps réel des opérations effectuées.

Les opérations de journalisation sont effectuées au cours du processus.

Le processus de journalisation permet un enregistrement en temps réel ou quotidien au plus tard des opérations effectuées.

En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'évènement. Les événements et données spécifiques à journaliser sont documentés par l'AC.

Les pratiques mises en œuvre sont décrites plus en détails dans la « [Procédure de journalisation](#) » et la « [Procédure d'archivage](#) ».

5.4.2. Fréquence de traitement des journaux d'événements

Cf. chapitre 5.4.8

5.4.3. Période de conservation des journaux d'événements

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

5.4.4. Protection des journaux d'événements

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

L'accès en écriture à ces fichiers est protégé au travers de contrôles d'accès logiques et physiques décrit plus en détail dans la « [Procédure de journalisation](#) », la « [Politique de contrôle d'accès logiques](#) » et la « [Politique de sûreté](#) ».

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).

La « [Procédure de synchronisation des horloges](#) » décrit les mesures mises en œuvre.



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 PC. Une sauvegarde est effectuée à fréquence élevée afin d'assurer la disponibilité de ces informations.

5.4.6. Système de collecte des journaux d'événements

Les journaux d'événements sont centralisés dans un concentrateur. La consolidation obtenue est accessible par le personnel Certigna. La protection de la confidentialité et de l'intégrité des journaux d'événements est assurée par le contrôle d'accès logique ainsi que par l'utilisation d'outil de scellement des fichiers.

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. Le contrôleur se fait assister si besoin par une personne disposant des compétences liées aux différents environnements utilisés.

Les pratiques mises en œuvre sont décrites plus en détails dans la « [Procédure de journalisation](#) ».

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 à minima sept ans et 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 à compter de l'acceptation du certificat par le RC. Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat peut être présenté par l'AC lors de toute sollicitation par les autorités habilitées. Ce dossier, complété par les mentions consignées par l'AE ou le MC, doit permettre de retrouver l'identité réelle du RC 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 cette AC et l'AC Racine, sont archivés pendant au moins sept ans après leur expiration.

Les réponses OCSP produites sont archivées pendant au moins trois mois après leur expiration. Les réponses sont détruites automatiquement après cette durée.

Journaux d'événements

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

Les archives sont conservées en plusieurs exemplaires grâce au processus de réplication entre les centres de production, ce qui assure la protection et la disponibilité des informations. Les archives électroniques sont effacées (Processus périodique) une fois leur période de conservation passée.

Les dossiers de demande papier sont physiquement détruits. Au-delà des 11 premières années d'exploitation de l'AC, une procédure manuelle d'effacement des archives est exécutée sur les différents centres de production.

5.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives sont protégées en intégrité. Elles peuvent être relues et exploitées par les membres dédiés de l'AC. L'accès en écriture à ces fichiers est protégé (gestion des droits). L'accès en lecture à ces journaux 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 réplication garantit l'existence d'une copie de secours de l'ensemble des archives.

Pour pallier l'impossibilité de réplication entre les sites de production, des sauvegardes quotidiennes 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

L'archivage est réalisé sur des serveurs d'archivage qui assurent la disponibilité, l'intégrité et la confidentialité des archives.

La « [Procédure de sauvegarde](#) » et la « [Procédure d'archivage](#) » décrivent les mesures mises en œuvre.

5.5.7. Procédures de récupération et de vérification des archives

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

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

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

5.6.1. Clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela, la période de validité du certificat de l'AC doit être supérieure à celle des certificats qu'elle signe. Au regard de la date de fin de validité de ce certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'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.

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

La « [Procédure de gestion des clés cryptographiques](#) » et le document de « [Suivi des clés](#) » décrivent les mesures mises en œuvre.



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 des Plans de Continuité d'Activité. En particulier pour les risques majeurs identifiés, ces plans abordent 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 les deux sites de production.

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

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

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

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

- Informera tous les RC et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;
- Révoquera tout certificat concerné.

La « [Procédure de gestion des incidents](#) » et les « [Plans de continuité d'activité](#) » décrivent les mesures mises en œuvre.

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 3 ans.

La « [Procédure de gestion des incidents](#) » et les « [Plans de continuité d'activité](#) » décrivent en détails les dispositions mises en œuvre.



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. De même, tous les certificats serveurs en cours de validité émis par cette AC seront révoqués.

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

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

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

La « [Procédure de gestion des clés cryptographiques](#) », la « [Procédure de gestion des incidents](#) » et les « [Plans de continuité d'activité](#) » décrivent les mesures mises en œuvre.

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.

L'AC utilise la redondance de ses systèmes d'informations sur plusieurs sites et ses plans de continuité d'activités pour assurer la continuité des services.

Les mesures sont décrites dans les « [Plans de continuité d'activité](#) ».

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 PC ;
- Elle prévient les RC dans le cas où les changements envisagés peuvent avoir des répercussions sur les engagements pris et ce, au moins sous le délai de 1 mois ;
- Elle communique aux responsables d'applications 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 de l'ANSSI est averti (<http://www.ssi.gouv.fr>). L'AC l'informerait notamment de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus de transfert ou de cessation d'activité.

La « [Procédure de gestion des incidents](#) » et les « [Plans de continuité d'activité](#) » décrivent en détails les dispositions mises en œuvre.

Cessation d'activité affectant l'AC

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

- Elle informe tous les RC, les autres composantes de l'IGC et les tiers par mail de la cessation d'activité. Cette information sera relayée également directement auprès des entités et le cas échéant de leur MC ;
- Elle révoque tous les certificats qu'elle a signés et qui sont encore valides ;
- Elle révoque son certificat ;
- Elle détruit la clé privée stockée dans le module cryptographique, ainsi que le contexte du module. Les porteurs de secret (clé privée et contexte) sont convoqués et détruisent leur(s) part(s) de secret. L'AC 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, l'AC 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, l'AC 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 l'ANSSI (<http://www.ssi.gouv.fr>) est immédiatement informé en cas de cessation d'activité de l'AC.

La « [Procédure de gestion des incidents](#) » et les « [Plans de continuité d'activité](#) » décrivent en détails les dispositions mises en œuvre.



6. Mesures de sécurité techniques

6.1. Génération et installation de bi-clés

6.1.1. Génération des bi-clés

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

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé (cf. chapitre 5). Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du 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, dans le cadre de « cérémonies de clés ».

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 ces dernières. Ces secrets sont des parties de la clé privée de l'AC décomposée suivant un schéma à seuil de Shamir.

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

Les scripts de cérémonie des clés ainsi que la répartition des parts de secrets sont suivis et documentés. La « [Procédure de gestion des clés cryptographiques](#) » et la « [Procédure de gestion des HSM](#) » décrivent les mesures mises en œuvre.

Clés générées par le RC

Le RC s'engage de manière contractuelle, en acceptant les conditions générales d'utilisation, à :

- Générer la clé privée dans un dispositif conforme aux exigences du chapitre 11.
- 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 et se réserve le droit de refuser la demande de certificat s'il était avéré que ce dispositif ne réponde pas à ces exigences.



Clés générées par l'AC

La génération des clés des porteurs s'effectue dans un dispositif conforme aux exigences du chapitre 11.

6.1.2. Transmission de la clé privée à son propriétaire

La clé privée est générée par l'Autorité d'enregistrement ou le RC et est transmise de manière sécurisée.

Dans le cas où la clé privée est générée par l'AC, la clé privée et/ou les données d'activation sont récupérées de manière sécurisée par le RC depuis son espace client et après authentification de ce dernier.

Une fois le certificat délivré, l'AC ne conserve ni ne duplique la clé privée.

6.1.3. Transmission de la clé publique à l'AC

Si la bi-clé n'est pas générée par l'AC, la demande de certificat (format PKCS#10), contenant la clé du serveur, est transmise à l'AC par le RC. 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 la PC, est effectuée par un moyen garantissant intégrité et authentification de cette clé publique.

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

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

6.1.5. Taille des clés

Clés d'AC

- AC Racine : bi-clé RSA 4096 bits / Algorithme de hachage SHA-256 (256 bits)
- AC Intermédiaire : bi-clé RSA 4096 bits / Algorithme de hachage SHA-256 (256 bits)

Clés serveurs

Bi-clé RSA 2048 bits / Algorithme de hachage 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. Dans le cadre de l'utilisation du RSA, la valeur de l'exposant public est un nombre impair supérieur ou égal à 3.

Clés d'AC

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

Clés serveurs

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

6.1.7. Objectifs d'usage de la clé

Clés d'AC

L'utilisation de la clé privée de l'AC et du certificat associé est exclusivement limitée à la signature de certificats et de LCR (cf. chapitre 1.4.5).

Clés serveurs

L'utilisation de la clé privée du serveur/service applicatif et du certificat associé est exclusivement limitée au service d'authentification du serveur (cf. chapitre 1.4.5).

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 Racine et l'AC pour la génération et la mise en œuvre de leurs clés de signature sont conformes aux exigences du chapitre 10.

Les modules cryptographiques utilisés sont des BULL Trustway Proteccio. La « [Procédure de gestion des HSM](#) » décrit plus en détails les dispositions mises en œuvre.

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

Dispositifs de protection des clés privées des serveurs

Le dispositif utilisé par l'AC ou le RC pour protéger la clé privée est conforme avec les exigences du chapitre 11.



Dans le cas où l'AC fournit le dispositif au RC, directement ou indirectement, l'AC s'assure que :

- La préparation du dispositif est contrôlée de façon sécurisée ;
- Le dispositif est stocké et distribué de façon sécurisée ;
- La désactivation et réactivation du dispositif est contrôlée de façon sécurisée.

6.2.2. Contrôle de la clé privée par plusieurs personnes

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

La « [Procédure de gestion des HSM](#) » et la « [Procédure de gestion des clés cryptographiques](#) » décrivent les mesures mises en œuvre.

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 ne sont jamais séquestrées.

6.2.4. Copie de secours de la clé privée

Clé d'AC

La clé privée de l'AC fait l'objet de copies de secours :

- Dans un second module cryptographique conforme aux exigences du chapitre 10.
- En dehors du module cryptographique sous la forme de parts de secret chiffrées par le module cryptographique et réparties entre plusieurs porteurs dans un rôle de confiance.

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 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 la clé privée de l'AC.

Clés serveurs

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



Pour les clés privées générées sur module cryptographique, 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 RC.

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

6.2.7. Stockage de la clé privée dans un module cryptographique

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

La « [Procédure de gestion des HSM](#) » et la « [Procédure de gestion des clés cryptographiques](#) » décrivent plus en détails les dispositions mises en œuvre.

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 « [Procédure de gestion des HSM](#) » et la « [Procédure de gestion des clés cryptographiques](#) » décrivent plus en détails les dispositions mises en œuvre.

Clés des serveurs

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

6.2.9. Méthode de désactivation de la clé privée

Clés d'AC

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

La désactivation d'une clé privée d'AC qui ne doit plus être opérationnelle est réalisée via la suppression de cette clé dans le module cryptographique. Dans le cas où le module cryptographique est dédié à cette clé, le module peut alors être éteint afin de désactiver cette clé.



Clés des 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.

Les mesures mises en œuvre sont décrites dans la « [Procédure de gestion des clés cryptographiques](#) ».

Clés des serveurs

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

6.2.11. Niveau d'évaluation sécurité du module cryptographique

Le niveau d'évaluation du module cryptographique de l'AC est précisé au chapitre 10.
Le niveau d'évaluation du dispositif du RC est 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 ont une durée de validité de 825 jours maximum en fonction du contrat souscrit.

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

La « [Procédure de gestion des HSM](#) » et la « [Procédure de gestion des clés cryptographiques](#) » décrivent plus en détails les dispositions mises en œuvre

[Génération et installation des données d'activation correspondant à la clé privée du serveur](#)

Le RC définit depuis l'espace client la donnée qui permettra de chiffrer directement la bi-clé générée. Cette donnée d'activation n'est pas conservée par l'AC.

Une fois les données d'activation personnalisée par le RC, l'AE n'en n'ayant pas connaissance, ne peut plus les renvoyer. Si le RC génère lui-même son bi-clé, il génère de manière autonome et sous sa seule responsabilité ses données d'activation.

6.4.2. Protection des données d'activation

[Protection des données d'activation correspondant à la clé privée de l'AC](#)

Les données d'activation sont directement remises aux porteurs lors des cérémonies des clés. Leurs conditions de stockage assurent leur disponibilité, leur intégrité et leur confidentialité.

Les secrets sont stockés dans des dispositifs à l'accès limité, dans des enveloppes sécurisées permettant de détecter toute ouverture non autorisée et tracée.

La « [Procédure de gestion des HSM](#) » et la « [Procédure de gestion des matériels](#) » décrivent les mesures mises en œuvre.

[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 RC, ces données d'activation ne sont pas sauvegardées par l'AE et sont modifiées par le RC lors de l'acceptation du certificat.

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

6.4.3. Autres aspects liés aux données d'activation

Sans objet.



6.5. Mesures de sécurité des systèmes informatiques

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

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

- Identification et authentification forte des utilisateurs pour l'accès au système (contrôle d'accès physique pour entrer dans la salle + contrôle logique par identifiant / mot de passe ou par certificat pour accéder au système) ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) ;
- Protection contre les virus informatiques et toutes formes de logiciel compromettant ou non autorisé et mises à jour des logiciels à l'aide du firewall ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Protection du réseau contre toute intrusion d'une personne non autorisée à l'aide du firewall ;
- Communication sécurisée inter-sites (tunnel VPN IP Sec) ;
- 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 « [Politique de sûreté](#) », la « [Politique de contrôle d'accès logiques](#) », la « [Charte de sécurité](#) », la « [Procédure de gestion des firewalls](#) » décrivent les mesures mises en œuvre.

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. Ces dispositions sont décrites en détails dans le « [Guide de développement](#) ».

La configuration des systèmes de l'AC ainsi que toute modification et mise à niveau sont documentées. Le développement est effectué dans un environnement contrôlé et sécurisé exigeant un niveau élevé d'autorisation.

Afin de permettre à ses prospects ou futurs clients de tester ou d'évaluer certaines de leurs applications d'échange dématérialisé, l'AC a mise 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. Les certificats émis ont une utilisation restreinte à des fins de test exclusivement.

Les solutions Certigna sont testées en premier lieu au sein d'un environnement de développement/test avant d'être utilisées dans l'environnement de production. Les environnements de production et de développement sont dissociés.

La description du contexte d'évolution de l'IGC est définie dans la « [Procédure de mise à jour de la plate-forme technique](#) ».

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](#) ».

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) sur chaque site et 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.

La « [Procédure de gestion des firewalls](#) », la « [Procédure de gestion de la supervision](#) » et la « [Politique de contrôle d'accès logiques](#) » décrivent en détails les dispositions mises en œuvre.

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.

La « [Procédure de synchronisation des horloges](#) » décrit les mesures mises en œuvre.

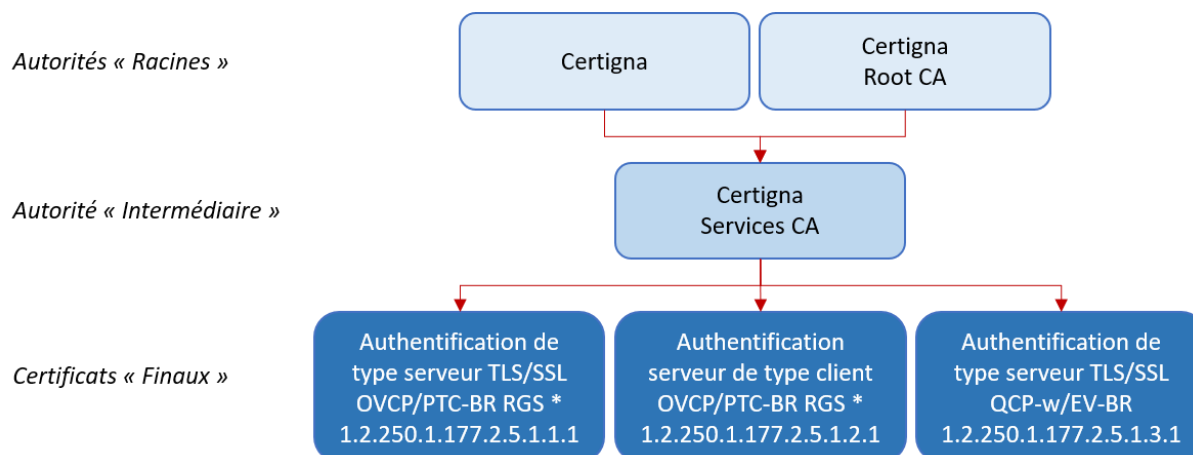


7. Profils des certificats et des LCR

Les certificats et les LCR produits par l'AC sont conformes au standard ITU-T Recommandation X.509 version 3 et à la RFC 5280. Les profils sont fournis au chapitre 7 de la Politique de Certification associée.

7.1. Hiérarchie de confiance

La hiérarchie de confiance est composée des autorités et certificats suivants :



7.2. Profils des certificats des Autorités Racines

Ces profils sont décrits dans les Politiques de Certification associées aux Autorités Racines et disponibles à l'adresse suivante : <https://www.certigna.fr/autorites/>

7.3. Pré-certificats

Dans le cadre de l'implémentation des exigences de la RFC 6962 relative au « Certificate Transparency », l'AC émet des pré-certificats. Ces derniers ne sont pas considérés comme des certificats assujettis aux exigences de la RFC 5280 et de la présente PC, et ne sont utilisés que pour l'obtention de SCT à intégrer dans l'extension des certificats émis et contenant des FQDN. Nous vous invitons à consulter la RFC 6962 pour plus de renseignements sur ce dispositif. Les SCT sont collectés à minima auprès des journaux suivants :

- ct.googleapis.com/rocketeer
- ct.googleapis.com/logs/xenon20XX (où 20XX est l'année d'expiration du certificat)
- mammoth.ct.comodo.com
- yeti20XX.ct.digicert.com (où 20XX est l'année d'expiration du certificat)



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 et du règlement européen eIDAS et, d'autre part, ceux que réalise ou fait réaliser l'AC afin de s'assurer que l'ensemble de son IGC est bien conforme à ses engagements affichés dans la PC et aux pratiques identifiées dans la DPC correspondante.

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 cette PC et les pratiques correspondantes.

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 par l'AC à minima une fois tous les trois ans. Les audits de qualification sont réalisés chaque année.

La « [Procédure de gestion des audits](#) » et le « [Programme d'audit](#) » décrivent plus en détails les dispositions mises en œuvre.

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.

Les audits internes sont réalisés par les personnes dans le rôle de confiance de « Contrôleur ». Des contrôles périodiques sont également réalisés par les responsables sécurité.

8.3. Relations entre évaluateurs et entités évaluées

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

Concernant les audits de certification/qualification, l'entité intervenant est externe et indépendante.

Concernant les audits internes, la sélection des auditeurs et rôles de confiance est décrite plus en détails dans le document « [Rôles, responsabilités et autorités](#) » et dans la « [Procédure de gestion des audits](#) ».



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](#) » décrit plus en détails les mesures mises en œuvre.

Durant la période au cours de laquelle l'AC émet des certificats, l'AC surveille l'adhésion aux exigences de sa PC et de sa DPC et contrôle strictement sa qualité de service en effectuant des audits à minima trimestriels sur un échantillon sélectionné au hasard d'au moins trois pourcents des dossiers de demande, et six pourcents des dossiers traités par des AED au cours de la période commençant immédiatement après la prise de l'échantillon de l'audit précédent.

L'AC contrôle strictement la qualité du service des certificats délivrés ou contenant des informations vérifiées par un tiers délégué en demandant à un spécialiste de la validation employé par l'AC d'effectuer des vérifications trimestrielles en cours sur un échantillon sélectionné au hasard d'au moins trois pour cent des Certificats vérifiés par le tiers délégué dans la période commençant immédiatement après la prise du dernier échantillon. L'autorité de certification examinera les pratiques et les procédures de chaque tiers délégué afin de s'assurer que le tiers délégué est en conformité avec les exigences de cette PC et de la DPC associée.

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 de 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 l'équipe d'audit sont tenus à la disposition de l'organisme en charge de la qualification de l'AC.



9. Autres problématiques métiers et légales

9.1. Tarifs

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

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

9.1.2. Tarifs pour accéder aux certificats

Sans objet.

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

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

9.1.4. Tarifs pour d'autres services

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

L'AC 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 RC à des tiers dans le cadre de procédures légales. Elle donne également accès à ces informations au RC, MC et le cas échéant à l'opérateur d'AED en relation avec le RC.

La « [Politique de classification et de manipulation de l'information](#) », la « [Procédure de gestion des matériels](#) » ainsi que la « [Politique d'archivage](#) » décrivent plus en détails les dispositions mises en œuvre.

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 n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée et au règlement européen « 2016/679/ UE du 27 Avril 2016 » relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, vous bénéficiez d'un droit d'accès, d'opposition, de rectification, de suppression et de portabilité de vos données personnelles. Vous pouvez exercer votre droit en vous adressant par e-mail à : privacy@dhimyotis.com, ou par courrier à l'adresse suivante :

DHIMYOTIS, Service du DPO,
20 Allée de Râperie, 59 650 Villeneuve d'Ascq, France

Votre demande devra indiquer votre nom et prénom, adresse e-mail ou postale, être signée et accompagnée d'un justificatif d'identité en cours de validité.

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 RC, des opérateurs d'AED et des MC.

9.4.3. Informations à caractère non personnel

Sans objet.

9.4.4. Responsabilité en termes de protection des données personnelles

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

9.4.5. Notification et consentement d'utilisation des données personnelles

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

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

La divulgation des informations confidentielles n'est effectuée qu'aux autorités judiciaires ou administratives habilitées officiellement et exclusivement sur leur demande expresse en conformité avec la législation française.



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

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

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 RC 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 RC sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un RC et l'AC est formalisée par un lien contractuel / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.
- Mettre en œuvre et suivre, lors de la délivrance d'un certificat, les exigences décrites aux chapitres 3.2 et 3.3 de la présente PC pour vérifier que le RC a le droit d'utiliser ou de contrôler le(s) nom(s) de domaine indiqué(s) dans les champs « commonName » et « subjectAltName » du certificat (ou uniquement dans le cas où les droits d'utilisation ou



de contrôle des noms de domaine ont été délégués par une personne disposant de ces droits).

- Mettre en œuvre et suivre, lors de l'émission d'un certificat, les exigences décrites au chapitre 3.2 et 3.3 pour vérifier que l'organisation rattachée au serveur a autorisé la délivrance du certificat, et que le RC est autorisé à demander le certificat au nom de l'organisation.
- Mettre en œuvre et suivre, lors de l'émission d'un certificat, les exigences décrites au chapitre 3.2 et 3.3 pour vérifier que les informations contenues dans le certificat sont exactes.
- Mettre en œuvre et suivre, lors de l'émission d'un certificat, les exigences décrites au chapitre 3.2 et 3.3 pour vérifier l'identité de l'organisation, de son représentant et du RC désigné.
- Si l'AC et l'organisation qui demande le certificat ne sont pas affiliées, ces parties s'engagent sur un accord de souscription juridiquement valide et exécutoire ;
- Si l'AC et l'organisation qui demande le certificat sont la même entité ou sont affiliées, le représentant de l'organisation qui demande le certificat a reconnu les conditions d'utilisation.
- Mettre à disposition du public 24h/24, 7j/7 les informations sur l'état (valide ou révoqué) des certificats non expirés ;
- Révoquer un certificat pour l'une des raisons spécifiées au chapitre 4.9 de la présente PC.

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

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

9.6.2. Service d'enregistrement

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

9.6.3. Responsable du Certificat

Le RC a le devoir de :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;



- Protéger la clé privée du 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 RC et l'AC ou ses composantes est formalisée par un engagement du RC visant à certifier l'exactitude des renseignements et des documents fournis.

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

9.6.4. Utilisateurs de certificats

Les tiers utilisateurs doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Pour chaque certificat de la chaîne de certification, du certificat du serveur jusqu'à l'AC racine, 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 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 l'AC ne saurait être tenue pour responsable, ni d'un dommage résultant d'une faute ou négligence d'un accepteur et/ou des RC, ni d'un dommage causé par un fait extérieur, notamment en cas de :

- Utilisation d'un certificat pour une autre application que les applications définies au chapitre 1.5.1 de la 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 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

L'AC a notamment souscrit un contrat « Responsabilité civile après livraison ».

L'AC comprends et reconnaît que les fournisseurs de logiciels d'application avec lesquels un accord de distribution du certificat d'AC racine est mise en œuvre n'assument aucune obligation ou responsabilité potentielle de l'AC ou qui autrement pourrait exister en raison de la délivrance ou de la maintenance de certificats ou de la dépendance de ceux-ci par des tiers de confiance ou autres.

L'AC défend, indemnise et couvre chaque fournisseur de logiciels d'application pour toutes les réclamations, dommages et pertes subis par ce fournisseur en rapport avec un certificat délivré par l'AC, quelle que soit la cause d'action ou la théorie juridique impliquée.

Toutefois, cela ne s'applique pas à toute réclamation, dommage ou perte subi par ce fournisseur de logiciel d'application lié à un certificat délivré par l'AC où une telle réclamation, dommage ou perte a été directement causée par le logiciel de ce fournisseur de logiciels d'application affichant un certificat qui est toujours valide comme pas digne de confiance ou affichant comme digne de confiance un certificat qui a expiré ou un certificat qui a été révoqué (mais seulement dans les cas où le statut de révocation est actuellement disponible en ligne auprès de l'AC et que le logiciel d'application a échoué dans la vérification de ce statut ou a ignoré une indication de l'état révoqué).

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 la PC.

9.10.2. Fin anticipée de validité

La publication d'une nouvelle version des documents cités au chapitre 1.1 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 citées au chapitre 1.1.

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. Une révision et mise à jour si nécessaire de la PC et DPC sont effectuées à minima 1 fois par an.

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

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

9.13. Dispositions concernant la résolution de conflits

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



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

9.14. Juridictions compétentes

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

9.15. Conformité aux législations et réglementations

La présente DPC est soumise au droit français et aux textes législatifs applicables à la présente PC.

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.

En cas de conflit entre les exigences de cette PC et une loi, un règlement ou une ordonnance gouvernementale (ci-après la « Loi ») de toute juridiction dans laquelle l'AC exploite ou émet des certificats, l'AC peut modifier toute exigence contradictoire dans la mesure du possible afin que l'exigence soit valide et légale dans la juridiction. Cela s'applique uniquement aux opérations ou aux émissions de certificats qui sont assujetties à cette Loi. Dans un tel cas, l'AC inclura immédiatement dans cette section (et avant de délivrer un certificat en vertu de l'exigence modifiée) une référence détaillée à la Loi exigeant une modification des exigences et les modifications spécifiques apportées à ces exigences par l'AC.

L'AC notifiera le CA/Browser Forum et l'ANSSI (avant de délivrer un certificat en vertu de l'exigence modifiée) des informations pertinentes nouvellement ajoutées à cette PC. Concernant le CA/Browser Forum, un message sera envoyé à questions@cabforum.org (ou à d'autres adresses et liens électroniques que le Forum peut désigner) donnant lieu à une confirmation.

Toute modification des exigences et pratiques de l'AC autorisées en vertu de cette section est interrompue si la Loi ne s'applique plus, ou que ces exigences sont modifiées pour permettre de se conformer à ces dernières et à la loi simultanément. Une modification appropriée des



pratiques, de la PC et DPC de l'AC, et la notification au CA/Browser Forum sont effectuées sous 90 jours.

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 ;
- Être capable d'identifier et d'authentifier ses utilisateurs ;
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- Être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Permettre de créer une signature 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 ;

10.2. Exigences sur la qualification

Le module cryptographique utilisé par l'AC doit être :

- Qualifié au niveau « renforcé » par l'ANSSI selon le processus décrit dans le RGS ;
- Certifié Critères Communs au niveau EAL4+ ou FIPS 140-2 Level 3.



11. Annexe 2 : exigences de sécurité du dispositif de d'authentification du serveur

11.1. Exigences sur les objectifs de sécurité

Le dispositif 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 de la bi-clé générée ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Générer une authentification qui ne peut être falsifiée 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 régénération de la clé privée ;
- Garantir la confidentialité et l'intégrité de la clé privée ;
- 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, d'une part, la fonction d'authentification et, d'autre part, la fonction de déchiffrement de clés symétriques de session, et protéger la clé privée contre toute utilisation par des tiers ;
- Permettre de garantir l'authenticité et l'intégrité de la clé symétrique de session, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données.

11.2. Exigences sur la qualification

Niveau qualifié/EV

Le dispositif de protection des clés privées fourni par l'AC ou utilisé par le RC est une solution matérielle ou logicielle respectant les exigences du chapitre 11.1.

RGS *

Le dispositif de protection des clés privées fourni par l'AC ou utilisé par le RC est :

- Soit un dispositif matériel de type carte à puce ou module cryptographique qualifié par l'ANSSI ;
- Soit une solution logicielle respectant les exigences du chapitre 11.1 via la mise en place de mesures de sécurité additionnelles propres à l'environnement dans lequel est déployée la clé privée. Cet environnement dans lequel est déployée la clé privée doit avoir fait l'objet d'un audit de sécurité.