PC/DPC

POLITIQUE DE CERTIFICATION / DÉCLARATION DES PRATIQUES DE CERTIFICATION

CERTIGNA TLS

AUTHENTIFICATION DE SERVEUR WEB

Edité le :	11/06/2026	
Version :	2.2	
OID :	1.2.250.1.177.1.0.1	CERTIGNA
	1.2.250.1.177.2.0.1	CERTIGNA ROOT CA
	1.2.250.1.177.6.0.1.1	CERTIGNA SERVER AUTHENTICATION ROOT CA
	1.2.250.1.177.14.0.1.1	CERTIGNA SERVER AUTHENTICATION EU ROOT CA
Classification :	Publique	

SOMMAIRE

1 INTRODUCTION 5

1.1 Présentation générale 5

1.2 Nom et identification du document 6

1.3 Entités intervenant dans l'IGC 9

1.4 Usage des certificats 13

1.5 Gestion de la PC 14

1.6 Définitions et acronymes 16

2 RESPONSABILITE CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS 23

2.1 Publication 23

2.2 Publication des informations de certification 23

2.3 Délais et fréquences de publication 26

2.4 Contrôle d'accès aux informations publiées 27

3 IDENTIFICATION ET AUTHENTIFICATION 28

3.1 Nommage 28

3.2 Validation initiale de l'identité 29

3.3 Identification et authentification d'une demande de renouvellement des clés 49

3.4 Identification et authentification d'une demande de révocation 50

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS 51

4.1 Demande de certificat 51

4.2 Traitement d'une demande de certificat 52

4.3 Délivrance du certificat 55

4.4 Acceptation du certificat 56

4.5 Usages de la bi-clé et du certificat 57

4.6 Renouvellement d'un certificat 58

4.7 Délivrance d'un nouveau certificat suite au changement du bi-clé 59

4.8 Modification du certificat 60

4.9 Révocation et suspension des certificats 61

4.10 Fonction d'information sur l'état des certificats 70

4.11 Fin de la relation entre le RC et l'AC 71

4.12 Séquestre de clé et recouvrement 71

5 MESURES DE SECURITE NON TECHNIQUES 72
5.1 Mesures de sécurité physique 73
5.2 Mesures de sécurité procédurales 75
5.3 Mesures de sécurité vis-à-vis du personnel 77
5.4 Procédures de constitution des données d'audit 79
5.5 Archivage des données 83
5.6 Renouvellement d'une clé de composante de l'IGC 85
5.7 Reprise suite à compromission et sinistre 85
5.8 Fin de vie de l'IGC 89

6 MESURES DE SECURITE TECHNIQUES 91
6.1 Génération et installation de bi-clés 91
6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques 95
6.3 Autres aspects de la gestion des bi-clés 98
6.4 Données d'activation 99
6.5 Mesures de sécurité des systèmes informatiques 100
6.6 Mesures de sécurité des systèmes durant leur cycle de vie 100
6.7 Mesures de sécurité réseau 101
6.8 Horodatage et Système de datation 101

7 PROFIL DES CERTIFICATS ET DES LCR 102
7.1 Profils des certificats 102
7.2 Profils des LCR 137
7.3 Profils des OCSP 141

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS 145
8.1 Fréquences et/ou circonstances des évaluations 145
8.2 Identités/qualifications des évaluateurs 145
8.3 Relations entre évaluateurs et entités évaluées 146
8.4 Sujets couverts par les évaluations 146
8.5 Actions prises suite aux conclusions des évaluations 146
8.6 Communication des résultats 147
8.7 Audits internes 147

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES 149

9.1 Tarifs 149
9.2 Responsabilité financière 150
9.3 Confidentialité des données professionnelles 150
9.4 Protection des données personnelles 151
9.5 Droits sur la propriété intellectuelle et industrielle 153
9.6 Interprétations contractuelles et garanties 153
9.7 Livraison et garantie 157
9.8 Limite de responsabilité 158
9.9 Indemnités 159
9.10 Durée et fin anticipée de validité de la PC 159
9.11 Notifications individuelles et communications entre les participants 160
9.12 Amendements à la PC 160
9.13 Dispositions concernant la résolution de conflits 161
9.14 Juridictions compétentes 162
9.15 Conformité aux législations et réglementations 162
9.16 Dispositions diverses 162
9.17 Autres dispositions 163

10 ANNEXE 1 : EXIGENCE DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC 164
10.1 Exigences sur les objectifs de sécurité 164
10.2 Exigences sur la qualification 164

11 ANNEXE 2 : EXIGENCES DE SÉCURITÉ DU DISPOSITIF UTILISÉ PAR LE SERVEUR 165
11.1 Exigences sur les objectifs de sécurité 165
11.2 Exigences sur la qualification 165

1 INTRODUCTION

1.1 Présentation générale

CERTIGNA, anciennement DHIMYOTIS, est une société du groupe TESSI qui est spécialisée dans la fourniture de services de confiance numérique.

CERTIGNA s'est dotée de plusieurs autorités de certifications (AC) pour délivrer des certificats électroniques à des personnes morales et des personnes physiques. Ce document est la Politique de Certification/Déclaration des Pratiques de certification (PC/DPC) que CERTIGNA applique et s'engage à respecter dans le cadre de la fourniture de son service de certification électronique. L'attention du lecteur est attirée sur le fait que la compréhension de la présente PC/DPC suppose qu'il soit familiarisé avec les notions liées à la technologie des Infrastructures de Gestion de Clés (IGC).

CERTIGNA est audité par l'organisme de certification français LSTI. L'état des qualifications et certifications des produits de CERTIGNA peut être consulté depuis les sites suivants :

- Qualifications RGS et certifications ETSI : Lien vers le site de LSTI
- Qualifications eIDAS : Lien vers la TSL Européenne

La présente PC/DPC vise la conformité aux exigences suivantes :

- aux « Baseline Requirements documents (SSL/TLS Server Certificates) » et aux « EV Guidelines for TLS Server certificate » en vigueur du CA/Browser Forum : http://www.cabforum.org ;
- aux dernières versions des politiques du CCADB et des navigateurs :
  - à la CCADB Policy : Lien vers la politique
  - à la Mozilla Root Store Policy : Lien vers la politique
  - à la Microsoft Trusted Root Program : Lien vers la politique
  - à la Chrome Root Program Policy : Lien vers la politique
  - à la Apple Root Certificate Program : Lien vers la politique
- aux standards et niveaux de sécurité suivants :

[AC RACINE] CERTIGNA SERVER AUTHENTICATION ROOT CA				
[AC] CERTIGNA SERVER AUTHENTICATION OVCP CA		RGS	ETSI	RSA
Authentification serveur	1.2.250.1.177.6.4.1.1.1		EN 319 411-1 OVCP	>=2048
[AC] CERTIGNA SERVER AUTHENTICATION AUTO OVCP CA		RGS	ETSI	RSA
Authentification serveur Auto	1.2.250.1.177.6.5.1.1.1		EN 319 411-1 OVCP	>=2048
[AC] CERTIGNA SERVER AUTHENTICATION QCP CA		RGS	ETSI	RSA
Authentification serveur	1.2.250.1.177.6.6.1.1.1		EN 319 411-2 QNCP-w	>=2048
[AC] CERTIGNA SERVER AUTHENTICATION AUTO QCP CA		RGS	ETSI	RSA
Authentification serveur Auto	1.2.250.1.177.6.7.1.1.1		EN 319 411-2 QNCP-w	>=2048

[AC RACINE] CERTIGNA SERVER AUTHENTICATION EU ROOT CA				
[AC] CERTIGNA SERVER AUTHENTICATION OVCP EU CA		RGS	ETSI	RSA
Authentification serveur	1.2.250.1.177.14.1.1.1.1	*	EN 319 411-1 OVCP	>=2048
[AC] CERTIGNA SERVER AUTHENTICATION AUTO OVCP EU CA		RGS	ETSI	RSA
Authentification serveur Auto	1.2.250.1.177.14.2.1.1.1	*	EN 319 411-1 OVCP	>=2048

[AC RACINE] CERTIGNA & CERTIGNA ROOT CA				
[AC] CERTIGNA SERVICES CA		RGS	ETSI	RSA
Authentification serveur	1.2.250.1.177.2.5.1.1.1	*	EN 319 411-1 OVCP	2048
Authentification serveur	1.2.250.1.177.2.5.1.1.2	*	EN 319 411-1 OVCP	>=3072
~~Authentification serveur~~	~~1.2.250.1.177.2.5.1.3.1~~		~~EN 319 411-2 QEVCP-w~~	~~2048~~
~~Authentification serveur~~	~~1.2.250.1.177.2.5.1.4.1~~		~~EN 319 411-2 QEVCP-w DSP2~~	~~2048~~
~~Authentification serveur~~	~~1.2.250.1.177.2.5.1.4.2~~		~~EN 319 411-2 QEVCP-w DSP2~~	~~3072~~
Authentification serveur	1.2.250.1.177.2.5.1.5.1		EN 319 411-2 QNCP-w	2048
Authentification serveur	1.2.250.1.177.2.5.1.5.2		EN 319 411-2 QNCP-w	>=3072
[AC] CERTIGNA SERVER AUTHENTICATION OVCP EU CA G1		RGS	ETSI	RSA
Authentification serveur	1.2.250.1.177.1.23.1.1.1	*	EN 319 411-1 OVCP	>=3072
[AC] CERTIGNA WILD CA		RGS	ETSI	RSA
Authentification serveur	1.2.250.1.177.2.7.1.1.1		EN 319 411-1 OVCP	2048
Authentification serveur	1.2.250.1.177.2.7.1.1.2		EN 319 411-1 OVCP	>=3072
Authentification serveur Wildcard	1.2.250.1.177.2.7.1.2.1		EN 319 411-1 OVCP	2048
Authentification serveur Wildcard	1.2.250.1.177.2.7.1.2.2		EN 319 411-1 OVCP	>=3072
[AC] CERTIGNA SERVER AUTHENTICATION OVCP CA G1		RGS	ETSI	RSA
Authentification serveur	1.2.250.1.177.1.22.1.1.1		EN 319 411-1 OVCP	>=2048

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

Cette PC/DPC est disponible aux formats PDF et Markdown. La version de la PC/DPC au format PDF est la version de référence.

Les certificats TLS couverts par la présente PC/DPC ne seront officiellement plus reconnus par l'ensemble des navigateurs web à compter du 15/09/2026.

1.2 Nom et identification du document

La présente PC/DPC peut être identifiée par plusieurs OID liés aux AC racines regroupées dans ce document :

- 1.2.250.1.177.1.0.1 CERTIGNA
- 1.2.250.1.177.2.0.1 CERTIGNA ROOT CA
- 1.2.250.1.177.6.0.1.1 CERTIGNA SERVER AUTHENTICATION ROOT CA
- 1.2.250.1.177.14.0.1.1 CERTIGNA SERVER AUTHENTICATION EU ROOT CA

Les certificats d'AC intermédiaires et finaux délivrés sous chaque AC racine disposent également d'un OID permettant d'identifier clairement les pratiques de cette PC/DPC qui lui sont applicables.

1.2.1 Révision du document

Cette PC/DPC est un regroupement de toutes les PC et DPC des différentes AC racines et intermédiaires utilisées pour l'émission de certificats d'authentification de serveur web. Afin de faciliter l'accès à l'information, il a été décidé de regrouper l'ensemble de ces documents en une seule PC/DPC. Le tableau ci-dessous présente l'historique des anciennes versions des PC et DPC regroupées dans ce document et consultables à la page suivante : https://www.certigna.com/autorite-crl.

Ver.	Date	Modifications apportées
1.0	05/04/2024	Création de cette PC dédiée aux AC d'authentification de serveur : - Intégration des nouvelles AC « SERVER AUTHENTICATION CA » - Intégration des AC historiques : o CERTIGNA et les certificats d'AC intermédiaires et finaux associés ; o CERTIGNA ROOT CA et les certificats d'AC intermédiaires et finaux associés.
1.1	25/06/2024	Révision du document et précisions apportées sur : - La durée d'utilisation des documents pour l'enregistrement (cf. 4.1.2.2) ; - L'acceptation des certificats en utilisant le service ACME (cf. 4.4.1.2) ; - L'acceptation des CVGU en utilisant le service ACME (cf. 4.5.1) ; - La durée de rétention des dossiers de demande (cf. 9.4.1) ; - Les obligations des RC, Porteurs et demandeurs (cf. 9.6.3 et 9.6.4) ; - L'usage des certificats de test (cf. 9.17.1).
1.2	12/07/2024	Révision du document et précisions apportées sur : - La méthode « Changement apporté au site web – ACME » (cf. 3.2.2.4.19)
1.3	13/09/2024	Révision du document et précisions apportées sur : - Les sections structurées en alignement avec la RFC 3647 ; - La vérification de l'existence opérationnelle de l'entité (cf. 3.2.2.1.3) ; - Les enregistrements CAA (Cf. 3.2.2.8) ; - L'identification et l'authentification sur renouvellement (cf. 3.3.1.2) ; - Le délai d'utilisation des validations (cf. 4.2.1.2) ; - L'AC n'émet pas de certificat avec un nouveau gTLD (cf. 4.2.2).
1.4	24/09/2024	Révision du document et précisions apportées sur : - Le retrait de la méthode d'email au contact du domaine (cf. 3.2.2.4.2) ; - L'ajout de la méthode d'email au contact DNS TXT (cf. 3.2.2.4.14) ; - La corroboration de l'émission multi-perspective (cf. 3.2.2.9).
1.5	19/03/2025	Regroupement de la PC et DPC dans un même document. Transfert des AC TLS des PC/DPC de « Certigna Root CA » dans ce document. Révision et précisions apportées sur : - L'ajout de nouveaux profils de certificats ; - Les journaux d'activité des routeurs et pare-feux SC69 (cf. 5.4.1.1) ; - Les clés faibles et compromises SC73 (cf. 6.1.1.3) ; - L'implémentation d'un processus de vérification SC75 (cf. 4.3, 6.6.1, 8.7) ; - La corroboration multi-perspectives SC67 (cf. 3.2.2.9, 5.4.1) ; - Le contenu du champ « OrganizationName » SC78 (cf. 3.2.2.2) ; - Les exigences sur l'OCSP SC76 (cf. 4.9.10) ; - La durée de conservation des dossiers de demande (cf. 5.5.2.1).
1.6	22/04/2025	Révision et précisions apportées sur : - Les profils de certificats d'authentification web RGS sous ACME (cf. 7.1.12.9, 7.1.12.10) ; - Le statut de révocation au-delà de la fin de validité (cf. 5.8.3) ; - La durée de conservation des dossiers de demande et journaux (cf. 5.5.2, 9.4.1).
1.7	20/05/2025	Révision et précisions apportées sur : - Le retrait des AC révoquées en mai 2025.
1.8	08/09/2025	Révision et précisions apportées sur : - La durée de validité des certificats et de réutilisation des données (cf. 4.2.1, 6.3.2) ; - L'usage du DNSSEC (cf. 3.2.2.4, 3.2.2.8.1) ; - La révocation massive de certificats (cf. 5.7.1.2).
1.9	18/09/2025	Révision et précisions apportées sur : - Création d'une version Markdown de la CP/CPS en version anglaise ; - Corrections typographiques.
2.0	12/12/2025	Révision et précisions apportées sur : - Conformité aux politiques du CCADB et des navigateurs (cf. 1.1) ; - Signature croisée de Certigna Root CA par l'AC racine Certigna (cf. 7).
2.1	11/03/2026	Révision et précisions apportées sur : - Les modalités d'accès aux serveurs de publication (cf. 2.4) ; - L'usage du DNSSEC (cf. 3.2.2.4) ; - L'usage des méthodes de contrôle de domaine (cf. 3.2.2.4.4 et 3.2.2.4.14) ;

		- Le délai maximal entre deux vérifications des configurations systèmes (cf. 6.5.1) ; - Le champ AIA des AC intermédiaires cross-signées (cf. 7.12.6 et 7.12.7) ; - La révocation des certificats d'AC en RSASSA-PKCS1-v1_5 avec SHA-1 (cf. 7.1.3.2.1).
2.2	11/06/2026	Révision et précisions apportées sur : - L'arrêt de reconnaissance des certificats TLS par les navigateurs (cf. 1.1) ; - L'ajout de la liste des références aux RFC (cf. 1.6.3) ; - L'ajout des nouvelles méthodes de contrôle (cf. 3.2.2.4.21, 3.2.2.4.22) ; - L'ajout de non-délivrance de certificat avec un suffixe de zone IP inversée (cf. 4.2.2) ; - Les raisons pour révoquer un certificat de personne morale (cf. 4.9.1.1) ; - La fréquence d'établissement des LCR (cf. 4.9.7) ; - Les exigences sur la vérification en ligne de la révocation (cf. 4.9.9) ; - Les mesures de sécurité techniques (cf. 5) ; - Type d'événements à enregistrer (cf. 5.4.1) ; - Retrait des certificats DSP2 non commercialisés et des références associées

1.3 Entités intervenant dans l'IGC

1.3.1 Autorité de certification

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

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

- Fonctions d'enregistrement et de renouvellement ;
- Fonction de génération des certificats ;
- Fonction de génération d'éléments secrets ;
- Fonction de publication des conditions générales, de la PC/DPC, 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 cette PC/DPC. 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 pourraient influer négativement sur la confiance dans les services fournis par l'AC. Les parties de l'AC concernées par la génération de certificats et de la gestion des révocations ont une structure documentée qui préserve l'impartialité des opérations.

1.3.2 Autorité d'enregistrement

L'AE assure les fonctions suivantes déléguées par l'AC, en vertu de la présente PC/DPC :

- La prise en compte et la vérification des informations du futur Responsable de Certificat (RC) ainsi que son 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 Mandataire de Certification (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 garde la responsabilité de ces fonctions ainsi que celle de l'archivage des pièces du dossier d'enregistrement (sous forme électronique et/ou papier).

Avant que l'AC autorise un tiers à assurer tout ou partie des fonctions de l'AE, l'AC s'assure que les exigences contractuelles avec ce tiers exigent notamment :

- Le respect des exigences de qualification du chapitre 5.3 de la présente PC/DPC lorsqu'applicables aux fonctions déléguées ;
- Le respect des exigences sur le maintien des archives du chapitre 5.5.2 de la présente PC/DPC ;
- Le respect des exigences de la présente PC applicables au tiers pour les fonctions qu'il assure ;
- Se conformer à la présente PC/DPC ou à la déclaration des pratiques de ce tiers dont l'AC a vérifié la conformité le cas échéant.

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 (MC) 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.

L'AC ne désigne pas d'AE tiers qui vérifient les demandes de certificats pour elle-même.

1.3.3 Demandeurs de certificats

Un demandeur est une personne physique rattachée ou non à l'entité désignée dans le certificat demandé, qui réalise la commande d'un ou plusieurs certificats pour lui-même ou au nom d'un Responsable de Certificat. Un demandeur est responsable des obligations incombant aux demandeurs, ainsi que celles incombant aux Responsables de Certificat le cas échéant.

1.3.4 Responsable de certificat

On parlera du « Responsable du certificat » (RC) lorsque le certificat délivré est destiné à un service applicatif ou à un serveur, tel qu'un service de cachet ou un serveur web. Le RC est la personne en charge de la gestion du certificat, mais n'est pas désigné explicitement dans ce certificat de personne morale.

Le RC doit respecter les conditions et obligations de cette PC/DPC et des CGVU.

1.3.4.1 Responsable du certificat d'une AC

Pour l'AC racine et les AC intermédiaires, le RC ne peut être que l'Autorité de Certification CERTIGNA.

1.3.4.2 Responsable du certificat d'un serveur web

Le 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 serveur concerné, et également l'entité pour le compte de laquelle il utilise le certificat et avec laquelle il entretient un lien contractuel/hiérarchique/réglementaire. Le certificat est rattaché au serveur 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.

1.3.5 Utilisateurs de certificats

Les utilisateurs de certificats doivent prendre toutes les précautions décrites dans cette PC/DPC ainsi que dans les CGVU.

1.3.5.1 Certificat d'AC

CERTIGNA & CERTIGNA ROOT CA	*AC racine*
Entité ou personne physique qui utilise un certificat d'autorité racine et qui s'y fie pour vérifier l'origine et la validité d'un certificat émis par cette autorité.	
AC intermédiaires	*AC intermédiaire*
Entité ou personne physique qui utilise un certificat d'autorité intermédiaire et qui s'y fie pour vérifier l'origine et la validité d'un certificat émis par cette autorité.	

1.3.5.2 Certificat de personne morale

Un utilisateur (ou accepteur) de certificats électroniques d'authentification serveur peut être notamment :

- 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.
- 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

1.3.6 Autres participants

1.3.6.1 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 :

- De traiter une demande de certificat ou de renouvellement de certificat ;
- De traiter une demande de révocation de certificat ;
- Le cas échéant, d'enregistrer les MC 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 et MC 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 respecter les parties de cette PC/DPC lui incombant.

1.3.6.2 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 MC 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 MC 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 MC. 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 respecter les parties de la présente PC/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.

1.3.6.3 Service clients

Pour assurer un service réactif et conforme aux exigences, Certigna peut recourir à un prestataire spécialisé dans les « Services clients » afin d'assister ses prospects et clients dans leurs demandes relatives aux certificats, A cette fin, les opérateurs de cette entité sont enrôlés en tant qu'opérateur d'AED pour leur permettre d'accéder aux dossiers de demande et d'assister au mieux les demandeurs dans leurs démarches.

Un contrat similaire au contrat avec un AED est établi avec l'entité en charge de ce service. Le prestataire s'engage ainsi à respecter les parties de cette PC/DPC lui incombant, et notamment les engagements des chapitres 3 et 4.

1.3.6.4 Hébergeurs de l'infrastructure technique

Certigna peut recourir à un prestataire pour l'hébergement physique de son infrastructure technique. Un contrat est établi avec le prestataire pour garantir la sécurité des services conformément aux engagements du chapitre 5.1 de cette PC/DPC.

1.3.6.5 Fournisseurs des supports cryptographiques

Le support cryptographique, délivré le cas échéant par Certigna au RC, pour stocker et utiliser la clé privée et le certificat, peut être acquis auprès d'un fournisseur avec lequel un contrat est établi visant à garantir la conformité du support avec une ou plusieurs qualifications et/ou certifications citées au chapitre 11 de la Politique de Certification.

Malgré ces dispositions, il est important de rappeler que dans le cas où l'une de ces qualifications ou certifications ne serait plus maintenue ou suspendue pour des raisons telles que l'identification d'une vulnérabilité ou l'arrêt de fabrication du produit, Certigna en informera le RC et révoquera son certificat, sans condition de remboursement.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

QNCP-w / QEVP-w
Les certificats électroniques sont utilisés par des applications pour lesquelles les besoins de sécurité sont très forts eu égard aux risques très élevés qui les menacent.
OVCP
Les certificats électroniques sont utilisés par des applications pour lesquelles les besoins de sécurité sont forts eu égard aux risques élevés qui les menacent.
RGS *
Les certificats électroniques sont utilisés par des applications pour lesquelles les besoins de sécurité sont moyens eu égard aux risques qui les menacent.

1.4.1.1 Certificat d'AC

CERTIGNA & CERTIGNA ROOT CA	*AC racine*
La bi-clé d'AC racine est utilisée pour la signature des certificats d'AC intermédiaires et des Listes de certificats d'AC Révoqués (LAR).	
AC intermédiaires	*AC intermédiaire*
La bi-clé d'AC intermédiaire est utilisée pour la signature des certificats finaux et des Listes de Certificats Révoqués (LCR).	

1.4.1.2 Certificat de personne morale

Authentification du serveur auprès d'autres serveurs ou de personnes, dans le cadre de l'établissement de sessions sécurisées, de type TLS/SSL 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 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).

1.4.2 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, des MC et des utilisateurs potentiels des CGVU qui peuvent être consultées sur le site https://www.certigna.com avant toute demande de certificat ou toute utilisation d'un certificat.

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

L'AC dispose d'un Comité de Sécurité responsable de l'élaboration, du suivi et de la modification de la présente PC/DPC. Il statue sur toute modification nécessaire à apporter à la PC/DPC à échéance régulière.

La validation formelle de cette PC/DPC et des CGVU est assurée à minima par une personne dans un rôle de confiance de contrôleur et d'une personne dans un rôle de confiance d'Officier de sécurité.

1.5.2 Point de contact

1.5.2.1 FAQ et support client

Les réponses aux questions communément posées sont disponibles dans notre FAQ accessible à l'adresse suivante : https://www.certigna.com/faq/. Pour toute autre question, vous pouvez joindre notre service client aux coordonnées suivantes :

- Contact mail : contact@certigna.fr ;
- Téléphone : 0 806 115 115 (Service gratuit) disponible du lundi au vendredi de 09h00 à 18h00 ;
- Chat sur le site https://www.certigna.com et disponible du lundi au vendredi de 09h00 à 18h00.

1.5.2.2 Demander une révocation

Comme évoqué au chapitre 3.4.2, 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 :

- Depuis l'espace client du site CERTIGNA https://www.certigna.com en sélectionnant le certificat à révoquer ;

- Courrier : demande remplie et signée à partir du formulaire de révocation d'un certificat disponible sur le site de CERTIGNA https://www.certigna.com. Le demandeur s'authentifie en joignant la photocopie de sa pièce d'identité au courrier envoyé.

Les informations relatives au traitement de vos données personnelles sont disponibles dans la Politique d'utilisation des données personnelles accessible à l'adresse suivante : https://www.certigna.com/politique-dutilisation-des-donnees-personnelles/.

1.5.2.3 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 : 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.com/contactez-nous/ et sélectionner le motif « Certificat jugé malveillant ou dangereux ».

1.5.2.4 Porter une réclamation

Pour porter une réclamation à la connaissance de Certigna, veuillez utiliser le formulaire de contact disponible à l'adresse suivante https://www.certigna.com/contactez-nous/ et sélectionner le motif « Réclamation ».

Vous pouvez également porter réclamation à notre service client aux coordonnées suivantes :
- Contact mail **:** contact@certigna.fr ;
- Téléphone : 0 806 115 115 (Service gratuit) disponible du lundi au vendredi de 09h00 à 18h00 ;
- Chat sur le site https://www.certigna.com et disponible du lundi au vendredi de 09h00 à 18h00 ;
- Courrier adressé à :

CERTIGNA
20 allée de la Râperie
Zone de la plaine
59650 Villeneuve d'Ascq, France

Les informations relatives au traitement de vos données personnelles sont disponibles dans la Politique d'utilisation des données personnelles accessible à l'adresse suivante : https://www.certigna.com/politique-dutilisation-des-donnees-personnelles/.

1.5.3 Entité déterminant la conformité de la DPC avec la PC

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

1.5.4 Procédures d'approbation de la conformité de la DPC

Initialement, 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 cette PC/DPC répondent aux exigences selon le processus d'approbation mis en place. Un contrôle de conformité de la PC/DPC 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 PC/DPC suit également ce processus.

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

1.6 Définitions et acronymes

1.6.1 Définitions

Les termes utiles à la bonne compréhension de la PC/DPC 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.

Autorisation de l'Autorité de Certification (CAA) : Emanant de la RFC 8659, l'enregistrement de ressource DNS CAA 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.

Certificat « cross-signé » - Un certificat qui est utilisé pour établir une relation de confiance entre deux AC Racines.

Clé privée – La clé d'une bi-clé qui est gardée secrète par le responsable de la bi-clé, et qui est utilisée pour créer des signatures électroniques et/ou pour déchiffrer des fichiers ou enregistrements électroniques qui sont chiffrés avec la clé publique correspondante.

CSPRNG – Un générateur de nombres aléatoires destiné à être utilisé dans un système cryptographique.

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.

Corroboration de délivrance en multi-perspectives - Processus par lequel les contrôles techniques fait lors de la validation du domaine et de la vérification du CAA par la perspective du réseau primaire sont corroborées par d'autres perspectives du réseau avant la délivrance du certificat.

Perspective de réseau - Liée à la corroboration de la délivrance multi-perspectives. Un système (Ex : une instance de serveur hébergée dans le cloud) ou un ensemble de composants réseau (Ex : un VPN et l'infrastructure correspondante) pour envoyer le trafic Internet sortant associé à une méthode de validation de contrôle de domaine et/ou à une vérification CAA. L'emplacement d'une perspective de réseau est déterminé par le point où le trafic Internet sortant non-encapsulé est généralement transmis pour la première fois à l'infrastructure de réseau fournissant une connectivité Internet à cette perspective.

Perspective de réseau primaire - Perspective de réseau utilisée par l'AC pour déterminer :
- l'autorité de l'AC à délivrer un certificat pour le(s) domaine(s) demandé(s), et
- l'autorité du demandeur et/ou l'autorisation ou le contrôle du(des) domaine(s) demandé(s).

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 responsable du certificat (ex. clé privée, code PIN, …). Il peut prendre la forme d'un module cryptographique, 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. Il peut s'agir d'une organisation privée, d'une entité gouvernementale, d'une entité commerciale ou d'une entité non commerciale.

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, une entité commerciale ou une entité non 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, …

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.

Linting – Un processus dans lequel le contenu des données signées électroniquement telles qu'un précertificat [RFC 6962], un certificat, une LCR ou une réponse OCSP, ou un objet de « données-à-signer » tel qu'un tbsCertificate (comme décrit dans la RFC 5280, chapitre 4.1.1.1) est vérifié en conformité avec les profils et exigences définies par les exigences du CA\Browser Forum.

Liste des certificats d'AC révoqués - 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.

Online Certificate Status Protocol (OCSP) – Un protocole de vérification de certificats en ligne qui permet à une tierce application de déterminer le statut d'un certificat identifié.

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 européen eIDAS décrivent les procédures 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.

Rapport d'audit - Un rapport d'un auditeur qualifié indiquant l'opinion de l'auditeur qualifié sur la conformité des processus et des contrôles avec les exigences applicables.

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.

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).

Société affiliée - une société, un partenariat, une coentreprise ou une autre entité contrôlant, contrôlée par ou sous contrôle commun avec une autre entité, ou une agence, un département, une subdivision politique ou tout autre entité opérant sous le contrôle direct d'une entité gouvernementale.

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 ou chiffrer des données à destination d'un RC.

Nota - Un agent d'une autorité administrative qui procède à des échanges électroniques avec une autre autorité administrative est, pour cette dernière, un usager.
Nota - Dans la suite du document le terme « entité » est utilisé pour désigner une entreprise ou une administration. La dénomination « entreprise » recouvre les entreprises au sens le plus large, à savoir toutes personnes morales de droit privé : sociétés, associations ainsi que les artisans et travailleurs indépendants.

1.6.2 Acronymes

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

AA	Autorité Administrative
AC	Autorité de Certification
ACME	Automatic Certificate Management Environment
ABE	Autorité Bancaire Européenne
ACN	Autorité Compétente Nationale
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information

CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CGVU	Conditions Générales de Vente et d'Utilisation
CNIL	Commission Nationale de l'Informatique et des Libertés
CSR	Certificate Signing Request
DBA	Doing Business As (Marque)
DN	Distinguished Name
DNS	Domain Name System
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
ICD	International Code Designator
IGC	Infrastructure de Gestion de Clés (= PKI : Public Key Infrastructure)
INPI	Institut National de la Propriété Industrielle
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
NIST	(US Government) National Institute of Standards and Technology
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
PSP	Prestataire de Services de Paiement
RC	Responsable du Certificat Cachet Serveur
RSA	Rivest Shamir Adleman
SCT	Signed Certificate Timestamp
S/MIME	Secure MIME (Extensions mail Internet multi-usages)
SMSI	Système de Management de la Sécurité de l'Information
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

1.6.3 Références

RGS Annexe 3, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ; Référentiel Général de sécurité ; Annexe A3 : Politique de certification type « certificats électroniques de services applicatifs ».

ETSI EN 319 411-1, Signatures électroniques et infrastructures (ESI) ; Exigences en matière de politique et de sécurité pour les prestataires de services de confiance émettant des certificats ; Partie 1 : Exigences générales.

RFC 3647, Appel à commentaires : 3647, Infrastructure à clé publique X.509 sur Internet : Cadre de politique de certification et de pratiques de certification.

RFC 4035, Appel à commentaires : 4035, Modifications du protocole pour les extensions de sécurité DNS.

RFC 4509, Appel à commentaires : 4509, Utilisation de SHA-256 dans les enregistrements de ressources (RR) de signataire de délégation (DS) DNSSEC.

RFC 5155, Appel à commentaires : 5155, Sécurité DNS (DNSSEC) : déni d'existence authentifié par hachage.

RFC 5280, Appel à commentaires : 5280, Infrastructure à clé publique X.509 sur Internet : certificats et liste de révocation de certificats (CRL)

RFC 5702, Appel à commentaires : 5702, Utilisation des algorithmes SHA-2 avec RSA dans les enregistrements de ressources DNSKEY et RRSIG pour DNSSEC.

RFC 6840, Appel à commentaires : 6840, Clarifications et notes de mise en œuvre pour la sécurité DNS (DNSSEC).

RFC 6960, Appel à commentaires : 6960, Infrastructure à clé publique Internet X.509 – Protocole de statut de certificat en ligne (OCSP).

RFC 6962, Appel à commentaires : 6962, Transparence des certificats.

RFC 7231, Appel à commentaires : 7231, Protocole de transfert hypertexte (HTTP/1.1) : sémantique et contenu.

RFC 7538, Appel à commentaires : 7538, Code d'état 308 du protocole de transfert hypertexte (redirection permanente).

RFC 8555, Appel à commentaires : 8555, Environnement de gestion automatique des certificats (ACME)

RFC 8659, Appel à commentaires : 8659, Enregistrement de ressource d'autorisation des autorités de certification DNS (CAA).

2 RESPONSABILITE CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS

L'AC élabore, met en œuvre, applique, et met à jour au moins tous les 366 jours la présente PC/DPC qui décrit en détail comment l'AC met en œuvre la dernière version des exigences applicables.

2.1 Publication

2.1.1 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.

2.1.2 Informations devant être publiées

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

- La PC/DPC ;
- Les Conditions Générales de Vente et 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 racine et les certificats d'AC intermédiaires en cours de validité ;
- Les listes des certificats révoqués (LAR / LCR).

Remarque : compte tenu de la complexité de lecture d'une PC pour les personnes non spécialistes du domaine, l'AC publie en dehors des PC et DPC des CGVU 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 Publication des informations de certification

La PC/DPC est structurée conformément à la RFC 3647.
La PC/DPC et les CGVU sont mises à jour au moins une fois par an et sont publiées.

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

La PC/DPC, les CGVU et les différents formulaires nécessaires pour la gestion des certificats sont publiés sous forme électronique à l'adresse http://cps.certigna.com.

2.2.2 Publication de la DPC

L'AC publie, à destination des RC, et des utilisateurs de certificats, sa PC/DPC. Les détails sensibles relatifs à ses pratiques ne sont toutefois pas rendus publics.

2.2.3 Publication des certificats d'AC

Les RC et les utilisateurs de certificat peuvent accéder aux certificats d'AC qui sont à l'adresse suivante https://www.certigna.com/autorites-de-certification/ ou directement via les adresses ci-dessous.

CERTIGNA SERVER AUTHENTICATION ROOT CA	
Certificat d'AC	http://cert.certigna.com/CertignaServerAuthenticationRootCA.cer
CERTIGNA SERVER AUTHENTICATION OVCP CA	
Certificat d'AC	http://cert.certigna.com/CertignaServerAuthenticationOVCPCA.cer
CERTIGNA SERVER AUTHENTICATION AUTO OVCP CA	
Certificat d'AC	http://cert.certigna.com/CertignaServerAuthenticationAutoOVCPCA.cer
CERTIGNA SERVER AUTHENTICATION QCP CA	
Certificat d'AC	http://cert.certigna.com/CertignaServerAuthenticationQCPCA.cer
CERTIGNA SERVER AUTHENTICATION AUTO QCP CA	
Certificat d'AC	http://cert.certigna.com/CertignaServerAuthenticationAutoQCPCA.cer
CERTIGNA SERVER AUTHENTICATION EU ROOT CA	
Certificat d'AC	http://cert.certigna.com/CertignaServerAuthenticationEURootCA.cer
CERTIGNA SERVER AUTHENTICATION OVCP EU CA	
Certificat d'AC	http://cert.certigna.com/CertignaServerAuthenticationOVCPEUCA.cer
CERTIGNA SERVER AUTHENTICATION AUTO OVCP EU CA	
Certificat d'AC	http://cert.certigna.com/CertignaServerAuthenticationAutoOVCPEUCA.cer
CERTIGNA	
Certificat d'AC	http://autorite.certigna.fr/certigna.der
CERTIGNA ROOT CA	
Certificat d'AC	http://autorite.certigna.fr/certignarootca.der
CERTIGNA SERVICES CA	
Certificat d'AC	http://autorite.certigna.fr/servicesca_rootca.der
CERTIGNA SERVER AUTHENTICATION OVCP EU CA G1	
Certificat d'AC	http://cert.certigna.com/CertignaServerAuthenticationOVCPEUCAG1cer
CERTIGNA WILD CA	
Certificat d'AC	http://autorite.certigna.fr/wildca_rootca.der
CERTIGNA SERVER AUTHENTICATION OVCP CA G1	
Certificat d'AC	http://cert.certigna.com/CertignaServerAuthenticationOVCPCAG1cer

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 notamment été mises en place :

- Instauration d'astreinte pendant les heures non ouvrées ;
- Souscription d'un service de surveillance de sécurité (24 heures sur 24) ;
- 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.

2.2.4 Publication de certificats de test

Pour les certificats d'authentification web, des certificats de tests sont publiés afin de permettre aux applications utilisatrices telles que les navigateurs de tester leur interprétation de l'état des certificats.

CERTIGNA SERVER AUTHENTICATION ROOT CA	
Test certificat valide	https://valid.serverauthenticationovcpca.certigna.com
Test certificat expire	https://expired.serverauthenticationovcpca.certigna.com
Test certificat révoqué	https://revoked.serverauthenticationovcpca.certigna.com
CERTIGNA SERVER AUTHENTICATION EU ROOT CA	
Test certificat valide	https://valid.serverauthenticationovcpeuca.certigna.com
Test certificat expire	https://expired.serverauthenticationovcpeuca.certigna.com
Test certificat révoqué	https://revoked.serverauthenticationovcpeuca.certigna.com
CERTIGNA	
Test certificat valide	https://valid.servicesca-racine.dhimyotis.com
Test certificat expire	https://expired.servicesca-racine.dhimyotis.com
Test certificat révoqué	https://revoked.servicesca-racine.dhimyotis.com
CERTIGNA ROOT CA	
Test certificat valide	https://valid.servicesca.dhimyotis.com
Test certificat expire	https://expired.servicesca.dhimyotis.com
Test certificat révoqué	https://revoked.servicesca.dhimyotis.com

2.2.5 Publication de la LAR

La liste des certificats d'autorités de certification révoqués est publiée au format électronique aux adresses du tableau ci-dessus. Ces adresses sont également indiquées dans les certificats.

CERTIGNA SERVER AUTHENTICATION ROOT CA et AC intermédiaires	
LAR	http://crl.certigna.com/CertignaServerAuthenticationRootCA.crl
CERTIGNA SERVER AUTHENTICATION EU ROOT CA et AC intermédiaires	
LAR	http://crl.certigna.com/CertignaServerAuthenticationEURootCA.crl
CERTIGNA et AC intermédiaires	
LAR	http://crl.certigna.fr/certigna.crl ou http://crl.dhimyotis.com/certigna.crl ou http://crl.certigna.com/Certigna.crl for ACME CAs
CERTIGNA ROOT CA et AC intermédiaires	
LAR	http://crl.certigna.fr/certignarootca.crl ou http://crl.dhimyotis.com/certignarootca.crl or http://crl.certigna.com/CertignaRootCA.crl for ACME CAs

2.2.6 Publication de la LCR

La liste des certificats finaux révoqués est publiée au format électronique aux adresses du tableau ci-dessus. Ces adresses sont également indiquées dans les certificats émis par l'AC.

CERTIGNA SERVER AUTHENTICATION ROOT CA	
CERTIGNA SERVER AUTHENTICATION OVCP CA	
CRL	http://crl.certigna.com/CertignaServerAuthenticationOVCPCA.crl
CERTIGNA SERVER AUTHENTICATION AUTO OVCP CA	
CRL	http://crl.certigna.com/CertignaServerAuthenticationAutoOVCPCA.crl
CERTIGNA SERVER AUTHENTICATION QCP CA	
CRL	http://crl.certigna.com/CertignaServerAuthenticationQCPCA.crl
CERTIGNA SERVER AUTHENTICATION AUTO QCP CA	
CRL	http://crl.certigna.com/CertignaServerAuthenticationAutoQCPCA.crl
CERTIGNA SERVER AUTHENTICATION EU ROOT CA	
CERTIGNA SERVER AUTHENTICATION OVCP EU CA	
CRL	http://crl.certigna.com/CertignaServerAuthenticationOVCPEUCA.crl
CERTIGNA SERVER AUTHENTICATION AUTO OVCP EU CA	
CRL	http://crl.certigna.com/CertignaServerAuthenticationAutoOVCPEUCA.crl
CERTIGNA & CERTIGNA ROOT CA	
CERTIGNA SERVICES CA	
CRL	http://crl.certigna.fr/servicesca.crl ou http://crl.dhimyotis.com/servicesca.crl
CERTIGNA SERVER AUTHENTICATION OVCP EU CA G1	
CRL	http://crl.certigna.com/CertignaServerAuthenticationOVCPEUCAG1.crl
CERTIGNA WILD CA	
CRL	http://crl.certigna.fr/wildca.crl ou http://crl.dhimyotis.com/wildca.crl
CERTIGNA SERVER AUTHENTICATION OVCP CA G1	
CRL	http://crl.certigna.com/CertignaServerAuthenticationOVCPCAG1.crl

2.3 Délais et fréquences de publication

2.3.1 Publication de la documentation

La PC/DPC, les CGVU et les différents formulaires nécessaires pour la gestion des certificats sont mis à jour annuellement et si nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectives de l'AC. Ces documents sont disponibles 24 heures sur 24, 7 jours sur 7. La fonction de publication de ces informations (hors informations d'état des certificats) est disponible les jours ouvrés.

2.3.2 Publication des certificats d'AC

Les certificats d'AC sont diffusés préalablement à toute diffusion de certificats émis par l'AC et de LCR correspondants. La disponibilité des systèmes publiant les certificats d'AC est garantie 24 heures sur 24, 7 jours sur 7.

2.3.3 Publication de la LAR

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

2.3.4 Publication de la LCR

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

2.4 Contrôle d'accès aux informations publiées

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

La PC/DPC et les CGVU sont publiées dans un format en lecture seule.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de nom

Dans chaque certificat conforme à la norme X.509, l'AC émettrice (correspondant au champ « issuer ») et la personne morale ou physique (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 la personne morale ou physique et est construit à partir de l'identité du serveur telle que figurant sur les justificatifs présentés lors de son enregistrement et son authentification auprès de l'AE ou du MC.

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

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 nom

Sans objet.

3.1.5 Unicité des noms

Note : L'attribut « serialNumber » présent dans le champ DN et le champ « serialNumber » du certificat sont des données distinctes.

3.1.5.1 Certificat d'AC

L'AC garantie que les noms positionnés dans le champ CN des certificats d'AC intermédiaires sont uniques sur le périmètre de l'AC.

3.1.5.2 Certificat de personne morale

La combinaison du pays, de l'entité et du FQDN identifie de manière univoque le titulaire du certificat. Durant toute la durée de vie de l'AC, le FQDN d'un serveur rattaché à une entité ne peut être attribué à une autre entité.

EN 319 411-1 OVCP
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 ».
EN 319 411-2 QNCP-w EN 319 411-2 QEVCP-w
L'attribut « serialNumber » est constitué du numéro d'immatriculation/d'enregistrement de l'entité.

3.1.6 Identification, authentification et rôle des marques déposées

L'AC est responsable de l'unicité des noms des personnes morales et physiques 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 (ou d'un AED), soit via un Mandataire de Certification de l'entité. Dans ce dernier cas, le MC 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 sur le site de CERTIGNA ou de l'AED et à certaines données d'activation lui permettant ainsi de récupérer et d'utiliser son certificat. 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.

La demande de certificat peut être communiquée à l'AE ou l'AED au format papier signé manuscritement par le RC et les cosignataires. La demande peut également être communiquée à l'AE ou l'AED au format électronique sous les conditions suivantes :

EN 319 411-2 QNCP-w EN 319 411-2 QEVCP-w
Au format électronique si signée par chaque signataire à l'aide d'un certificat de signature électronique qualifié au sens du Règlement eIDAS. Le certificat doit être valide lors de l'enregistrement par l'AE.
EN 319 411-1 OVCP RGS *
Au format électronique si possible signée à l'aide d'un procédé de signature électronique conforme aux exigences du niveau RGS *.

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, le RC génère la bi-clé sur un dispositif conforme aux exigences du chapitre 11, et fournit à l'AC une preuve de possession de la clé privée en signant la 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 Authentification de l'organisation

L'AC inspecte la copie pour rechercher toute altération ou falsification qui aurait été effectuée.

3.2.2.1 Identité

L'AC collecte et conserve les preuves relatives aux attributs d'identité suivant pour l'entité :

- Le Nom officiel de l'entité ;
- Le nom d'emprunt enregistré pour l'entité (si inclus dans le sujet) ;
- L'unité organisationnelle de l'entité (si incluse dans le Sujet) ;
- L'adresse de l'Entité (si incluse dans le sujet) ;
- La juridiction de constitution ou d'enregistrement de l'entité ; et
- L'Identifiant unique et le type d'identifiant de l'entité. L'identifiant unique est inclus dans le champ « subject:organizationIdentifier » du certificat.

3.2.2.1.1 Vérification de l'identité et de l'existence légale

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).

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.

Dans le cas de l'utilisation d'une référence de données LEI, l'AE vérifie les données enregistrées à l'aide de la « Global Legal Entity Identifier Foundation » accessible via ce lien : https://search.gleif.org/#/search/.

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.

3.2.2.1.2 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 boite aux lettres ou boite 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.

3.2.2.1.3 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 et que son enregistrement reste valide.

3.2.2.1.4 Vérification des moyens de communication de l'entité

3.2.2.1.4.1 Validation du contrôle de l'adresse E-mail via l'envoi d'un mail

Lors de la demande de certificat, l'adresse email du demandeur est contrôlée via l'envoi d'un lien d'activation. L'AC ne délègue pas la vérification de contrôle ou d'autorisation sur l'adresse E-mail.

3.2.2.1.4.2 Validation des moyens de communications via téléphone

CERTIGNA SERVICES CA	*Authentification web*
EN 319 411-2 QEVCP-w	
Le numéro de téléphone communiqué dans la demande de certificat 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.	

3.2.2.2 DBA et Nom commercial

Si les informations sur l'identité du sujet doivent inclure un DBA ou un nom commercial, l'AC vérifie le droit du demandeur pour utiliser le DBA / nom commercial en utilisant au moins l'un des éléments suivants :

- Une documentation fournie ou communiquée par un organisme gouvernemental dans la juridiction de création, d'existence ou de reconnaissance légale du demandeur ;
- Une source de données fiable ;
- Communication avec un organisme gouvernemental responsable de la gestion de ces DBA ou noms commerciaux ;
- Une lettre d'attestation accompagnée d'un support documentaire ;
- Une facture de services publics, un relevé bancaire, un relevé de carte de crédit, un document fiscal émis par le gouvernement ou toute autre forme d'identification que l'AC juge fiable.

Le champ "organizationName" peut contenir le nom de l'organisation ou un nom commercial/Dénomination sociale. L'AC peut inclure une information dans ce champ qui diffère légèrement du nom vérifié, telles que des variantes ou des abréviations courantes, à condition que l'AC documente la différence et que toutes les abréviations utilisées soient des abréviations acceptées localement ; par exemple, si le registre officiel indique « Company Name Incorporated », l'AC peut utiliser « Company Name Inc. » ou « Company Name ». Si les deux sont inclus, le nom commercial/dénomination sociale apparaît en premier, suivi du nom de l'organisation entre parenthèse.

3.2.2.3 Vérification du pays

L'AC vérifie le pays associé au champ « *countryName* » du sujet en utilisant l'un des éléments suivants:

- L'attribution de la plage d'adresses IP par pays pour l'adresse IP du site Web, comme indiqué par l'enregistrement DNS du site Web ou l'adresse IP du demandeur ;
- Le ccTLD du nom de domaine demandé ;
- Les informations fournies par le fournisseur des noms de domaine ;
- Une méthode identifiée à la section 3.2.2.1.

L'AC met en œuvre un processus de filtrage des serveurs proxy afin d'empêcher la dépendance sur les adresses IP attribuées dans des pays autres que celui où le demandeur se trouve réellement.

3.2.2.4 Validation de l'autorisation ou du contrôle du 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 4.2.1. 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. Cette vérification est réalisée avant la délivrance de chaque certificat, même lors de son renouvellement. L'AC conserve une trace de la méthode de validation utilisée pour valider chaque domaine.

À compter du 15 mars 2026 : la validation DNSSEC par rapport à l'ancrage de confiance racine DNSSEC de l'IANA est effectuée sur toutes les requêtes DNS associées à la validation de l'autorisation ou du contrôle du domaine par la perspective réseau primaire. Le résolveur DNS utilisé pour toutes les requêtes DNS associées à la validation de l'autorisation ou du contrôle du domaine par la perspective réseau primaire :

- effectue la validation DNSSEC à l'aide de l'algorithme défini dans la section 5 de la RFC 4035 ; et
- prend en charge NSEC3 tel que défini dans la RFC 5155 ; et • prendre en charge SHA-2 tel que défini dans les RFC 4509 et 5702 ; et
- traite correctement les problèmes de sécurité énumérés dans la section 4 de la RFC 6840.

À compter du 15 mars 2026 :

Pour les méthodes de validation de domaine par e-mail décrites aux sections 3.2.2.4.4 et 3.2.2.4.14, la validation DNSSEC par rapport à l'ancrage de confiance racine DNSSEC de l'IANA est effectuée sur toutes les requêtes DNS CNAME, CAA, TXT qui tentent d'obtenir le nom de domaine d'autorisation associé à la validation de l'autorisation ou du contrôle du domaine par la perspective réseau primaire, et l'AC n'utilise pas de politique locale pour désactiver la validation DNSSEC.

Pour toutes les autres méthodes de validation de domaine, la validation DNSSEC par rapport à l'ancrage de confiance racine DNSSEC de l'IANA est effectuée sur toutes les requêtes DNS associées à la validation de l'autorisation ou du contrôle du domaine par la perspective réseau primaire, et l'AC n'utilise pas de politique locale pour désactiver la validation DNSSEC sur les requêtes DNS associées à la validation de l'autorisation ou du contrôle du domaine.

La validation DNSSEC remontant à l'ancrage de confiance racine DNSSEC de l'IANA est considérée comme hors du champ d'application :
- des audits internes effectués pour respecter les engagements de la section 8.7,
- des engagements en matière de journalisation de la section 5.4.1.

La validation DNSSEC par rapport à l'ancrage de confiance racine DNSSEC de l'IANA peut être effectuée sur toutes les requêtes DNS associées à la validation de l'autorisation ou du contrôle du domaine par les perspectives réseau distantes utilisées pour la corroboration de l'émission multiperspective.

L'autorité de certification conserve une trace de la méthode de validation de domaine, y compris le numéro de version BR correspondant, qu'elle a utilisée pour valider chaque domaine.

3.2.2.4.1 Validation du demandeur comme un contact du domaine

Sans objet.

3.2.2.4.2 Email au contact du domaine

Sans objet. Cette méthode a été retirée par l'AC.

3.2.2.4.3 Contact téléphonique avec le contact du domaine

Sans objet.

3.2.2.4.4 Email à une adresse construite

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'un jeton de demande 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.

Le jeton de demande aléatoire est unique pour chaque FQDN et reste valide jusqu'à 30 jours après sa création. Le mail pourra être renvoyé dans son intégralité, intégrant la réutilisation du jeton de demande, à condition que l'ensemble de son contenu et son destinataire restent inchangés.

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.

À partir du 15 mars 2028 : l'AC ne doit plus utiliser cette méthode et les validations antérieures effectuées à l'aide de cette méthode et les données de validation recueillies conformément à cette méthode ne pourront pas être utilisées pour délivrer des certificats de serveurs.

3.2.2.4.5 Document d'autorisation du domaine

Sans objet.

3.2.2.4.6 Changement apporté au site web

Sans objet.

Cette méthode a été retirée et remplacée par la méthode « 3.2.2.4.18 Changement apporté au site web v2 ».

3.2.2.4.7 Changement DNS

Un enregistrement de type DNS CNAME est affiché au demandeur lors de la personnalisation de sa demande de certificat, Cet enregistrement est à positionner dans la configuration DNS du site web et est composé du nom de domaine préfixé par un label commençant par un underscore (" _") ainsi que d'un jeton de demande. Le jeton de demande est unique pour chaque FQDN et reste valide jusqu'à 30 jours après sa création. Un nouveau jeton de demande sera fourni pour chaque FQDN au-delà des 30 jours, rendant invalide l'enregistrement fourni précédemment.

Si plusieurs FQDNs sont concernés par une même demande, plusieurs enregistrements à créer. Le demandeur doit ajouter tous les enregistrements dans la configuration DNS du site web afin de permettre le contrôle de chaque FQDN. À compter du 15/03/2025, l'AC implémente la corroboration de la délivrance en multi-perspectives telle que spécifiée au chapitre 3.2.2.9. D'autres perspectives réseau observent la même information de vérification (jeton de demande) que la première perspective réseau.

3.2.2.4.8 Adresse IP

Sans objet.

3.2.2.4.9 Certificat de test

Sans objet.

3.2.2.4.10 TLS utilisant un nombre aléatoire

Sans objet.

3.2.2.4.11 Tout autre méthode

Sans objet.

3.2.2.4.12 Validation du demandeur comme un contact du domaine

Sans objet.

3.2.2.4.13 Email au contact DNS CAA

Sans objet.

3.2.2.4.14 Email au contact DNS TXT

Un mail est envoyé par CERTIGNA à l'une des adresses de contact présente dans l'enregistrement DNS TXT. Ce mail fournit un lien composé d'un jeton de demande 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.

Le jeton de demande aléatoire est unique pour chaque FQDN et reste valide jusqu'à 30 jours après sa création. Le mail pourra être renvoyé dans son intégralité, intégrant la réutilisation du jeton de demande, à condition que l'ensemble de son contenu et son destinataire restent inchangés.

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

À partir du 15 mars 2028 : l'AC ne doit plus utiliser cette méthode et les validations antérieures effectuées à l'aide de cette méthode et les données de validation recueillies conformément à cette méthode ne pourront pas être utilisées pour délivrer des certificats de serveurs.

3.2.2.4.15 Contact téléphonique avec le contact du domaine

Sans objet.

3.2.2.4.16 Contact téléphonique avec le contact téléphonique du DNS TXT

Sans objet.

3.2.2.4.17 Contact téléphonique avec le contact téléphonique du DNS CAA

Sans objet.

3.2.2.4.18 Changement apporté au site web v2

Un jeton de demande est affiché au demandeur lors de la personnalisation de sa demande de certificat, et doit être positionnée par le demandeur dans un fichier texte.

Le jeton de demande contenu dans le fichier n'apparait pas dans la requête utilisée pour la vérification. L'AC doit recevoir une réponse HTTP réussie lors de la demande.

Le fichier texte contenant le jeton de demande doit :
- être placé sur le nom de domaine autorisé, et ;
- être placé dans le répertoire "/.wellknown/pki-validation" du site web et ;
- être récupéré automatiquement via HTTP ou HTTPS, et ;
- être accessible via un port autorisé.

Lorsque l'AC suit les redirections, alors :

- Les redirections sont initiées au niveau du protocole HTTP. Les redirections doivent être le résultat d'une réponse de code d'état 301, 302 ou 307 (cf. RFC 7231 §6.4) ou une réponse de code d'état 308 (cf. RFC 7538 §3). Les redirections doivent être vers la valeur finale de l'entête de réponse HTTP Location (cf. RFC 7231 § 7.1.2) ;
- Les redirections doivent être vers des URLs de ressources avec le schéma HTTP ou HTTPS.
- Les redirections doivent être dirigées vers des URL de ressources accessibles via des ports autorisés.

Le jeton de demande est unique pour chaque FQDN et reste valide jusqu'à 30 jours après sa création. Un nouveau jeton de demande sera fourni pour chaque FQDN au-delà des 30 jours rendant invalide l'enregistrement fourni précédemment. Si plusieurs FQDNs sont concernés par une même demande, plusieurs fichiers seront à créer, chaque fichier contenant une valeur pour un FQDN. Le demandeur doit positionner tous les fichiers dans le répertoire afin de permettre le contrôle de chaque FQDN.

À compter du 15/03/2025, l'AC implémente la corroboration de la délivrance en multi-perspectives telle que spécifiée au chapitre 3.2.2.9. D'autres perspectives réseau observent la même information de vérification (jeton de demande) que la première perspective réseau.

Cette méthode n'est pas autorisée pour les certificats de type « Wildcard ».

3.2.2.4.19 Changement apporté au site web - ACME

La validation du contrôle du domaine du FQDN peut être opérée via la méthode ACME HTTP challenge définie dans la section 8.3 de la RFC 8555.

L'AC réceptionne une réponse HTTP à partir de la requête (un code de statut 2xx HTTP doit être reçu). Le jeton (comme défini dans la RFC 8555, section 8.3) reste valide jusqu'à 30 jours après sa création.

Le fichier texte contenant le jeton de demande doit :

- être placé sur le nom de domaine autorisé, et ;
- être placé dans le répertoire "/.well-known/acme-challenge/" du site web et ;
- être récupéré automatiquement via HTTP, et ;
- être accessible via un port autorisé.

Lorsque l'AC suit les redirections, alors :

- Les redirections sont initiées au niveau du protocole HTTP. Les redirections doivent être le résultat d'une réponse de code d'état 301, 302 ou 307 (cf. RFC 7231 §6.4) ou une réponse de code d'état 308 (cf. RFC 7538 §3). Les redirections doivent être vers la valeur finale de l'entête de réponse HTTP Location (cf. RFC 7231 § 7.1.2) ;
- Les redirections doivent être vers des URLs de ressources avec le schéma HTTP ou HTTPS.
- Les redirections doivent être dirigées vers des URL de ressources accessibles via des ports autorisés.

Le jeton de demande est unique pour chaque FQDN. Un nouveau jeton de demande sera fourni pour chaque FQDN au-delà des 30 jours rendant invalide l'enregistrement fourni précédemment. Si

plusieurs FQDNs sont concernés par une même demande, plusieurs fichiers seront à créer, chaque fichier contenant une valeur pour un FQDN. Le demandeur doit positionner tous les fichiers dans le répertoire afin de permettre le contrôle de chaque FQDN.

À compter du 15/03/2025, l'AC implémente la corroboration de la délivrance en multi-perspectives telle que spécifiée au chapitre 3.2.2.9. D'autres perspectives réseau observent la même information de vérification (jeton de demande) que la première perspective réseau.

Cette méthode n'est pas autorisée pour les certificats de type « Wildcard ».

3.2.2.4.20 TLS utilisant ALPN

Sans objet.

3.2.2.4.21 Enregistrement DNS labélisé avec l'ID du compte - ACME

Sans objet.

3.2.2.4.22 Enregistrement TXT DNS à valeur permanente

Sans objet.

3.2.2.5 Authentification pour une adresse IP

Sans objet.

3.2.2.6 Validation d'un domaine Wildcard

CERTIGNA WILD CA	*Authentification web*
CERTIGNA SERVER AUTHENTICATION OVCP CA	*Authentification web*
CERTIGNA SERVER AUTHENTICATION AUTO OVCP CA	*Authentification web*
CERTIGNA SERVER AUTHENTICATION QCP CA	*Authentification web*
CERTIGNA SERVER AUTHENTICATION AUTO QCP CA	*Authentification web*
Avant l'émission d'un certificat Wildcard avec le caractère « * » dans le CN ou l'extension "subjectAltName" de type DNS-ID, l'AC détermine si le caractère générique apparaît dans la première position du label à gauche du label « registry-controlled » ou « public suffix » (exemple "*.com", " *.co.uk »). Si le caractère tombe dans le label immédiatement à gauche du registry-controlled1 ou du public suffix, l'AC refuse la délivrance à moins que le demandeur ne prouve son contrôle légitime sur l'ensemble de l'espace de noms de domaine. (Exemple, l'AC ne peut émettre un certificat « *.co.uk» ou «* .local», mais émettre un certificat «* .example.com» à Example Co.).	

3.2.2.7 Pertinence des sources de données

Avant d'utiliser une source de données comme source de données fiable, l'AC évalue la source pour sa fiabilité, sa précision et sa résistance à l'altération ou à la falsification. L'AC tient compte des éléments suivants lors de son évaluation :

- L'âge des informations fournies ;
- La fréquence des mises à jour de la source d'information ;
- Le fournisseur de données et le but de la collecte de données ;
- L'accessibilité publique de la disponibilité des données ;

La relative difficulté de falsifier ou de modifier les données.

3.2.2.7.1 Autres listes noires ou listes des entités sous surveillance

CERTIGNA SERVICES CA	*Authentification web*
EN 319 411-2 QEVCP-w	
L'AE vérifie si l'un des signataires (RC, 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.	

3.2.2.7.2 Maison mère/filiale/Affilié

CERTIGNA SERVICES CA	*Authentification web*
EN 319 411-2 QEVCP-w	
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.	

3.2.2.7.3 Contrôles croisés et obligation de vigilance

CERTIGNA SERVICES CA	*Authentification web*
EN 319 411-2 QEVCP-w	
Les dossiers de demandes de certificats qualifiés (QEVCP-w) font l'objet de contrôles croisés entre deux opérateurs distincts de l'AE. Les résultats des processus et procédures de vérification réalisés 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 (QEVCP-w) 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 au demandeur.

3.2.2.8 Enregistrement CAA

Dans le cadre du processus de délivrance de certificat, l'AC récupère et traite les enregistrements CAA conformément à la RFC 8659 pour chaque nom de domaine présent dans l'extension « subjectAltName » du certificat.

À compter du 15 mars 2025, la réponse d'une perspective de réseau distant à la vérification de l'enregistrement CAA est interprétée comme une autorisation d'émettre, que les réponses des deux perspectives soient identiques ou non, octet par octet. En outre, l'AC peut considérer la réponse d'une perspective de réseau distant comme corroborante si l'une des perspectives ou les deux connaissent un échec acceptable de la consultation de l'enregistrement CAA, tel que défini dans la présente section.

L'AC peut vérifier les enregistrements CAA à tout autre moment.

Lors du traitement des enregistrements CAA, l'AC traite les tags « issue », « issuewild » et « iodef property » comme spécifiés par le RFC 8659, Ces contrôles permettent de vérifier que l'AC figure bien parmi les autorités autorisées à délivrer un certificat pour ces domaines.

Les cas suivants ne permettent pas à l'AC d'autoriser l'émission du certificat :

- Le champ DNS CAA est présent, il contient un tag « issue », « issuewild » ou « iodef property » et ne liste pas CERTIGNA comme une Autorité de Certification autorisée ;
- Le champ DNS CAA est présent, il est désigné comme « critique » et le tag utilisé n'est pas supporté par l'AC (il ne s'agit pas d'un tag « issue » ou « issuewild ») ;
- La zone est signée via DNSSEC de manière valide et la requête de l'AC sur le champ DNS CAA n'obtient pas de réponse.

Si l'un de ces cas est rencontré, la demande de certificat est bloquée automatiquement et le demandeur est notifié par mail de la nécessité de mettre à jour les enregistrements DNS concernés.

Pour ajouter CERTIGNA aux enregistrements DNS CAA, plusieurs syntaxes sont disponibles en fonction du serveur utilisé :

- example.com. IN CAA 0 issue "certigna.fr"

- example.com. IN CAA 0 issue "certigna.com"

L'AC délivre un certificat sous la durée de vie (TTL) de l'enregistrement CAA ou dans les 8 heures maximum.

3.2.2.8.1 Validation DNSSEC des enregistrements CAA

À compter du 15 mars 2026 : la validation DNSSEC par rapport à l'ancrage de confiance racine DNSSEC de l'IANA est effectuée sur toutes les requêtes DNS associées à la validation de l'autorisation ou du contrôle du domaine par la perspective réseau primaire. Le résolveur DNS utilisé pour toutes les requêtes DNS associées à la validation de l'autorisation ou du contrôle du domaine par la perspective réseau primaire :
- effectue la validation DNSSEC à l'aide de l'algorithme défini dans la section 5 de la RFC 4035 ; et
- prend en charge NSEC3 tel que défini dans la RFC 5155 ; et
- prend en charge SHA-2 tel que défini dans les RFC 4509 et 5702 ; et
- traite correctement les problèmes de sécurité énumérés dans la section 4 de la RFC 6840.

À compter du 15 mars 2026 : l'AC n'utilise pas de politique locale pour désactiver la validation DNSSEC sur toute requête DNS associée à la validation de l'autorisation ou du contrôle d'un domaine.

La validation DNSSEC par rapport à l'ancrage de confiance racine DNSSEC de l'IANA peut être effectuée sur toutes les requêtes DNS associées à la validation de l'autorisation ou du contrôle de domaine par des perspectives réseau distantes utilisées pour la corroboration de l'émission multiperspective.

La validation DNSSEC par rapport à l'ancrage de confiance racine DNSSEC de l'IANA est considérée comme hors du champ d'application des auto-audits effectués pour satisfaire aux exigences de la section 8.7.

3.2.2.9 Corroboration de délivrance multi-perspectives

La corroboration de l'émission multi-perspectives tente de corroborer les déterminations (c'est-à-dire la validation du domaine réussite/échec, l'autorisation/interdiction de CAA) faites par le point de vue du réseau principal à partir de plusieurs points de vue du réseau à distance avant l'émission du certificat. Ce processus peut améliorer la protection contre des attaques ou des détournements du protocole BGP (Border Gateway Protocol) portant sur des préfixes également spécifiques.

L'AC peut utiliser soit le même ensemble, soit différents ensembles de perspectives de réseau lors de la corroboration de la délivrance multi-perspectives pour l'autorisation ou le contrôle de domaine requis et les vérifications de l'enregistrement CAA.

L'ensemble des réponses provenant des perspectives de réseau utilisées fournit à l'AC les informations nécessaires pour lui permettre d'évaluer avec certitude :
- la présence du jeton de demande attendu, comme l'exige la méthode de validation fiable spécifiée dans les sections 3.2.2.4 et ;
- l'autorité de l'AC à délivrer au(x) domaine(s) demandé(s), comme spécifié dans la section 3.2.2.8.

La section 3.2.2.4 décrit les méthodes de validation qui nécessitent l'utilisation de la corroboration de l'émission multi-perspectives et la manière dont une perspective réseau peut corroborer les résultats déterminés par la perspective réseau primaire. Les résultats ou les informations obtenus à partir d'une

perspective de réseau ne peuvent pas être réutilisés ou mis en cache lors de la validation par les perspectives de réseau suivantes (par exemple, différentes perspectives de réseau ne peuvent pas s'appuyer sur un cache DNS partagé pour empêcher un adversaire contrôlant le trafic d'une perspective de réseau d'empoisonner le cache DNS utilisé par d'autres perspectives de réseau).

L'infrastructure de réseau fournissant la connectivité Internet à une perspective de réseau est administrée par la même organisation que celle qui fournit les services informatiques nécessaires au fonctionnement de la perspective de réseau. Toutes les communications entre une perspective de réseau distante et l'autorité de certification s'effectuent sur un canal authentifié et crypté reposant sur des protocoles modernes (par exemple, HTTPS).

Une perspective de réseau peut utiliser un résolveur DNS récursif qui n'est pas colocalisé avec la perspective de réseau. Toutefois, le résolveur DNS utilisé par la perspective de réseau doit se trouver dans la même région de service du registre Internet régional que la perspective de réseau qui s'appuie sur lui. En outre, pour toute paire de résolveurs DNS utilisée lors d'une tentative de corroboration d'émission multi-perspectives, la distance en ligne droite entre les deux résolveurs DNS doit être d'au moins 500 km. L'emplacement d'un résolveur DNS est déterminé par le point où les requêtes DNS sortantes non encapsulées sont généralement transmises pour la première fois à l'infrastructure de réseau fournissant la connectivité Internet à ce résolveur DNS. L'AC peut immédiatement réessayer la corroboration de l'émission multi-perspective en utilisant la même méthode de validation ou une autre méthode (par exemple, l'AC peut immédiatement réessayer la validation en utilisant « Email to DNS TXT Contact » si « Agreed-Upon Change to Website - ACME » ne corrobore pas le résultat de la corroboration de l'émission multi-perspective).

Lors de la nouvelle tentative de corroboration d'émission multi-perspective, l'AC ne peut pas s'appuyer sur les corroborations des tentatives précédentes. Il n'existe aucune stipulation concernant le nombre maximal de tentatives de validation pouvant être effectuées au cours d'une période donnée.

Le tableau « Exigences en matière de quorum » décrit les exigences en matière de quorum liées à la corroboration d'émission multi-perspectives. Si l'AC ne s'appuie pas sur le même ensemble de perspectives réseau pour les vérifications d'autorisation ou de contrôle de domaine et d'enregistrement CAA, les exigences en matière de quorum sont remplies pour les deux ensembles de perspectives réseau (c'est-à-dire l'ensemble d'autorisation ou de contrôle de domaine et l'ensemble de vérification d'enregistrement CAA). Les perspectives réseau sont considérées comme distinctes lorsque la distance en ligne droite entre elles est d'au moins 500 km. Les perspectives réseau sont considérées comme « distantes » lorsqu'elles sont distinctes de la perspective réseau principale et des autres perspectives réseau représentées dans un quorum.

L'AC peut réutiliser des preuves corroborantes pour la conformité du quorum des enregistrements CAA pendant un maximum de 398 jours. Après avoir émis un certificat pour un domaine, les perspectives réseaux distantes peuvent omettre la récupération et le traitement des enregistrements CAA pour le même domaine ou ses sous-domaines dans les demandes de certificat ultérieures du même demandeur pendant un maximum de 398 jours.

Exigences du Quorum	
Nombre de perspective réseau distinctes utilisées	**Nombre de non-corrobotations autorisé**
2-5	1
6+	2

Perspectives de réseau distantes effectuant une corroboration d'émission multi-perspectives :

- Renforcement du réseau : s'appuyer sur les réseaux (par exemple, les fournisseurs de services Internet ou les réseaux de fournisseurs de cloud) mettant en œuvre des mesures pour atténuer les incidents de routage BGP dans le système de routage Internet mondial pour fournir une connectivité Internet à la perspective réseau.

L'AC mettra en œuvre la corroboration d'émission multi-perspectives en utilisant au moins :

- **Deux (2)** perspectives réseau distantes. L'AC peut procéder à la délivrance du certificat si le nombre de perspectives réseau distantes qui ne corroborent pas les déterminations faites par la perspective réseau principale (« non-corroborations ») est supérieur à celui autorisé dans le tableau des exigences de quorum. **En vigueur le 15 mars 2025**
- **Deux (2)** perspectives réseau distantes. L'AC ne procédera pas à la délivrance du certificat si le nombre de non-corroborations est supérieur à celui autorisé dans le tableau des exigences de quorum. **En vigueur le 15 septembre 2025**
- **Trois (3)** perspectives réseau distantes. **En vigueur le 15 mars 2026**
- **Quatre (4)** perspectives réseau distantes. **En vigueur le 15 juin 2026**
- **Cinq (5)** perspectives réseau distantes. **En vigueur le 15 décembre 2026**

L'AC ne procède pas à l'émission de certificats si le nombre de non-corroborations est supérieur à celui autorisé dans le tableau des exigences de quorum et si les perspectives de réseau distantes qui corroborent les déterminations faites par la perspective de réseau principale ne se situent pas dans les régions de service d'au moins deux (2) registres Internet régionaux distincts.

3.2.3 Validation de l'identité d'un individu

La vérification de l'identité d'un individu cible :

- Un Responsable de Certificat de personne morale ;
- Le représentant légal de l'organisation rattachée au certificat, le cas échéant ;
- Le mandataire de certification associée à l'organisation, le cas échéant.

L'AC collecte et conserve les preuves relatives aux attributs suivants d'identité du RC :

- Prénom(s) et nom(s) qui constituent le nom utilisé ;
- Toute information complémentaire nécessaire pour identifier le RC.

Pour authentifier l'identité d'un individu, la vérification de la photocopie d'un élément d'identification de l'individu est nécessaire. Il peut s'agir d'une pièce d'identité (Carte nationale d'identité, passeport ou carte de séjour), 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), ou d'une référence au dossier administratif de l'agent. Cet élément d'identification doit être valide et être présumé authentique ou l'AC doit pouvoir présumer qu'il existe selon une source faisant autorité. L'AC inspecte la copie pour rechercher toute altération ou falsification qui aurait été

effectuée. L'existence de l'identité alléguée est connue d'une source faisant autorité et l'AC doit pouvoir présumer que la personne est bien celle qu'elle prétend être. 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.

3.2.3.1 Certificat d'AC

L'enregistrement d'une nouvelle demande de certificat d'AC est réalisé auprès de l'AE par le responsable de l'Autorité de certification. Cette demande est formalisée au travers du script rempli lors de la cérémonie des clés ayant servi à la génération du certificat.

3.2.3.2 Certificat de personne morale

L'enregistrement du service applicatif ou du serveur auquel un certificat doit être délivré se fait via l'enregistrement du RC correspondant. Un RC peut être amené à changer en cours de validité du certificat du service ou du 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 service applicatif ou du serveur correspondant, peut se faire soit directement auprès de l'AE, d'un AED, ou d'un MC de l'entité. Dans ce dernier cas, le MC doit être préalablement enregistré par l'AE.

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 service ou serveur considéré et pour l'entité considérée.

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

3.2.3.2.1 Enregistrement d'un RC

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	
Objet	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 rattachée au service ou serveur
	Désignation des CGVU applicables
Date	Signature du formulaire de moins de 3 mois
Signature	Signature d'un représentant légal de l'entité ou d'un MC pour habiliter le futur RC Signature du futur RC pour accepter le rôle de RC et les CGVU

Pièce d'identité officielle du RC	
Objet	La photocopie d'un élément d'identification du RC en cours de validité, reconnu par l'Etat membre dans lequel est déposée la demande de certificat.
Date	Pièce valide au moment de l'enregistrement

Pièce d'identité officielle du Représentant légal ou du MC	
Objet	La photocopie d'un élément d'identification du représentant légal ou du MC de l'entité rattachée au certificat, en cours de validité, reconnu par l'Etat membre dans lequel est déposée la demande de certificat.
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. *Ex : un exemplaire des statuts de l'entreprise, en cours de validité, portant signature de ses représentants.* **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

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. *Ex : extrait KBIS ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements*
Date	Justificatif valide au moment de l'enregistrement

EN 319 411-2 QNCP-w

L'authentification du RC par l'AE est réalisée via l'un des moyens suivants :

- Authentification en face à face physique avec le RC avec présentation d'une pièce d'identité valide lors du face-à-face (Carte nationale d'identité, Passeport ou Carte de séjour).
- Authentification du RC à distance à l'aide d'un moyen d'identification électronique qualifié au niveau substantiel ou élevé au sens du règlement eIDAS.

- Authentification du RC à l'aide d'une méthode d'identification reconnue au niveau national qui fournit une garantie équivalente en termes de fiabilité à la présence en personne. La garantie équivalente est confirmée par un organisme d'évaluation de la conformité.
- Authentification du RC à l'aide d'un certificat de signature électronique qualifié au sens du Règlement eIDAS.

EN 319 411-2 QEVCP-w

L'authentification du RC par l'AE est réalisée lors d'un face-à-face physique lors duquel sont contrôlés les éléments suivants :

- 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 règlementé contenant une date d'expiration et qui n'est pas expirée ;
    - Un relevé de compte bancaire d'un établissement bancaire règlementé 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 fixe 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.

EN 319 411-1 OVCP

L'authentification du 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).

RGS *

L'authentification du 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).

3.2.3.3 Enregistrement d'un Mandataire de Certification

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 MC 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 du MC	
Objet	Désignation d'un représentant légal de l'entité et de ses coordonnées
	Désignation du futur MC habilité et de ses coordonnées
	Désignation de l'identité de l'entité à laquelle est rattaché le MC
Date	Signature du formulaire de moins de 3 mois
Signature	Signature d'un représentant légal de l'entité pour habiliter le futur MC Signature du futur MC pour accepter le rôle de MC et les CGVU

Lettre d'engagement du MC	
Objet	Désignation du futur MC habilité et de ses coordonnées
	Désignation du rôle et des responsabilités du MC 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.
Date	Signature du formulaire de moins de 3 mois
Signature	Signature du futur MC pour s'engager à respecter ces responsabilités

Pièce d'identité officielle du MC	
Objet	La photocopie d'un élément d'identification du MC en cours de validité, reconnu par l'Etat membre dans lequel est déposée la demande de certificat.
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. *Ex : un exemplaire des statuts de l'entreprise, en cours de validité, portant signature de ses représentants.* **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

EN 319 411-2 QNCP-w
EN 319 411-2 QEVCP-w

L'authentification du MC par l'AE est réalisée via l'un des moyens suivants :

- Authentification en face à face physique avec le MC avec présentation d'une pièce d'identité valide lors du face-à-face (Carte nationale d'identité, Passeport ou Carte de séjour).
- Authentification du MC à distance à l'aide d'un moyen d'identification électronique qualifié au niveau substantiel ou élevé au sens du règlement eIDAS.

- Authentification du MC à l'aide d'une méthode d'identification reconnue au niveau national qui fournit une garantie équivalente en termes de fiabilité à la présence en personne. La garantie équivalente est confirmée par un organisme d'évaluation de la conformité. - Authentification du MC à l'aide d'un certificat de signature électronique qualifié au sens du Règlement eIDAS.
EN 319 411-1 OVCP RGS *
L'authentification du MC par l'AE s'effectue via l'envoi du dossier papier par courrier accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, MC). Cette authentification peut également se faire sous forme dématérialisée à condition que les différentes pièces justificatives du dossier soient signées à l'aide d'un procédé de signature électronique conforme aux exigences du niveau RGS * et que la signature soit vérifiée et valide au moment de l'enregistrement. Si le mandataire n'est pas équipé d'un certificat de niveau RGS * ou supérieur, les dossiers ne pourront être envoyés sous forme dématérialisée. Dans ce cas, chaque dossier ne sera validé qu'après réception des documents originaux par courrier.

3.2.4 Informations non vérifiées

Sans objet.

3.2.5 Validation de l'autorité du demandeur et des signatures

Cette étape est effectuée en même temps que la validation de l'identité du représentant légal et du RC (directement par l'AE ou par le MC).

3.2.6 Critères d'interopérabilité

L'AC divulgue tous les certificats croisés qui identifient l'AC en tant que sujet, à condition que l'AC ait organisé ou accepté l'établissement de la relation de confiance (c'est-à-dire le certificat croisé en cause).

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

3.3.1 Identification et authentification d'une demande de renouvellement courant

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

3.3.1.1 Certificat d'AC

L'identification et l'authentification d'une demande de renouvellement courant de certificat d'AC sont identiques à la demande initiale.

3.3.1.2 Certificat de personne morale

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.

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

Les documents fournis pour valider l'identité du sujet, du MC, du représentant légal et de l'entité peuvent être utilisés conformément aux exigences de la section 4.2.1.2.

Pour la validation des noms de domaine conformément à la section 3.2.2.4, toute donnée, tout document ou toute validation complète utilisée est obtenue au plus tard dans le délai décrit à la section 4.2.1.2.

EN 319 411-1 OVCP EN 319 411-2 QNCP-w EN 319 411-2 QEVCP-w
Lors du premier renouvellement et des suivants, l'AC vérifie que le demandeur a toujours le contrôle du domaine via l'une des méthodes utilisées pour la demande initiale.

3.3.2 Identification et authentification pour un renouvellement après révocation

L'identification et l'authentification d'une demande de renouvellement après révocation sont identiques à la demande initiale.

3.4 Identification et authentification d'une demande de révocation

3.4.1 Certificat d'AC

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.

3.4.2 Certificat de personne morale ou physique

3.4.2.1 Demande de révocation courante

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 https://www.certigna.com. Le demandeur s'authentifie en joignant la photocopie de sa pièce d'identité au courrier envoyé.
- Depuis l'espace client du site CERTIGNA https://www.certigna.com en sélectionnant le certificat à révoquer ;
- Au travers du service ACME en envoyant une requête de révocation du certificat.

L'adresse postale du service de révocation est disponible sur le site de CERTIGNA https://www.certigna.com

La demande papier doit comporter les éléments suivants :

- Le prénom et le nom du serveur concerné ;
- L'adresse e-mail du RC le cas échéant ;
- 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

4.1.1.1 Certificat d'AC

La demande de certificat doit émaner d'un représentant légal de l'AC.

4.1.1.2 Certificat de personne morale ou physique

Pour les certificats rattachés à une organisation, 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

4.1.2.1 Certificat d'AC

Le dossier de demande est établi directement par le responsable de l'AC lors de la Cérémonie des clés.

4.1.2.2 Certificat de personne morale ou physique

Le dossier de demande est établi soit directement par le futur RC à partir des éléments fournis par son entité le cas échéant, 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 email lors de son enregistrement, pour que l'AE puisse prendre contact avec ce dernier pour toute question relative à l'enregistrement des RC. Le dossier de demande de certificat doit contenir les éléments décrits au chapitre 3.2.3. 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.

Les justificatifs fournis pour valider l'identité du RC, du Représentant Légal et de l'entité peuvent être utilisés pendant l'une des périodes indiquées au chapitre 4.2.1.2 pour émettre un certificat, sous réserve qu'ils soient encore valides au moment de la validation de la demande du certificat. Pour la validation des noms de domaine conformément à la section 3.2.2.4, toute donnée, tout document ou toute validation complète utilisée est obtenue au plus tard sous l'une des périodes indiquées au chapitre 4.2.1.2

Un certificat nécessitant l'authentification du RC au moyen d'un face-à-face physique, d'un eID, ou d'une signature électronique à l'aide d'un certificat qualifié eIDAS, ne peut être renouvelé qu'après une nouvelle authentification du RC via l'un de ces procédés. Le procédé utilisé pour le renouvellement (Ex : certificat qualifié eIDAS pour signer électroniquement la demande de renouvellement) doit lui-même avoir été remis sur la base de la réalisation d'un face-à-face physique.

4.2 Traitement d'une demande de certificat

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

4.2.1.1 Certificat d'AC

La demande est validée par l'ensemble des témoins présents lors de la cérémonie des clés parmi lesquels figurent obligatoirement un administrateur de l'AE.

4.2.1.2 Certificat de personne morale ou physique

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 ;
- Validation de l'identité de l'entité ;
- Validation de l'identité des signataires de la demande (RC, représentant légal ou MC) ;
- Validation de l'autorisation d'émettre un certificat pour ce serveur ;
- Validation du contrôle du domaine pour un serveur ;
- 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.

Les documents fournis pour valider l'identité du Porteur, du RC, du représentant légal et de l'entité peuvent être utilisés pendant l'une des périodes définies dans le tableau ci-dessous, pour délivrer un certificat, à condition qu'ils soient encore valides au moment de la validation de la demande de certificat.

Certificat émis	Période pendant laquelle les documents d'identité valides sont réutilisables
Avant le 15 mars 2026	825 jours
Après le 15 mars 2026	398 jours

Pour la validation des noms de domaine conformément à la section 3.2.2.4, toutes les données, tous les documents ou toutes les validations utilisées sont réutilisables pour délivrer un nouveau certificat pendant l'une des périodes du tableau ci-dessous.

Certificat émis		Période pendant laquelle la validation du nom de domaine est réutilisable
Après le	Et avant le	
	15 mars 2026	398 jours
15 mars 2026	15 mars 2027	200 jours
15 mars 2027	15 mars 2029	100 jours
15 mars 2029		10 jours

Toutes les opérations citées ci-dessus sont réalisées par l'AE, mais dans le cas d'une demande réalisée via un opérateur d'AED ou un MC, ces derniers retransmettent le dossier à l'AE après avoir effectué les contrôles suivants :

- S'assurer que le RC a pris connaissance des CGVU, en complément de leur diffusion opérée par l'AC ;
- Vérifier l'identité du RC et les pièces originales attestant de son identité afin de l'identifier et de l'authentifier ;
- Vérifier l'exhaustivité du dossier de demande.

L'AE s'assure que la demande correspond au mandat de l'opérateur d'AED ou du MC. Dans tous les cas, le dossier de demande est archivé par l'AE. L'identité du futur RC et du représentant légal est approuvée si les pièces justificatives fournies sont valides à la date de réception.

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).

Conformément à la RFC 8659, des contrôles sont réalisés sur l'enregistrement CAA (cf. chapitre 3.2.2.8.

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. Ces pratiques sont portées par l'AC et ne sont pas déléguées aux tiers (Ex : AED).

4.2.2 Acceptation ou rejet de la demande de certificat

Après traitement de la demande, 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 ;

En cas d'acceptation par l'AE, après génération du certificat par l'AC, l'AE envoie un mail au RC pour effectuer l'acceptation du certificat et la récupération de données d'activation.

L'AC n'émet pas de certificat SSL/TLS de serveurs sur internet contenant des noms internes, d'adresses IP réservées, un nom de domaine qui se terminant par un suffixe de zone IP inversée ou contenant un nouveau gTLD en cours d'étude par l'ICANN.

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.

CERTIGNA SERVICES CA	*Authentification web*
EN 319 411-2 QEVCP-w	
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.	

4.2.3 Durée d'établissement du certificat

4.2.3.1 Certificat d'AC

La demande de certificat d'AC étant formellement établie lors de la cérémonie des clés, le certificat concerné est généré dans les heures qui suivent la demande.

4.2.3.2 Certificat de personne morale

A compter de la réception du dossier d'enregistrement complet et de la demande électronique (CSR), le certificat est établi dans un délai de 30 jours.

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 ».

4.3.1.1 Autorisation manuelle de délivrance de certificat d'AC racines

Les bi-clés et certificats de l'AC racine et les AC intermédiaires sont générées lors de cérémonie des clés. Les opérations de génération et de signature des certificats émis par l'AC racine sont effectuées dans les mêmes circonstances contrôlées que la génération des bi-clés d'AC (cf. 6.1.1), en présence de personnes dans des rôles de confiance autorisées par l'AC (Ex : Opérateur système d'AC, Officier de sécurité, Administrateur PKI) et dans le cadre de « cérémonies de clés ». L'administrateur d'AC effectue les commandes de génération et de signature des certificats par l'AC racine en présence des rôles de confiance qui s'assurent de la conformité des pratiques avec les exigences de sécurité et le script défini.

4.3.1.2 Vérification du contenu de certificat à signer

En raison de la complexité de la mise en œuvre des profils de certificats conformes aux exigences, à compter du 15/03/2025, l'AC implémente systématiquement un processus de vérification pour évaluer la conformité technique de chaque artefact à signer avant de le signer.

4.3.1.3 Vérification des certificats émis

L'AC utilise un processus de vérification de chaque certificat de serveur émis.

4.3.2 Notification par l'AC de la délivrance du certificat

4.3.2.1 Certificat d'AC

La remise du certificat d'AC est réalisée lors de la cérémonie des clés, auprès d'un administrateur de l'AC habilité par l'AC en charge de son exploitation et de sa diffusion.

4.3.2.2 Certificat de personne morale

Le certificat complet et exact est mis à disposition de son RC depuis l'espace client ou sur le dispositif remis par l'AC le cas échéant. Le RC s'authentifie sur son espace client pour accepter son certificat ou remplit le formulaire d'acceptation au format Papier.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

4.4.1.1 Certificat d'AC

Le représentant de l'autorité et les différents témoins, présents lors la cérémonie, contrôlent que le contenu du certificat est conforme à la demande. L'acceptation est formalisée au travers du procès-verbal de la cérémonie des clés.

4.4.1.2 Certificat de personne morale ou physique

L'acceptation du certificat est effectuée par le RC, depuis son espace client et préalablement au téléchargement de son certificat ou à la récupération de la donnée d'activation de son support. Le RC choisit explicitement d'accepter ou non le certificat et la notification d'acceptation ou de refus est transmise automatiquement à l'AC. Dans le cadre de l'usage du Service ACME, le certificat est tacitement accepté par le RC.

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

4.4.2.1 Certificat d'AC

Les certificats d'AC Racine et d'AC intermédiaires sont publiés par l'AC. Cf. chapitre 2.

4.4.2.2 Certificat de personne morale

Préalablement à l'émission du certificat du serveur, un précertificat similaire au certificat est émis et enregistré auprès des journaux publics liés au dispositif « Certificate Transparency », afin d'assurer la reconnaissance des certificats d'authentification de serveurs par les navigateurs. La liste des journaux utilisés et publiant le précertificat est fournie au chapitre 7.2 de ce document.

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

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

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

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat

L'AC ou le RC doit respecter strictement les usages autorisés des bi-clés et des certificats décrits au chapitre 1.5.1. 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 le cas échéant.

Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du RC 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 https://www.certigna.com.

Les CGVU acceptées lors de la demande de certificat restent applicables pendant toute la durée de vie du certificat. Dans le cas de l'usage du service ACME pour une demande de certificat d'authentification web SSL/TLS, le RC accepte à la première demande les CGVU applicables via le site https://www.certigna.com. Le RC est ensuite informé automatiquement par mail de l'application de nouvelles CGVU qu'il accepte tacitement en maintenant l'utilisation du service ACME pour toute nouvelle demande de certificat.

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 et cités au chapitre 1.5.1. 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). Dans le cas où le RC génère la bi-clé, il s'engage en acceptant les CGVU, à générer une nouvelle bi-clé à chaque demande.

4.6.1 Circonstance pour le renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification de la délivrance d'un nouveau certificat

Sans objet.

4.6.5 Modalité d'acceptation d'un nouveau certificat

Sans objet.

4.6.6 Publication du renouvellement du certificat par l'AC

Sans objet.

4.6.7 Notification de la délivrance par l'AC aux autres entités

Sans objet.

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 AC et serveurs, et les certificats correspondants, sont renouvelés régulièrement (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 certificat.

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. 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 RC qui lui est rattaché.

4.7.3 Traitement d'une demande de changement de clé

Cf. chapitre 4.2.1

4.7.4 Notification de la délivrance d'un nouveau certificat

Cf. chapitre 4.3.2.

4.7.5 Modalité d'acceptation d'un nouveau certificat

Cf. chapitre 4.4.1.

4.7.6 Publication du renouvellement du certificat par l'AC

Cf. chapitre 4.4.2.

4.7.7 Notification de la délivrance par l'AC aux autres entités

Cf. chapitre 4.4.3.

4.8 Modification du certificat

La modification des certificats d'AC ou de serveur 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.

4.8.1 Circonstance pour la modification d'un certificat

Sans objet.

4.8.2 Origine d'une demande de modification de certificat

Sans objet.

4.8.3 Traitement d'une demande de modification de certificat

Sans objet.

4.8.4 Notification de la délivrance d'un nouveau certificat

Sans objet.

4.8.5 Modalité d'acceptation d'un certificat modifié

Sans objet.

4.8.6 Publication du certificat modifié par l'AC

Sans objet.

4.8.7 Notification de la délivrance par l'AC aux autres entités

Sans objet.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Raisons pour révoquer un certificat de personne morale

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat par l'AC dans les vingt-quatre (24) heures :

- **La compromission de la clé** (RFC 5280 CRLReason #1) :
  - Le RC ou 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 car il a raison de croire que la clé privée du certificat a été compromise, par exemple une personne non autorisée ayant eu accès à la clé privée du certificat ;
  - L'AC obtient la preuve que la clé privée correspondant à la clé publique du certificat est suspectée de compromission, est compromise,
  - L'AC est informée d'une méthode démontrée ou éprouvée qui peut facilement calculer la clé privée du serveur sur la base de la clé publique du certificat, y compris, mais sans s'y limiter, celles identifiées à la section 6.1.1.3 ;
  - L'AC est informée par une démonstration ou une méthode éprouvée que la clé privée est compromise ou il y une preuve évidente que la méthode spécifique pour générer la clé privée était défectueuse. Des méthodes ont été développées qui peuvent aisément permettre de la calculer sur la base de la clé publique incluant notamment celle

- **Le retrait de privilège** (RFC 5280 CRLReason #9) :
  - Le représentant légal de l'entité à laquelle le serveur appartient ou le RC informe l'AC que la demande de certificat originelle n'était pas autorisée et n'a pas obtenu d'autorisation rétroactive ;
  - L'AC obtient la preuve que l'usage du certificat est détourné ;
  - L'AC est informée d'un changement dans les informations contenues dans le certificat ;
  - L'AC est informée que le RC n'a pas respecté toute ou partie des dispositions du contrat ou une ou plusieurs de ses obligations en vertu des CGVU ;
  - L'AC est informée qu'un certificat Wildcard a été utilisé pour authentifier un FQDN subordonné frauduleusement trompeur.
  - L'AC détecte ou est informée que les informations apparaissant dans le certificat sont inexactes ou trompeuses ;
  - Le support cryptographique utilisé pour stocker le certificat et la clé privée du serveur n'est pas conforme ou ne sera plus conforme aux exigences du chapitre 11 de cette PC/DPC (Ex : une qualification ou certification ne serait plus maintenue ou serait suspendue) ;

- **L'arrêt des opérations** (RFC 5280 CLReason #5)
  - 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),

- L'arrêt définitif serveur ou la cessation d'activité de l'entité du RC ;
- Le RC n'a plus le contrôle ou n'est plus autorisé à utiliser les noms de domaines figurant dans le certificat ;
- Le RC ne peut plus utiliser le certificat parce qu'il interrompt le site web.

- **Le changement d'affiliation** (RFC 5280 CLReason #3)
  - Les informations du serveur figurant dans le certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple, modification de l'identité du serveur), ceci avant l'expiration normale du certificat ;

- **Le remplacement ou l'annulation du certificat** (RFC 5280 CLReason #4)
  - L'AC obtient la preuve que la validation de l'autorisation du domaine ou du contrôle d'un ou plusieurs FQDN dans le certificat n'est pas fiable, y compris les cas où l'AC n'a pas effectué correctement la vérification CAA ou lorsque la délivrance n'était pas autorisée conformément à la section 3.2.2.8 (Enregistrements CAA),
  - Le certificat n'est plus conforme aux exigences des chapitres 6.1.5 et 6.1.6 de cette PC/DPC ;
  - L'AC est informée que le certificat n'a pas été émis en conformité avec les exigences et pratiques formulées dans la PC/DPC ;
  - Le RC, l'entité, le cas échéant le MC ou l'opérateur d'AED, n'a pas respecté ses obligations découlant de la PC/DPC ;
  - Le RC a demandé un nouveau certificat pour remplacer un certificat existant.

- **Une autre raison de révocation qui résulte de l'absence d'extension « reasonCode » dans la CRL :**
  - Le RC, ou le représentant légal de l'entité à laquelle il appartient, demande par écrit, sans spécifier une raison de révocation, que l'AC révoque le certificat.
  - L'AC obtient la preuve que la clé privée correspondant à la clé publique du certificat est perdue ou volée (ou éventuellement les données d'activation associées à la clé privée) ;
  - Le RC, ou 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 et/ou de son support) ;
  - Le droit de l'AC de délivrer des certificats sous les exigences du CA/Browsers Forum expire ou est révoqué ou terminé, à moins que l'AC ait prévu de continuer le maintien des services de CRL/OCSP ;
  - La révocation est requise par cette PC/DPC pour une raison qui ne nécessite pas d'être spécifiée dans ce présent chapitre ;
  - 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 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.

- Une erreur (intentionnelle ou non) a été détectée dans la demande de certificat et le dossier d'enregistrement correspondant ;
- Pour des raisons techniques (échec de l'envoi du certificat, …).

4.9.1.2 Raisons pour révoquer un certificat d'AC

Une ou plusieurs des circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'AC racine ou intermédiaire sous 7 jours :

- L'AC demande la révocation du certificat ;
- L'AC notifie l'AC émettrice que la demande de certificat originale n'était pas autorisée et n'accorde pas d'autorisation rétroactive ;
- L'AC obtient la preuve que la clé privée de l'AC correspondant à la clé publique dans le certificat est compromise ou n'est plus conforme avec les exigences des chapitres 6.1.5 et 6.1.6 ;
- L'AC obtient la preuve que l'usage du certificat d'AC est détourné ;
- L'AC est informée que le certificat d'AC n'a pas été émis en conformité avec les exigences et pratiques formulées dans la présente PC/DPC ;
- L'AC détermine que les informations apparaissant dans le certificat d'AC sont inexactes ou trompeuses ;
- L'AC cesse toute activité pour une raison quelconque ;
- Le droit de l'AC de délivrer des certificats sous les exigences du CA/Browsers Forum expire ou est révoqué ou terminé, à moins que l'AC ait prévu de continuer le maintien des services de CRL/OCSP.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificat d'AC

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.

4.9.2.2 Certificat de personne morale

Les personnes ou entités qui peuvent demander la révocation d'un certificat sont :

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

Le RC est informé, en particulier par le biais des CGVU qu'il a acceptées, des personnes ou entités susceptibles d'effectuer une demande de révocation pour le certificat dont il a la responsabilité. En complément, des demandeurs, des fournisseurs de services applicatifs ou des tiers peuvent remonter auprès de l'AC un rapport de problème sur un certificat afin de l'informer d'une cause raisonnable pour le révoquer.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Certificat d'AC

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

Le contact identifié sur le site de l'ANSSI (https://www.ssi.gouv.fr) est immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification. Le mécanisme de révocation est décrit dans la « Procédure opérationnelle de demande de révocation ». Le processus est détaillé dans la « Procédure de gestion des clés cryptographiques » et dans la « Procédure de gestion des certificats de composante ».

4.9.3.2 Certificat de personne morale

La demande de révocation est effectuée auprès de l'AE, d'un MC ou de l'AC. L'AC fournit un processus disponible 24H/24, 7J/7 pour demander la révocation des certificats depuis son espace client. 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 ;
- 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.

Si la demande est effectuée en ligne, l'habilitation de la personne à effectuer cette demande est vérifiée. En l'occurrence la personne à l'origine de la demande peut être :

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

Les étapes sont les suivantes :

- Le demandeur de la révocation transmet sa demande à l'AE, par courrier ou en ligne ;
- L'AE authentifie et valide la demande de révocation selon les exigences du 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 est en mesure de révoquer un certificat supposé exister, si la révocation du certificat est requise en vertu de cette PC/DPC, même si le certificat final n'existe pas réellement. L'AC fourni des services et des réponses CRL et OCSP conformément à la présente PC pour tous les certificats présumés exister sur la base de la présence d'un précertificat, même si le certificat n'existe pas réellement.

A compter du 01/10/2022, la cause de révocation d'un certificat sera publiée dans la LCR lorsque l'une des raisons de révocation suivantes est utilisée :
- La compromission de la clé ;
- Le retrait de privilège ;
- L'arrêt des opérations ;
- Le changement d'affiliation ;
- Le remplacement ou l'annulation du certificat.

Le RC est informé de la publication de la cause de révocation lors de sa demande afin d'obtenir son accord. Si aucune de ces causes de révocation n'est sélectionnée, le champ « CRLReason » est fixé à « Unspecified (0) » par défaut et aucune extension « ReasonCode » n'est placée dans la CRL.

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 : 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.com/contactez-nous/ et sélectionner l'objet « Certificat jugé malveillant ou dangereux ».

4.9.4 Délai accordé 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

4.9.5.1 Certificats d'AC

La révocation d'un certificat d'AC 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) 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 ».

4.9.5.2 Certificat de personne morale

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.

Dans les 24 heures qui suivent la réception d'un signalement relatif à un problème de certificat, l'AC investigue les faits et circonstances relatées et fournit un rapport préliminaire sur ses investigations au RC et à l'entité qui a émis le signalement. Après l'analyse des faits et circonstances, l'AC travaille avec le RC et avec l'entité ayant déposé le signalement ou tout autre avis relatif à la révocation afin de déterminer si oui ou non le certificat sera révoqué, et le cas échéant, la date à laquelle l'AC révoquera le certificat. Le délai entre la réception du signalement ou l'avis relatif à la révocation, et la publication de la révocation n'excédera pas le délai évoqué au chapitre 4.9.1. La date sélectionnée par l'AC peut notamment prendre en compte les critères suivants :

- La nature du problème allégué (périmètre, contexte, gravité, ampleur, risque de préjudice) ;
- Les conséquences de la révocation (les impacts directs ou collatéraux pour le Responsable de Certificat et les tiers) ;
- Le nombre de signalement réceptionné concernant un certificat ou un Responsable de certificat particulier ;
- L'entité qui dépose la plainte (par exemple, une plainte émanant d'un agent de la force publique qui affirme qu'un site Web se livre à des activités illégales est jugé plus pertinent qu'une plainte d'un consommateur alléguant qu'il n'a pas reçu les biens qu'il avait commandé);

La législation applicable.

La fonction de gestion des révocations est disponible 24h/24 7J/7 pour les révocations en ligne.

RGS *
La durée maximale d'indisponibilité de la fonction de gestion des révocations est : - Par interruption (panne ou maintenance) de 2 heures (jours ouvrés) ; - Par mois de 16 heures (jours ouvrés).

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

L'utilisateur d'un certificat de 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

Les CRL sont disponibles via une URL http accessible publiquement (cf. chapitres 2.2.5 et 2.2.6).

Dans les vingt-quatre (24) heures suivants l'émission du premier certificat, l'AC génère et publie une LCR complète.

La LAR est émise au minimum tous les ans. En outre, une nouvelle LAR est systématiquement générée et publiée sous vingt-quatre (24) heures après la révocation d'un certificat d'AC.

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

L'AC continue d'émettre des LCR jusqu'à ce que tous les certificats d'AC intermédiaires contenant la même clé publique du sujet soient expirés ou révoqués, ou que la clé privée de l'AC intermédiaire correspondante est détruite.

4.9.8 Délai maximum de publication d'une LCR

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

4.9.9 Disponibilité de 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 conforme à la RFC 6960 et/ou à la RFC 5019. Le répondeur OCSP répond aux exigences d'intégrité, de disponibilité et de délai pour la publication décrite dans cette PC/DPC.

La durée de validité d'une réponse OCSP correspond à l'intervalle de temps compris entre les champs « thisUpdate » et « nextUpdate », inclus. Aux fins du calcul de cet intervalle, une différence de 3 600 secondes équivaut à une heure, et une différence de 86 400 secondes équivaut à un jour, sans tenir compte des secondes intercalaires.

Un numéro de série de certificat est considéré comme « assigned » si :

- un certificat ou un précertificat portant ce numéro de série a été émis par l'autorité de certification émettrice ; ou
- un précertificat portant ce numéro de série a été émis par un certificat de signature de précertificat, associé à l'autorité de certification émettrice.

Un numéro de série de certificat est considéré comme « unassigned» s'il n'est pas « assigned ».

Pour connaître le statut d'un certificat de serveurs ou du précertificat correspondant, une réponse OCSP faisant autorité est disponible (c'est-à-dire que le répondeur ne doit pas renvoyer le statut « unknown ») au plus tard 15 minutes après la première publication ou la mise à disposition du certificat ou du précertificat.

Les informations fournies par le répondeur OCSP pour les certificats de serveurs sont mises à jour au plus tard tous les quatre (4) jours, et les réponses OCSP sont valides pendant sept (7) jours. L'autorité de certification fournit une réponse OCSP mise à jour au moins huit heures avant la prochaine mise à jour (nextUpdate) et au plus tard quatre jours après la mise à jour actuelle (thisUpdate).

Les informations fournies par le répondeur OCSP pour les certificats d'AC intermédiaires sont mises à jour tous les douze (12) mois au maximum et sous 24 heures après la révocation du certificat de l'AC intermédiaire

Les répondeurs OCSP exploités par l'autorité de certification prennent en charge la méthode « HTTP GET », telle que décrite dans les RFC 6960 et/ou RFC 5019. Les réponses OCSP sont signées par un répondeur OCSP dont le certificat est signé par l'AC qui délivre le certificat dont l'état de révocation est vérifié. Les réponses OCSP sont signées par un répondeur OCSP conforme au profil de certificat de répondeur OCSP de la section 7.3. Le certificat du répondeur OCSP contient une extension de type « id-pkix-ocsp-nocheck », telle que définie par la RFC6960.

4.9.10 Exigences sur la vérification en ligne de la révocation

Les certificats révoqués et expirés sont conservés dans les LCR et les répondeurs OCSP.

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

CERTIGNA SERVER AUTHENTICATION ROOT CA	
CERTIGNA SERVER AUTHENTICATION CA	
CERTIGNA SERVER AUTHENTICATION AUTO CA	
CERTIGNA SERVER AUTHENTICATION AUTO FR CA	
OCSP	http://ocsp.certigna.com
CERTIGNA & CERTIGNA ROOT CA	
CERTIGNA SERVICES CA	
OCSP	http://servicesca.ocsp.certigna.fr ou http://servicesca.ocsp.dhimyotis.com
CERTIGNA WILD CA	
OCSP	http://wildca.ocsp.certigna.fr ou http://wildca.ocsp.dhimyotis.com

4.9.11 Autres moyens disponibles d'information sur les révocations

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. Ces dispositions sont formulées à destination des RC notamment au travers des CGVU.

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.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

L'AC, le MC ou 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.). 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 ».

Les méthodes suivantes peuvent être utilisées pour remonter au contact décrit au chapitre 4.9.3.2, la compromission d'une clé privée associée à un certificat CERTIGNA :

- Soumettre une CSR signée par la clé privée et vérifiable avec la clé publique ;
- Soumettre un fichier de test signé par la clé privée et vérifiable avec la clé publique ;
- Fournir des références aux sources de vulnérabilités et/ou d'incident de sécurité à partir desquelles la compromission est vérifiable ;
- Soumettre la clé privée compromise à CERTIGNA. Cette méthode n'est pas recommandée mais sera considérée comme preuve de compromission.

CERTIGNA peut autoriser des méthodes complémentaires qui n'apparaissent pas dans ce chapitre à sa seule discrétion et mettra à jour la PC/DPC si une nouvelle méthode est acceptée.

4.9.13 Suspension de certificat

Les certificats émis par les AC couvertes par cette PC ne peuvent pas être suspendus.

4.9.14 Origine d'une demande de suspension

Non applicable.

4.9.15 Procédure d'une demande de suspension

Non applicable.

4.9.16 Limites de la période de suspension

Non applicable.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

L'AC fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC Racine), c'est à dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR/LAR et l'état du certificat de l'AC Racine. La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR/LAR. Ces LCR/LAR sont des LCR au format V2, publiées sur le site http://www.certigna.com (accessible avec le protocole HTTP).

La CRL et le répondeur OSCP peuvent fournir une réponse différente quant à l'état d'un certificat pendant un délai de 30 minutes maximum après la validation de sa révocation. Pour rappel, lors de validation d'une révocation, le répondeur OCSP est mis à jour aussitôt, tandis que la CRL est produite puis publiée sous 30 minutes maximum. Les activités relatives au service de publication sont définies dans la « Procédure de gestion du service publication ». Les certificats révoqués et expirés ne sont pas supprimés dans les CRL et répondeurs OCSP après leur date d'expiration.

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. L'AC maintient une capacité continue 24 heures sur 24 et 7 jours sur 7 pour répondre en interne à un rapport de problème de certificat malveillant et, le cas échéant, transmettre une telle plainte aux autorités chargées de l'application de la loi et/ou révoquer un certificat faisant l'objet d'une telle plainte.

RGS *
La durée maximale d'indisponibilité de la fonction d'information d'état des certificats est : - Par interruption (panne ou maintenance) de 4 heures (jours ouvrés) ; - Par mois de 32 heures (jours ouvrés).

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

4.10.3 Autres caractéristiques

Sans objet.

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, le certificat est révoqué.

4.12 Séquestre de clé et recouvrement

4.12.1 Politique et pratiques de séquestre de clé et de recouvrement

Le séquestre des clés privées est interdit.

4.12.2 Politique et pratique d'encapsulation de clé de session et de recouvrement

Non applicable.

5 MESURES DE SECURITE 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 PC/DPC a été élaborée en fonction de cette analyse. 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 ».

La présente PC/DPC vise également la conformité aux « Network and Certificate System Security Requirements » en vigueur du CA/Browser Forum.

L'AC élabore, met en œuvre et assure la maintenance d'un système de management de la sécurité de l'information (SMSI) destiné à :

- Protéger la confidentialité, l'intégrité et la disponibilité des données de certificat et des processus de gestion des certificats ;
- Assurer une protection contre les menaces ou les risques anticipés pesant sur la confidentialité, l'intégrité et la disponibilité des données de certificat et des processus de gestion des certificats ;
- Assurer une protection contre tout accès, utilisation, divulgation, altération ou destruction non autorisés ou illicites de toute donnée de certificat ou de tout processus de gestion des certificats ;
- Protéger contre la perte, la destruction ou l'endommagement accidentels de toute donnée de certificat ou de tout processus de gestion des certificats ; et
- Se conformer à toutes les autres exigences de sécurité applicables à l'autorité de certification en vertu de la loi.

Le processus de gestion des certificats inclut :

- des contrôles de sécurité physique et environnementale ;
- des contrôles d'intégrité du système, y compris la gestion de la configuration, le maintien de l'intégrité du code de confiance et la détection/prévention des logiciels malveillants ;
- la sécurité du réseau et la gestion des pare-feux, y compris les restrictions de ports et le filtrage des adresses IP ;
- la gestion des utilisateurs, l'attribution distincte de rôles de confiance, la sensibilisation et la formation ; et
- des contrôles d'accès logiques, la journalisation des activités et des délais d'inactivité pour garantir la responsabilité individuelle.

Le SMSI inclut une évaluation annuelle des risques qui :

- Identifie les menaces internes et externes prévisibles susceptibles d'entraîner un accès non autorisé, une divulgation, une utilisation abusive, une altération ou la destruction de toute donnée de certificat ou de tout processus de gestion des certificats ;
- Évalue la probabilité et les dommages potentiels de ces menaces, en tenant compte de la sensibilité des données de certificat et des processus de gestion des certificats ; et
- Évalue l'adéquation des politiques, procédures, systèmes d'information, technologies et autres dispositifs mis en place par l'autorité de certification pour contrer ces menaces.

Sur la base de l'évaluation des risques, l'autorité de certification élabore, met en œuvre et maintient un SMSI comprenant des procédures, des mesures et des produits de sécurité destinés à atteindre les objectifs énoncés ci-dessus et à gérer et contrôler les risques identifiés lors de l'évaluation des risques, en fonction du niveau de sensibilité des données de certificat et des processus de gestion des certificats.

Le SMSI inclut des mesures de protection administratives, organisationnelles, techniques et physiques adaptées à la sensibilité des données de certificat et des processus de gestion des certificats. Le SMSI tient compte des technologies alors disponibles et du coût de mise en œuvre des mesures spécifiques, et met en œuvre un niveau de sécurité raisonnable adapté au préjudice pouvant résulter d'une violation de la sécurité et à la nature des données à protéger.

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 composantes 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 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 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 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 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'évènements. 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.
- **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. Pour certaines tâches sensibles telles que les opérations sur les HSM (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 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 du personnel 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.

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.

L'AC maintient les traces des formations dispensées et s'assure que les personnels enrôlés comme Officier d'enregistrement maintiennent un niveau de compétence qui leur permet de réaliser leurs missions. L'AC s'assure que les Officiers d'enregistrement possèdent les compétences nécessaires avant de leur permettre de réaliser leurs missions et que chaque Officier d'enregistrement réussisse les évaluations prévues par l'AC sur la vérification des informations en lien avec les exigences du CA/Browser Forum.

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 informatique 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 ;
- Evénements liés à la journalisation : actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

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

- Les accès physiques ;
- Les accès logiques aux systèmes PKI ;
- Les actions réalisées sur les systèmes PKI et de sécurité ;
- Les actions de maintenance et de changement de la configuration des systèmes ;
- L'installation, la mise à jour et la désinstallation de logiciels sur un système de certificats ;
- Les crashes de systèmes, les pannes matériels, et autres anomalies ;
- Les activités des pares-feux et routeurs ;
- Le cycle de vie des supports cryptographiques utilisés pour les clés d'AC ;
- Les changements apportés au personnel ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels des RC).

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

- Evénements liés aux clés de signature et aux certificats d'AC ou aux données d'activation (génération, sauvegarde et récupération, révocation, destruction, destruction des supports, ...) ;
- Ajout de nouveaux profils de certificats et le retrait de profils de certificats existant ;
- Réception d'une demande de certificat (initiale et renouvellement) ;
- Les contrôles réalisés pour la validation de la demande de certificat, incluant :

    - les informations faisant l'objet de la vérification (par exemple, le FQDN faisant l'objet de la demande ou le nom de l'organisation) ;
    - l'autorisation de nom de domaine utilisé (le cas échéant et s'il diffère du FQDN demandé) ; et
    - la méthode de validation utilisée (par exemple, le numéro de section des « TLS Baseline Requirements » du CAB Forum ou le label enregistré d'une méthode de validation ACME) ;
- 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, CGVU, etc.)
- Réception d'une demande de révocation ;
- Validation / rejet d'une demande de révocation ;
- Génération puis publication des LCR ;
- Signature des réponses OCSP (tel que décrit aux chapitres 4.9 et 4.10) ;
- Destruction des supports contenant des renseignements personnels des RC ;
- Tentatives de corroboration de l'émission multi-perspectives de chaque perspective réseau, enregistrant au minimum les informations suivantes :
    - Un identifiant qui identifie de manière unique la perspective réseau utilisée ;
    - Le nom de domaine et/ou l'adresse IP tentés ; et
    - Le résultat de la tentative (par exemple, « validation de domaine réussie/échouée », « autorisation/interdiction CAA »).
- Résultats du quorum de corroboration de l'émission multi-perspectives pour chaque nom de domaine tenté représenté dans une demande de certificat (c'est-à-dire « 3/4 » qui doit être interprété comme « Trois (3) perspectives réseau sur quatre (4) tentées ont corroboré les déterminations faites par la perspective réseau principale).

Le processus de journalisation permet un enregistrement en temps réel des opérations effectuées. Chaque enregistrement d'un événement dans un journal contient au minimum les champs suivants :
- Le type d'événement ;
- La date et heure de l'événement (l'heure exacte des événements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat est enregistrée) ;
- Le nom de l'exécutant ou la référence du système ayant déclenché l'événement (pour imputabilité) ;
- Le résultat de l'événement (réussite ou échec).

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

Les opérations de journalisation sont effectuées au cours du processus. En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'événement.

En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'évènement.

Les évènements 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 ».

L'AC met ces enregistrements à disposition de l'auditeur qualifié comme preuves de sa conformité avec les exigences applicables.

5.4.1.1 Journaux d'activité des routeurs et pares-feux

La journalisation des activités des routeurs et pares-feux inclue au minimum :

- Les tentatives d'accès réussies et en échec sur les routeurs et pare-feux ;
- La journalisation des actions d'administration réalisées sur les routeurs et pares-feux, incluant les changements de configuration, les mises à jour firmware, et les modifications de contrôles d'accès ;
- La journalisation des changements réalisés sur les règles de filtrage, incluant les ajouts, modifications ou suppressions ;
- La journalisation de tous les évènements et erreurs système, incluant les dysfonctionnements matériels, les pannes de logiciels et les redémarrages système.

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

5.4.6 Système de collecte des journaux (Internes ou externes)

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

Une appréciation des risques est réalisée annuellement afin d'identifier :

- Les menaces internes et externes prévisibles qui pourraient entraîner un accès non autorisé, une divulgation, une utilisation abusive, une altération ou une destruction de toute donnée de certificat ou processus de gestion de certificat ;
- La probabilité et les dommages potentiels de ces menaces, en tenant compte de la sensibilité des données de certificat et des processus de gestion des certificats ; et
- La suffisance des politiques, procédures, systèmes d'information, technologies et autres dispositifs que l'AC a mis en place pour contrer ces menaces.

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 par jour ouvré 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 semaine 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 documentations relatives à la sécurité de leurs systèmes de management de certificats, les systèmes d'AC racines et les systèmes des tiers impliqués dans la délivrance de certificats ;
- Les documentations relatives à la vérification des demandes de certificats, la délivrance et la révocation des certificats ;
- 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/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

5.5.2.1 Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé à minima sept ans à compter de l'expiration du certificat, 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. 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 certificat émis par l'AC.

5.5.2.2 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 génération.

Les réponses OCSP produites sont archivées pendant au moins deux ans après leur expiration.

Les réponses sont détruites automatiquement après cette durée.

5.5.2.3 Journaux d'événements

Les journaux d'événements traités au chapitre 5.4 sont archivés pendant au moins sept ans après l'expiration des certificats associés.

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. Une procédure d'effacement des archives est exécutée sur les différents centres de production une fois la durée de rétention atteinte.

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 » (automatique ou manuel en cas de reprise) 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 (Internes ou externes)

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'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats. Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

L'IGC CERTIGNA communiquera en temps utiles sur son site en cas de génération d'un nouveau certificat 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/DPC. 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

5.7.1.1 Plans d'intervention en cas d'incident et de reprise après sinistre

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 à 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.

Le plan de continuité d'activité est revu, mis à jour et testé annuellement au travers d'un ou plusieurs scénarios de sinistre simulés. Le plan de continuité inclut :

- Les conditions d'activation du plan ;
- Les procédures d'urgence ;
- Les procédures de secours ;
- Les modalités de reprise ;
- Un calendrier de maintien du plan ;
- Les exigences en matière de sensibilisation et d'éducation ;
- Les responsabilités des intervenants ;
- Les objectifs de temps de récupération (RTO) ;
- Les tests réguliers des plans d'urgence ;
- Le plan de l'AC pour maintenir et restaurer les opérations métiers de l'AC en temps opportun après l'interruption ou la défaillance de processus métiers critiques ;
- L'obligation de stocker les matériels cryptographiques critiques à un autre emplacement ;
- Ce qui constitue une panne de système acceptable et un temps de récupération ;
- La fréquence à laquelle des copies de sauvegardes des informations métiers et des logiciels essentiels sont effectuées ;
- La distance entre les installations de récupération et le site principal de l'AC ;
- Les procédures de sécurisation de ses installations dans la mesure du possible pendant la période suivant une catastrophe et avant de restaurer un environnement sécurisé, soit sur le site d'origine, soit sur un site distant.

5.7.1.2 Plans de révocation massive

L'AC maintien un plan complet et réalisable pour les événements de révocation massive. L'AC effectue un test annuel du plan de révocation massive et intègre à ce plan les leçons apprises afin d'améliorer continuellement la préparation aux événements de révocation massive au fil du temps.

Le plan de révocation massive de l'AC inclut des procédures clairement définies, réalisables et complètes, conçues pour garantir une réponse rapide, cohérente et fiable aux scénarios de révocation de certificats à grande échelle. L'AC n'est pas tenue de divulguer publiquement son plan ou ses procédures de révocation massive, mais le met à la disposition de ses auditeurs sur demande.

L'AC teste, révise et met à jour chaque année son plan et ces procédures.

Le plan de révocation massive de l'AC peut être intégré dans le plan de réponse aux incidents, de continuité des activités, de reprise après sinistre ou dans d'autres plans ou procédures similaires de l'AC, à condition que les dispositions régissant les événements de révocation massive restent clairement identifiables et satisfassent à ces exigences.

Les dispositions relatives à la révocation massive comprennent :

1. Les critères d'activation : seuils spécifiques, objectifs et mesurables à partir desquels le plan de révocation massive est déclenché en fonction du profil de risque de l'AC, des volumes d'émission et des capacités opérationnelles ;
2. Les coordonnées des clients : comment les coordonnées des Responsables de Certificats et des clients sont stockées, conservées et mises à jour ;
3. Les points d'automatisation : les processus automatisés ou pouvant être automatisés, et processus nécessitant une intervention manuelle ;
4. Les objectifs et délais pour le tri des incidents, le lancement de la révocation, le remplacement des certificats et l'examen post-événement ;
5. Les méthodes de notification des Responsables de certificats : mécanismes de notification des Responsables de certificats concernés ;
6. Les attributions des rôles : rôles et responsabilités du personnel chargé de lancer, de coordonner et d'exécuter le plan ;
7. Les Formations et éducation : les activités de formation, de sensibilisation et de préparation du personnel responsable du plan ou qui le soutient ;
8. Les tests du plan : le test opérationnel annuel visant à évaluer la préparation et à démontrer la faisabilité de la mise en œuvre, à l'aide d'un ou plusieurs exercices sur table, simulations, tests parallèles ou environnements de test contrôlés qui n'impliquent pas la révocation de certificats actifs de Responsables de Certificats ; et
9. L'analyse post-test et calendrier de mise à jour : comment les enseignements tirés des tests ou des incidents réels sont intégrés dans le plan, et à quelle fréquence celui-ci est révisé et mis à jour.

5.7.2 Procédures de reprise en cas de corruption des ressources informatiques

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

Ce plan est testé au minimum une fois tous les trois ans.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité d'activité de la composante en tant que sinistre (cf. chapitre 5.7.2). Dans le cas de compromission d'une clé d'AC, le certificat correspondant sera immédiatement révoqué. 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 à 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 s'appuie sur la redondance de ses systèmes d'informations sur plusieurs sites et ses plans de continuité d'activité 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.

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

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

- Elle assure la continuité du service d'archivage, en particulier des certificats et des dossiers d'enregistrement ;
- Elle assure la continuité du service de révocation, conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC ;
- Elle prévient les RC dans le cas où les changements envisagés peuvent avoir des répercussions sur les engagements pris et ce, au moins sous le délai de 1 mois ;
- Elle communique aux responsables d'applications 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'informera 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.

5.8.2 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.

5.8.3 Accessibilité du statut de révocation au-delà de la fin de validité

L'AC s'engage à assurer la disponibilité du statut de révocation à tout moment et au-delà de la période de validité du certificat, en respectant les pratiques suivantes :

- Après l'expiration d'un certificat qualifié eIDAS :
    - La LCR publiée comportera l'extension « ExpiredCertsOnCRL », comme prévu par la recommandation ITU-T X.509 ; et contiendra les numéros de série de l'ensemble des certificats révoqués, y compris les certificats étant arrivés à expiration après leur révocation.
    - Si un répondeur OCSP est mis en œuvre sur cette AC, les réponses OCSP comporteront l'extension « archive cutoff », comme prévu par la RFC 6960, avec une date identique à la date de début de validité du certificat de l'AC, et le statut de révocation du certificat sera maintenu disponible après son expiration.

- Si la clé de l'AC émettrice d'un certificat qualifié eIDAS est sur le point d'expirer :
    - Les certificats non-expirés émis par cette AC seront révoqués si leur date de fin de validité est supérieure à celle de l'AC ;
    - Une dernière LCR sera publiée avec une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« 99991231235959Z ») ;
    - Si un répondeur OCSP est mis en œuvre sur cette AC, une dernière réponse OCSP sera pré-générée pour chaque certificat émis, avec une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« 99991231235959Z »).

  Ces dispositions seront mises en œuvre même si CERTIGNA cesse de fournir le service de confiance qualifié eIDAS, sans le transférer vers un autre prestataire de service de confiance qualifié eIDAS.

- Si CERTIGNA cesse de fournir le service de confiance qualifié eIDAS, sans le transférer vers un autre prestataire de service de confiance qualifié eIDAS, CERTIGNA n'est pas tenu de maintenir la publication des LCR ni de maintenir le service OCSP, mais les LCR et/ou réponses OCSP produites seront mises à disposition des clients de CERTIGNA dans des conditions permettant de garantir leur intégrité. Ces dispositions seraient rendues publiques si la situation venait à être rencontrée.

6 MESURES DE SECURITE TECHNIQUES

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Génération des bi-clés d'AC

Ce chapitre décrit le contexte de génération de la bi-clé de l'AC Racine et des AC intermédiaires.

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.

Pour une nouvelle bi-clé d'AC qui est utilisée pour un certificat d'AC racine ou d'AC intermédiaire, où l'AC subordonnée n'est pas opérateur de l'AC racine ou une affiliée de l'AC Racine, l'AC :

- Prépare un script de génération de clé ;
- Dispose d'un auditeur qualifié afin d'assister au processus de génération de la bi-clé d'AC ou enregistre une vidéo de l'ensemble du processus de génération de la bi-clé d'AC, et
- Obtient de l'auditeur qualifié un rapport indiquant que l'AC a suivi sa cérémonie de remise des clés lors de son processus de génération de clés et de certificats et les contrôles utilisés pour assurer l'intégrité et la confidentialité de la bi-clé.

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.

6.1.1.2 Génération des bi-clés d'AE

Sans objet.

Note : L'AE utilise tant que possible les certificats finaux délivrés par les AC couvertes par cette PC/DPC pour authentifier son personnel et sécuriser ses services.

6.1.1.3 Génération des bi-clés de personne morale

Le RC s'engage de manière contractuelle, en acceptant les CGVU 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'AC.

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

L'AC rejette une demande de certificat si :

- La clé publique demandée ne répond pas aux exigences stipulées aux chapitres 6.1.5 et 6.1.6 ;
- Des preuves évidentes que la méthode utilisée pour générer la clé privée était défectueuse
- L'AC a connaissance d'une méthode démontrée ou éprouvée qui expose la clé privée du demandeur à une compromission ;
- L'AC a été informée au préalable que la clé privée du demandeur a subi une compromission de clé en utilisant la procédure de demande de révocation de l'AC décrite à la section 4.9.3 et à la section 4.9.12 ;
- La clé publique correspond à une clé privée dont la faiblesse a été démontrée par l'industrie. Pour les demandes soumises à partir du 15 novembre 2024, les précautions suivantes sont au moins mises en œuvre :
    - Dans le cas de la vulnérabilité des clés faibles de Debian (https://wiki.debian.org/SSLkeys), l'AC rejette toutes les clés trouvées sur https://github.com/cabforum/Debian-weak-keys/ pour chaque type de clé (par exemple RSA, ECDSA) et chaque taille répertoriée dans le référentiel. Pour toutes les autres clés répondant aux exigences de la section 6.1.5, à l'exception des tailles de clés RSA supérieures à 8192 bits, l'AC rejette les clés faibles de Debian.
    - Dans le cas de la vulnérabilité ROCA, l'AC rejette les clés identifiées par les outils disponibles sur https://github.com/crocs-muni/roca ou équivalent.
    - Dans le cas de la vulnérabilité Close Primes (https://fermatattack.secvuln.info/), l'AC rejette les clés faibles qui peuvent être factorisées en 100 tours en utilisant la méthode de factorisation de Fermat.

Si le certificat contient une extension extKeyUsage contenant soit la valeur id-kp-serverAuth [RFC5280] ou anyExtendedKeyUsage [RFC5280], l'AC ne doit pas générer la bi-clé au nom du RC, et ne doit pas accepter une demande de certificat utilisant une bi-clé générée préalablement par l'AC.

Les parties autres que le RC n'archivent pas la clé privée sans son autorisation.

Si l'AC ou un AED est informé que la clé privée de la personne morale a été communiquée a une personne ou une organisation non autorisée et non affiliée à la personne morale, alors l'AC révoquera tous les certificats qui incluent la clé publique correspondante à la clé privée communiquée.

6.1.2 Transmission de la clé privée au demandeur

Le RC assure la génération de la clé privée du serveur.

Les parties autres que le RC ne doivent pas archiver la clé privée du serveur sans l'autorisation du RC.

Si l'AC ou l'AE est informée que la clé privée destinée au RC a été communiquée à une personne non autorisée ou à une organisation non affiliée avec le sujet du certificat, alors l'AC révoquera tous les certificats qui incluent la clé publique correspondant à la clé privée communiquée.

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 web, est transmise à l'AC par le RC. Cette demande est signée avec la clé privée, ce qui permet à l'AE d'en vérifier l'intégrité et de s'assurer que le RC possède la clé privée associée à la clé publique transmise dans cette demande. Une fois ces vérifications effectuées, l'AE signe la demande puis la transmet à l'AC.

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

La délivrance de la clé publique de l'AC, qui permet à tous ceux qui en ont besoin de valider un certificat émis par l'AC en vertu de cette PC, est effectuée par un moyen garantissant intégrité et authentification de cette clé publique. La clé publique d'une 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 https://www.certigna.com. Cf. chapitre 2.2.1.2.

6.1.5 Taille des clés

6.1.5.1 Certificat d'AC racine

- Algorithme de hachage : SHA-256,
- Taille modulus RSA (bits) : 4096

6.1.5.2 Certificat d'AC intermédiaire

- Algorithme de hachage : SHA-256, ou SHA-384 pour les nouvelles AC
- Taille modulus RSA (bits) : 4096

6.1.5.3 Certificat de personne morale

- Algorithme de hachage : Egale ou supérieur à SHA-256 (SHA-256, SHA-384 ou SHA512)
- Taille RSA modulus (bits) : 2048, 3072 or 4096 (Cf. chapitre 7)

6.1.6 Vérification de la génération des paramètres des clés publiques 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. L'AC confirme que la valeur de l'exposant public est un nombre impair supérieur à 3 et compris entre $2^{16}+1$ et $2^{256}-1$

6.1.6.1 Clé d'AC

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

6.1.6.2 Clé de personne morale

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

6.1.7 Objectifs d'usage de la clé (pour champ d'utilisation de la clé X.509 v3)

6.1.7.1 Clé d'AC

La clé privée de l'AC racine est utilisée pour signer le certificat de l'AC racine, les LAR et les certificats d'AC intermédiaires. La clé privée d'une AC intermédiaire est utilisée pour signer les certificats de personne morale ou physique, les LCR, ainsi que le certificat du répondeur OCSP.

6.1.7.2 Clé de personne physique ou morale

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

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'AC

Les modules cryptographiques utilisés par l'AC Racine et les AC intermédiaires pour la génération et la mise en œuvre de leurs clés de signature sont conformes aux exigences du chapitre 10. Ces boitiers sont des ressources exclusivement accessibles aux serveurs d'AC via un VLAN dédié. Les modules cryptographiques utilisés sont des BULL Trustway Proteccio. La « Procédure de gestion des HSM » décrit plus en détails les dispositions mises en œuvre. L'AC met en œuvre des protections physiques et logiques pour empêcher de la délivrance non autorisée de certificats.

6.2.1.2 Dispositifs de protection des clés privées de personne morale ou physique

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

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

6.2.3.1 Clés d'AC

Les clés privées d'AC ne sont jamais séquestrées.

6.2.3.2 Clés de personne morale ou physique

Le séquestre des clés privées est interdit.

6.2.4 Copie de secours de la clé privée

6.2.4.1 Clé privée d'AC

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

- Dans un ou plusieurs modules cryptographiques conformes 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 de secrets.

6.2.4.2 Clé privée de personne morale

Les clés privées des serveur web ne font pas l'objet de copies de secours pour l'ensemble des autorités de certification hormis pour les certificats de chiffrement de l'AC Certigna Identity CA.

6.2.5 Archivage de la clé privée

6.2.5.1 Clé privée d'AC

La clé privée d'une AC n'est en aucun cas archivée.

6.2.5.2 Clé privée de personne morale

La clé privée du serveur web n'est en aucun cas archivée.

6.2.6 Transfert de la clé privée avec le module cryptographique

6.2.6.1 Clé privée d'AC

La clé privée d'une AC est générée dans le module cryptographique conforme aux exigences du chapitre 10. Comme décrit en 6.2.4, la clé n'est exportable/importable du module que sous forme chiffrée. Si l'AC est informée que la clé privée d'une AC subordonnée a été communiquée à une personne ou une organisation non autorisée et non affiliée à l'AC, alors l'AC révoque tous les certificats qui intègre la clé publique correspondante à la clé privée communiquée.

6.2.6.2 Clé privée de personne morale

La clé privée du serveur web est générée sous la responsabilité du RC.

6.2.7 Stockage de la clé privée dans un module cryptographique

6.2.7.1 Clé privée d'AC

La clé privée de l'AC racine est générée dans un module cryptographique décrit au chapitre 6.2.1 et est exportée conformément aux exigences du chapitre 6.2.4 afin de continuellement la maintenir hors ligne. La clé est reconstituée dans le module cryptographique pour permettre la génération annuelle des LAR ou la création d'une nouvelle autorité intermédiaire, puis supprimée du module une fois l'opération terminée. La « Procédure de gestion des HSM » et la « Procédure de gestion des clés cryptographiques » décrivent plus en détails les dispositions mises en œuvre.

6.2.7.2 Clé privée de personne morale

La clé privée du serveur web est générée et stockée dans un dispositif conforme aux exigences du chapitre 11, le cas échéant.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clé privée d'AC

L'activation de la clé privée d'une AC dans le module cryptographique 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. La « Procédure de gestion des HSM » et la « Procédure de gestion des clés cryptographiques » décrivent plus en détails les dispositions mises en œuvre.

6.2.8.2 Clé privée de personne morale

L'activation des clés privées est contrôlée via des données d'activation (Cf. chapitre 6.4) qui sont utilisées par le dispositif utilisé le cas échéant.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clé privée 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.

6.2.9.2 Clé privée de personne morale

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

6.2.10 Méthode de destruction de la clé privée

6.2.10.1 Clé privée 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 l'opération. Les mesures mises en œuvre sont décrites dans la « Procédure de gestion des clés cryptographiques ».

6.2.10.2 Clé privée de personne morale

Le RC étant l'unique détenteur de la 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

6.2.11.1 Clé d'AC

Le niveau d'évaluation du module cryptographique de l'AC est précisé au chapitre 10.

6.2.11.2 Clé de personne morale

Le niveau d'évaluation du dispositif utilisé par le 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 personnes morales et physiques sont archivées dans le cadre de l'archivage des certificats correspondants.

6.3.2 Durées de vie des bi-clés et des certificats

6.3.2.1 Bi-clé et certificat d'AC

AC racine	Durée de validité du certificat
Certigna	20 ans maximum
Subordinate CAs	10 ans maximum
Certigna Root CA	20 ans maximum
Subordinate CAs	18 ans maximum
Certigna Server Authentication Root CA	15 ans maximum
Subordinate CAs	15 ans maximum
Certigna Server Authentication EU Root CA	15 ans maximum
Subordinate CAs	15 ans maximum

6.3.2.2 Bi-clé et certificat de personne morale

Les certificats des serveurs délivrés ont une durée de vie fixée en fonction de leur date d'émission et définie dans le tableau ci-dessous.

Certificat émis		**Durée de validité du certificat**
Après le	**et avant le**	
1er Septembre 2020	15 mars 2026	398 jours maximum
15 mars 2026	15 mars 2027	200 jours maximum
15 mars 2027	15 mars 2029	100 jours maximum
15 mars 2029		47 jours maximum

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

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

La génération et l'installation des données d'activation 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.

6.4.1.2 Génération et installation des données d'activation correspondant à la clé privée de la personne morale

La bi-clé est générée et installée par le RC.

6.4.2 Protection des données d'activation

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

Les données d'activation sont directement remises aux porteurs de secrets 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.

6.4.2.2 Protection des données d'activation correspondant à la clé privée de la personne morale

La bi-clé est générée et installée par le RC.

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 multi-facteurs et forte des utilisateurs pour l'accès au système (Ex : 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 via le firewall ;
- Communication sécurisée inter-sites (tunnel VPN IP Sec) ;
- Fonctions d'audit (non-répudiation et nature des actions effectuées).

Des dispositifs de surveillance 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.

Les configurations des systèmes sont analysées quotidiennement par des outils de l'entité qui réinitialisent toute configuration pour laquelle une anomalie est identifiée. Les modèles de configurations déployés sur les systèmes par ces outils sont revus au maximum tous les ans.

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

Afin de permettre à ses prospects ou futurs clients de tester ou 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 ».

Lorsque l'AC utilise un logiciel de vérification développé par des tiers (Ex : pkimetal Linter), elle supervise les versions à jour de ce logiciel et prévoit les mises à jour au plus tard trois (3) mois après la publication de la mise à jour. L'AC peut procéder à la vérification de l'ensemble des certificats de serveurs non expirés et non révoqués chaque fois qu'elle met à jour le logiciel de vérification.

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

La présente PC/DPC vise également la conformité aux « Network and Certificate System Security Requirements » en vigueur du CA/Browser Forum. 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. 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 PROFIL DES CERTIFICATS ET DES LCR

7.1 Profils des certificats

L'AC respecte les exigences techniques énoncées dans les chapitres :

- 6.1.5 Algorithmes et tailles de clé ;
- 6.1.6 Vérification de la qualité et de la génération des paramètres de clés publiques.

L'AC génère des numéros de série non-séquentiels, supérieurs à zéro (0) de 64 bits et provenant d'une méthode CSPRNG. Les certificats et les LCR produits par l'AC sont conformes au standard ITU-T Recommandation X.509 version 3, à la RFC 5280 et aux spécifications ETSI EN 319 412 applicables.

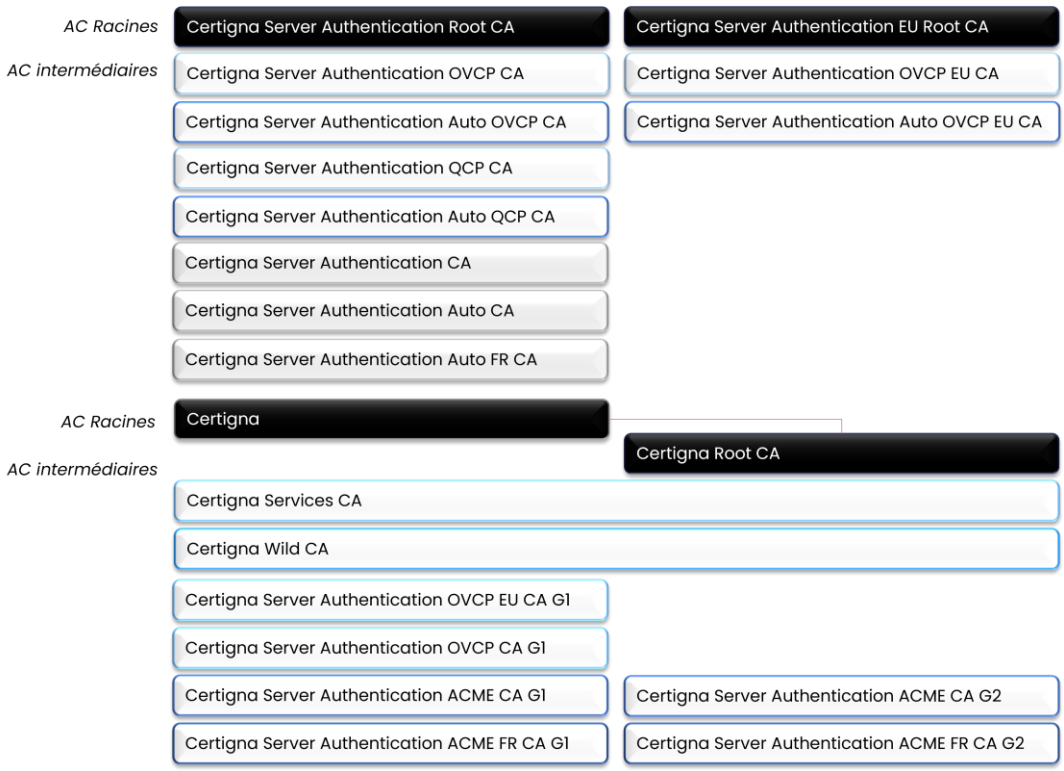
CERTIGNA dispose des AC racines suivantes :

- L'historique « Certigna » ;
- L'actuelle « Certigna Root CA » (également signée par Certigna : Cross Signing) ;
- La nouvelle dédiée au TLS « Certigna Server Authentication Root CA » ;
- La nouvelle dédiée au TLS européen « Certigna Server Authentication EU Root CA ».

A compter du 1er juillet 2023, l'AC ne signe plus de hash SHA-1 sur :

- les certificats avec une extension d'usage (EKU) de type « id-kp-ocspSigning » ;
- les certificats d'AC intermédiaires ;
- les réponses OCSP, ou ;
- les CRL.

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



7.1.1 Numéro de version

Les certificats sont de type X.509 v3.

7.1.2 Extensions des certificats

Se référer aux exigences du chapitre 7.10.

7.1.2.1 Traitement des extensions de certificats par les applications

Les extensions définies pour les certificats X509 V3 permettent d'associer des informations complémentaires à une clé publique, relatives au serveur ou à l'AC.

7.1.2.2 Criticité

Le caractère de criticité doit se traiter de la façon suivante selon que l'extension est critique ou non :

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

7.1.2.3 Description des extensions

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

Subject Key Identifier : Cette extension identifie la clé publique du serveur associée au certificat. Elle permet de distinguer les différentes clés utilisées par le Porteur. Sa valeur est la valeur contenue dans le champ keyIdentifier.

Key Usage : Cette extension définit l'utilisation prévue de la clé contenue dans le certificat. L'AC Indique l'usage prévu de la clé et gère la criticité.

Extended Key Usage : Cette extension définit l'utilisation avancée de la clé.

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

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

Authority Information Access : Cette extension identifie (avec Method=OCSP) l'emplacement du(des) serveur(s) OCSP fournissant des informations sur le statut des certificats, ainsi que sur l'AC émettrice en fournissant un lien vers son certificat.

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

Certificate Transparency : Cette extension permet de contrôler l'enregistrement du certificat dans les journaux utilisés pour le dispositif « Certificate Transparency ».

7.1.3 Algorithm object identifiers

7.1.3.1 SubjectPublicKeyInfo

7.1.3.1.1 RSA

L'AC indique une clé RSA en utilisant l'identifiant de l'algorithme rsaEncryption (OID : 1.2.840.113549.1.1.1). Le paramètre est présent et est un NULL explicite. L'AC n'utilise pas un algorithme différent, tel que l'identificateur d'algorithme id-RSASSA-PSS (OID : 1.2.840.113549.1.1.10), pour indiquer une clé RSA. Lorsqu'il est codé, l'AlgorithmIdentifier pour les clés RSA est identique, octet par octet, aux octets suivants codés en hexadécimal : 300d06092a864886f70d0101010500.

7.1.3.2 Signature AlgorithmIdentifier

7.1.3.2.1 RSA

Pour les certificats TLS, S/MIME and Code Signing, l'AC utilise l'un des algorithmes de signature et l'un des codages suivants :

- RSASSA-PKCS1-v1_5 with SHA-256: Encoding: 300d06092a864886f70d01010b0500.
- RSASSA-PKCS1-v1_5 with SHA-384: Encoding: 300d06092a864886f70d01010c0500.

Avant le 15/09/2026, l'AC révoquera tous les certificats d'AC intermédiaire qui contiennent le codage RSASSA-PKCS1-v1_5 avec SHA-1 dans le certificat.

7.1.4 Format de nom

Les valeurs des attributs sont codées conformément à la norme RFC 5280.

7.1.4.1 Encodage du nom

Pour chaque chemin de certification valide (tel que défini par la RFC 5280, section 6) :

- Pour chaque certificat du chemin de certification, le contenu codé du champ Issuer Distinguished Name d'un certificat est identique, octet par octet, à la forme codée du champ Subject Distinguished Name du certificat de l'autorité de certification émettrice.
- Pour chaque certificat d'AC dans le chemin de certification, le contenu codé du champ Subject Distinguished Name d'un certificat est identique octet par octet à tous les certificats dont les Subject Distinguished Names peuvent être comparés comme étant égaux conformément à la section 7.1 de la RFC 5280, y compris les certificats expirés et révoqués.

7.1.4.2 Information du sujet – Demandeur de certificat

Voir les exigences applicables à tous les profils au chapitre 7.10.

7.1.5 Contrainte de nom

Pas de stipulation. Voir les exigences pour tous les profils à la section 7.10.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Identificateur de politique de certification réservés

Les identificateurs de politique de certification suivants sont réservés pour affirmer qu'un certificat est conforme aux exigences du CA\Browsers Forum.

7.1.6.1.1 Certificats TLS

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3)

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines(1)} (2.23.140.1.1)

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines (1) } (2.23.140.1.1)

7.1.7 Utilisation de la politique de contraintes

Sans objet.

7.1.8 Syntaxe et sémantique des qualifiants de politiques

Sans objet.

7.1.9 Sémantique de traitement pour l'extension des politiques de certificats critiques

Sans objet.

7.1.10 Profils des certificats des AC Racines

7.1.10.1 Champs de base

Autorité Champs	Certigna Server Authentication Root CA	Certigna Server Authentication EU Root CA	Certigna Root CA	Certigna
Version	V3			
Serial Number	0D AA 23 68 DC F4 02 35 D1 11 7F 1E B7 FC 1E 03 2B 5B 4F 46	11A064F5746CC6CCB5FD081CC F0A857051F569A5	00 CA E9 1B 89 F1 55 03 0D A3 E6 41 6D C4 E3 A6 E1	00 FE DC E3 01 0F C9 48 FF
Signature	SHA-384 RSA 4096	SHA-384 RSA 4096	SHA-256 RSA 4096	SHA-128 RSA 2048
Subject Public Key Info	RSA 4096 bits	RSA 4096 bits	RSA 4096 bits	RSA 2048 bits
Validity	Dates et heures d'activation et d'expiration du Certificat			
Issuer DN	CN = Certigna Server Authentication Root CA O = Certigna C = FR	CN = Certigna Server Authentication EU Root CA O = Certigna C = FR	CN = Certigna Root CA OU = 0002 48146308100036 O = Dhimyotis C = FR	CN = Certigna O = Dhimyotis C = FR
Subject DN	CN = Certigna Server Authentication Root CA O = Certigna C = FR	CN = Certigna Server Authentication EU Root CA O = Certigna C = FR	CN = Certigna Root CA OU = 0002 48146308100036 O = Dhimyotis C = FR	CN = Certigna O = Dhimyotis C = FR

7.1.10.2 Extensions

Extensions	Crit	Certigna Server Authentication Root CA	Certigna Server Authentication EU Root CA	Certigna Root CA	Certigna
SKI	No	Identifiant de la clé publique de l'AC			
AKI	No	Identifiant de la clé publique de l'AC racine			
Certificate Policies	No			OID=anyPolicy CPS=https://www.certigna.fr/autorites/	
CRL Distribution Points	No			URL=http://crl.certigna.fr/certignarootca.crl URL=http://crl.dhimyotis.com/certignarootca.crl	
Netscape Cert type	No				SSL CA SMIME CA Signature CA
Basic Constraints	Yes	cA = TRUE			
Key Usage	Yes	Certificate signing CRL signing			

7.1.11 Profils des certificats des AC intermédiaires

Autorité		SERVER AUTHENTICATION ROOT CA						
		SERVER AUTHENTICATION CA	SERVER AUTHENTICATION AUTO CA	SERVER AUTHENTICATION AUTO FR CA	SERVER AUTHENTICATION OVCP CA	SERVER AUTHENTICATION AUTO OVCP CA	SERVER AUTHENTICATION QCP CA	SERVER AUTHENTICATION AUTO QCP CA
Champs		**Description**						
Version		V3						
Serial Number		Numéro de série unique						
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-384 RSA 4096						
Subject Public Key Info		RSA 4096						
Validité		15 ans						
Issuer DN	CN =	Certigna Server Authentication Root CA						
	O =	Certigna						
	C =	FR						
Subject DN	CN =	Certigna Server Authentication CA	Certigna Server Authentication Auto CA	Certigna Server Authentication Auto FR CA	Certigna Server Authentication OVCP CA	Certigna Server Authentication Auto OVCP CA	Certigna Server Authentication QCP CA	Certigna Server Authentication Auto QCP CA
	OI =	NTRFR-48146308100036						
	O =	Certigna						
	C =	FR						
SKI	No	CA public key identifier						
AKI	No	Root CA Public key identifier						
Certificate Policies	No	OID=2.23.140.1.2.1 (DV) OID=2.23.140.1.2.2 (OV) OID= 2.23.140.1.1 (EV) OID=1.2.250.1.177.6.0.1.1 CPS = http://cps.certigna.com/			OID=2.23.140.1.2.2 (OV) OID=1.2.250.1.177.6.0.1.1 CPS = http://cps.certigna.com/			
Authority Informat. Access	No	URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/CertignaServerAuthenticationRootCA.cer			caIssuers= http://cert.certigna.com/CertignaServerAuthenticationRootCA.cer			
CRL Distributi. Points	No	URL=http://crl.certigna.com/CertignaServerAuthenticationRootCA.crl						
Basic Constraints	Yes	cA = TRUE PathLengthConstraint = 0						
Key Usage	Yes	Certificate signature CRL signature						
Extended Key Usage	Non	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)						

Autorité		SERVER AUTHENTICATION EU ROOT CA	
		SERVER AUTHENTICATION OVCP EU CA	SERVER AUTHENTICATION AUTO OVCP EU CA
Champs		**Description**	
Version		V3	
Serial Number		Numéro de série unique	
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-384 RSA 4096	
Subject Public Key Info		RSA 4096	
Validity		15 ans	
Issuer DN	CN =	Certigna Server Authentication EU Root CA	
	O =	Certigna	
	C =	FR	
Subject DN	CN =	Certigna Server Authentication OVCP EU CA	Certigna Server Authentication Auto OVCP EU CA
	OI =	NTRFR-48146308100036	
	O =	Certigna	
	C =	FR	
SKI	No	Identifiant de la clé publique de l'AC	
AKI	No	Identifiant de la clé publique de l'AC racine	
Certificate Policies	No	OID=2.23.140.1.2.2 (OV) OID=1.2.250.1.177.14.0.1.1 CPS = http://cps.certigna.com/	
Authority Informat. Access	No	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationEURootCA.cer	
CRL Distribution Points	No	URL=http://crl.certigna.com/CertignaServerAuthenticationEURootCA.crl	
Basic Constraints	Yes	cA = TRUE	PathLengthConstraint = 0
Key Usage	Yes	Certificate signature	CRL signature
Extended Key Usage	No	Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)

Autorité		CERTIGNA				
		SERVER AUTHENTICATION OVCP EU CA G1	SERVER AUTHENTICATION OVCP CA G1	SERVICES CA	WILD CA	CERTIGNA ROOT CA
Champs		**Description**				
Version		V3				
Serial Number		Numéro de série unique				
Signature		Identifiant de l'algorithme de signature de l'AC SHA-384 RSA 4096		Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096		
Subject Public Key Info		RSA 4096				
Validity		< 3 ans (2027-06-28)		18 ans		< 3 ans (2027-06-28)
Issuer DN	CN = O = C =	Certigna Dhimyotis FR				
Subject DN	CN =	Certigna Server Authentication OVCP EU CA G1	Certigna Server Authentication OVCP CA G1	Certigna Services CA	Certigna Wild CA	Certigna Root CA
	OU =					0002 48146308100036
	OI =	NTRFR-48146308100036				
	O =	Certigna		Dhimyotis		
	C =	FR				
SKI	Non	Identifiant de la clé publique de l'AC				
AKI	Non	Identifiant de la clé publique de l'AC racine				
Certificate Policies	Non	OID=2.23.140.1.2.2 (OV) OID=1.2.250.1.177.1.0.1.2 CPS = http://cps.certigna.com/				OID=2.23.140.1.2.2 (OV)
Authority Info Access	Non	caIssuers= http://cert.certigna.com/Certigna.cer				
CRL Distribution Points	Non	URL=http://crl.certigna.com/Certigna.crl				
Basic Constraints	Oui	cA = TRUE	PathLengthConstraint = 0			cA = TRUE
Key Usage	Oui	Certificate signature	CRL signature			
Extended Key Usage	Non	Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)			Server Authentication

		CERTIGNA ROOT CA	
Autorité		SERVICES CA	WILD CA
Champs		**Description**	
Version		V3	
Serial Number		Numéro de série unique	
Signature		SHA-256 RSA 4096	
Subject Public Key Info		RSA 4096	
Validity		18 ans	
Issuer DN	CN = OU = O = C =	Certigna Root CA 0002 48146308100036 DHIMYOTIS FR	
Subject DN	CN =	Certigna Services CA	Certigna Wild CA
	OI =	NTRFR-48146308100036	
	O =	Dhimyotis	
	C =	FR	
SKI	Non	Identifiant de la clé publique de l'AC	
AKI	Non	Identifiant de la clé publique de l'AC racine	
Certificate Policies	Non	OID=1.2.250.1.177.2.0.1.1 CPS=https://www.certigna.fr/autorites/	
Authority Informat. Access	Non	caIssuers= http://autorite.certigna.fr/certignarootca.der caIssuers= http://autorite.dhimyotis.com/certignarootca.der	
CRL Distribution Points	Non	URL=http://crl.certigna.fr/certignarootca.crl URL=http://crl.dhimyotis.com/certignarootca.crl	
Basic Constraints	Oui	cA = TRUE	PathLengthConstraint = 0
Key Usage	Oui	Certificate signature	CRL signature
Extended Key Usage	Non	Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)

Autorités		CERTIGNA		CERTIGNA ROOT CA	
		SERVEUR AUTHENTICATION ACME CA G1	SERVEUR AUTHENTICATION ACME FR CA G1	SERVEUR AUTHENTICATION ACME CA G2	SERVEUR AUTHENTICATION ACME FR CA G2
Champs		**Description**			
Version		V3			
Serial Number		Numéro de série unique			
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-384 RSA 4096			
Subject Public Key Info		RSA 4096			
Validity		15 ans			
Issuer DN	CN = OU = O = C =	Certigna Dhimyotis FR		Certigna Root CA 0002 48146308100036 Dhimyotis FR	
Subject DN	CN =	Certigna Server Authentication ACME CA G1	Certigna Server Authentication ACME FR CA G1	Certigna Server Authentication ACME CA	Certigna Server Authentication ACME FR CA
	OI =	NTRFR-48146308100036			
	O =	CERTIGNA			
	C =	FR			
SKI	Non	Identifiant de la clé publique de l'AC			
AKI	Non	Identifiant de la clé publique de l'AC racine			
Certificate Policies	Non	OID= 2.23.140.1.2.1 (DV) OID= 2.23.140.1.2.2 (OV) OID= 2.23.140.1.1 (EV) OID= 1.2.250.1.177.1.0.1.2 id-qt-cps = http://cps.certigna.com		OID= 2.23.140.1.2.1 (DV) OID= 2.23.140.1.2.2 (OV) OID= 2.23.140.1.1 (EV) OID= 1.2.250.1.177.2.0.1.1 id-qt-cps = http://cps.certigna.com	
Authority Informat. Access	Non	URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/Certigna.cer		URL=http://ocsp.certigna.com caIssuers= http://autorite.dhimyotis.com/certignarootca.der	
CRL Distribution Points	Non	URL=http://crl.certigna.com/Certigna.crl		URL=http://crl.certigna.com/CertignaRootCA.crl	
Basic Constraints	Oui	cA = TRUE	PathLengthConstraint = 0		
Key Usage	Oui	Certificate signature	CRL signature		
Extended Key Usage	Non	Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)		

7.1.12 Profils des certificats des serveurs

7.1.12.1 Profils des certificats délivrés par Certigna Server Authentication OVCP CA & AUTO OVCP CA

7.1.12.1.1 Champs de base

	Autorité	CERTIGNA SERVER AUTHENTICATION ROOT CA	
		CERTIGNA SERVER AUTHENTICATION OVCP CA	CERTIGNA SERVER AUTHENTICATION AUTO OVCP CA
Usage		Server authentication	
OID 1.2.250.1.177.6		.4.1.1.1	.5.1.1.1
ETSI 319 411		OVCP	OVCP
Champs		**Description**	
Version		V3	
Serial Number		Numéro de série unique délivré par un CSPRNG. Entre 128 et 160 bits	
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-256 minimum	
Subject Public Key Info		RSA 2048 minimum avant le 31/12/2025 / RSA 3072 minimum à compter du 31/12/2025	
Validity		398 jours maximum	
Issuer DN	CN = OI = O = C =	Certigna Server Authentication OVCP CA NTRFR-48146308100036 Certigna FR	Certigna Server Authentication Auto OVCP CA NTRFR-48146308100036 Certigna FR
Subject DN	Serial Number	Série de caractères constituée d'un aléa	
	Common Name	Un des FQDN de l'extension « Subject Alternative Name »	
	Organization Identifier		
	Organizat. Unit Name		
	Organization Name	Nom de l'entité à laquelle le serveur est rattaché	
	Street Address		
	Locality Name	Ville ou village de domiciliation de l'entité (2.5.4.7)	
	Postal Code		
	State or Province Name		
	Country Name	Pays de domiciliation de l'entité	
	Business Category		
	Jurisd. Locality Name		
	Jurisd. State/Prov. Name		
	Jurisd. Country Name		

7.1.12.1.2 Extensions

Autorité		CERTIGNA SERVER AUTHENTICATION ROOT CA	
		CERTIGNA SERVER AUTHENTICATION OVCP CA	CERTIGNA SERVER AUTHENTICATION AUTO OVCP CA
Usage		Server authentication	
OID 1.2.250.1.177.6		.4.1.1.1	.5.1.1.1
ETSI 319 411		OVCP	OVCP
RGS v2			
Extension	**Crit.**	**Description**	
Authority Key Ident.	Non	Identifiant de la clé publique de l'AC	
Subject Key Ident.	Non	Identifiant de la clé publique du serveur	
Subject Alt. Name	Non	FQDN des différents domaines à protéger. Le caractère « _ » ne doit pas être présent aux entrées dNSName.	
Key Usage	**Oui**	Digital signature / Key Encipherment	
Extended Key Usage	Non	id-kp-serverAuth / id-kp-clientAuth	
Certificate Policies	Non	.4.1.1.1	.5.1.1.1
		2.23.140.1.2.2 (OVCP)	
		0.4.0.2042.1.7 (OVCP)	
		CPS= http://cps.certigna.com	
CRL Distribut. Points	Non	URL=http://crl.certigna.com/CertignaServerAuthenticationOVCPCA.crl	http://crl.certigna.com/CertignaServerAuthenticationAutoOVCPCA.crl
Authority Info. Access	Non	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationOVCPCA.cer	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationAutoOVCPCA.cer
Basic Constraints	**Oui**	cA = FALSE	
Cabf Organization. Identifier 2.23.140.3.1	Non		
Certif. Transparency	Non	Liste de SCTs. *Uniquement pour les certificats contenant un ou plusieurs FDQN.*	
QC Statement	Non		

7.1.12.2 Profils des certificats délivrés par Certigna Server Authentication QCP CA & AUTO QCP CA

7.1.12.2.1 Champs de base

Autorité		CERTIGNA SERVER AUTHENTICATION ROOT CA	
		CERTIGNA SERVER AUTHENTICATION QCP CA	CERTIGNA SERVER AUTHENTICATION AUTO QCP CA
Usage		Server authentication	
OID 1.2.250.1.177.6		.6.1.1.1	.7.1.1.1
ETSI 319 411		QNCP-w	QNCP-w
RGS v2			
Champs		**Description**	
Version		V3	
Serial Number		Numéro de série unique délivré par un CSPRNG. Entre 128 et 160 bits	
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-256 minimum	
Subject Public Key Info		RSA 2048 minimum avant le 31/12/2025 / RSA 3072 minimum à compter du 31/12/2025	
Validity		398 jours maximum	
Issuer DN	CN = OI = O = C =	Certigna Server Authentication QCP CA NTRFR-48146308100036 Certigna FR	Certigna Server Authentication Auto QCP CA NTRFR-48146308100036 Certigna FR
Subject DN	Serial Number	Série de caractères constituée d'un aléa	
	Common Name	Un des FQDN de l'extension « Subject Alternative Name »	
	Organization Identifier	Numéro d'enregistrement de l'entité rattachée au certificat	
	Organizat. Unit Name		
	Organization Name	Nom de l'entité à laquelle le serveur est rattaché	
	Street Address		
	Locality Name	Ville ou village de domiciliation de l'entité (2.5.4.7)	
	Postal Code		
	State or Province Name		
	Country Name	Pays de domiciliation de l'entité	
	Business Category		
	Jurisd. Locality Name		
	Jurisd. State/Prov. Name		
	Jurisd. Country Name		

7.1.12.2.2 Extensions

Autorité		CERTIGNA SERVER AUTHENTICATION ROOT CA	
		CERTIGNA SERVER AUTHENTICATION QCP CA	CERTIGNA SERVER AUTHENTICATION AUTO QCP CA
Usage		Server authentication	
OID 1.2.250.1.177.6		.6.1.1.1	.7.1.1.1
ETSI 319 411		QNCP-w	QNCP-w
RGS v2			
Extension	**Crit.**	**Description**	
Authority Key Ident.	Non	Identifiant de la clé publique de l'AC	
Subject Key Ident.	Non	Identifiant de la clé publique du serveur	
Subject Alt. Name	Non	FQDN des différents domaines à protéger. Le caractère « _ » ne doit pas être présent aux entrées dNSName.	
Key Usage	**Oui**	Digital signature / Key Encipherment	
Extended Key Usage	Non	id-kp-serverAuth / id-kp-clientAuth	
Certificate Policies	Non	.6.1.1.1	.7.1.1.1
		2.23.140.1.2.2 (OVCP)	
		0.4.0.194112.1.5 (QNCP-w)	
		CPS= http://cps.certigna.com	
CRL Distribut. Points	Non	URL=http://crl.certigna.com/CertignaServerAuthentication QCPCA.crl	http://crl.certigna.com/CertignaServerAuthenticationAuto QCPCA.crl
Authority Info. Access	Non	caIssuers= http://cert.certigna.com/CertignaServerAuthentication QCPCA.cer	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationAuto QCPCA.cer
Basic Constraints	**Oui**	cA = FALSE	
Cabf Organization. Identifier 2.23.140.3.1	Non		
Certif. Transparency	Non	Liste de SCTs. *Uniquement pour les certificats contenant un ou plusieurs FDQN.*	
QC Statement	Non	QcCompliance	
		QcEuPDS	
		QcType 3 (web)	

7.1.12.3 Profils des certificats délivrés par Certigna Server Authentication CA

7.1.12.3.1 Champs de base

CERTIGNA SERVER AUTHENTICATION CA							
Usage		Server authentication					
OID 1.2.250.1.177.6		.1.1.1.1	.1.1.1.2	.1.1.1.3	.1.1.2.1	.1.1.2.2	.1.1.2.3
ETSI 319 411		OVCP	OVCP	OVCP	QNCP-w	QNCP-w	QNCP-w
RGS v2		RGS *	RGS *	RGS *			
Champs		Description					
Version		V3					
Serial Number		Numéro de série unique délivré par un CSPRNG. Entre 128 et 160 bits					
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-256 minimum					
Subject Public Key Info		RSA 2048	RSA 3072	RSA 4096	RSA 2048	RSA 3072	RSA 4096
Validity		398 jours maximum					
Issuer DN	CN =	Certigna Server Authentication CA					
	OI =	NTRFR-48146308100036					
	O =	Certigna					
	C =	FR					
Subject DN	Serial Number	Série de caractères constituée d'un aléa					
	Common Name	Un des FQDN de l'extension « Subject Alternative Name »					
	Organization Identifier				Numéro d'enregistrement de l'entité rattachée au certificat		
	Organizat. Unit Name						
	Organization Name	Nom de l'entité à laquelle le serveur est rattaché					
	Street Address						
	Locality Name	Ville ou village de domiciliation de l'entité (2.5.4.7)					
	Postal Code						
	State or Province Name						
	Country Name	Pays de domiciliation de l'entité					
	Business Category						
	Jurisd. Locality Name						
	Jurisd. State/Prov. Name						
	Jurisd. Country Name						

7.1.12.3.2 Extensions

CERTIGNA SERVER AUTHENTICATION CA							
Usage		Server authentication					
OID 1.2.250.1.177.6		.1.1.1.1	.1.1.1.2	.1.1.1.3	.1.1.2.1	.1.1.2.2	.1.1.2.3
ETSI 319 411		OVCP	OVCP	OVCP	QNCP-w	QNCP-w	QNCP-w
RGS v2		RGS *	RGS *	RGS *			
Extension	**Crit.**	**Description**					
Authority Key Ident.	Non	Identifiant de la clé publique de l'AC					
Subject Key Ident.	Non	Identifiant de la clé publique du serveur					
Subject Alt. Name	Non	FQDN des différents domaines à protéger. Le caractère « _ » ne doit pas être présent aux entrées dNSName.					
Key Usage	**Oui**	Digital sign. / Key Enciph.					
Extended Key Usage	Non	id-kp-serverAuth / id-kp-clientAuth			id-kp-serverAuth / id-kp-clientAuth		
Certificate Policies	Non	.1.1.1.1	.1.1.1.2	.1.1.1.3	.1.1.2.1	.1.1.2.2	.1.1.2.3
		2.23.140.1.2.2 (OVCP)					
		0.4.0.2042.1.7 (OVCP)			0.4.0.194112.1.5 (QNCP-w)		
		CPS= http://cps.certigna.com					
CRL Distribut. Points	Non	URL=http://crl.certigna.com/CertignaServerAuthenticationCA.crl					
Authority Info. Access	Non	URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/CertignaServerAuthenticationCA.cer					
Basic Constraints	**Oui**	cA = FALSE					
Cabf Organization. Identifier 2.23.140.3.1	Non				Info. Entité [2]		
Certif. Transparency	Non	Liste de SCTs. *Uniquement pour les certificats contenant un ou plusieurs FDQN.*					
QC Statement	Non				QcCompliance		
					QcEuPDS		
					QcType 3 (web)		

7.1.12.4 Profil des certificats délivrés par Certigna Server Authentication Auto CA & Auto FR CA

7.1.12.4.1 Champs de base

CERTIGNA SERVER AUTHENTICATION		AUTO CA				AUTO FR CA	
Usage		Server authentication					
OID 1.2.250.1.177.6		.2.1.2.1	.2.1.2.2	.2.1.3.1	.2.1.3.2	.3.1.1.1	.3.1.1.2
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	OVCP	OVCP
RGS v2						RGS *	RGS *
Champs		Description					
Version		V3					
Serial Number		Numéro de série unique délivré par un CSPRNG. Entre 128 et 160 bits					
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-256 minimum					
Subject Public Key Info		RSA 3072	RSA 4096	RSA 3072	RSA 4096	RSA 3072	RSA 4096
Validity		Maximum 398 jours					
Issuer DN	CN =	Certigna Server Authentication Auto CA				Certigna Server Authentication Auto FR CA	
	OI =	NTRFR-48146308100036				NTRFR-48146308100036	
	O =	Certigna				Certigna	
	C =	FR				FR	
Subject DN	Serial Number	Série de caractères constituée d'un aléa					
	Common Name	Un des FQDN de l'extension « Subject Alternative Name »					
	Organization Identifier						
	Organizat. Unit Name						
	Organization Name	Nom de l'entité à laquelle le serveur est rattaché					
	Street Address						
	Locality Name	Ville ou village de domiciliation de l'entité (2.5.4.7)					
	Postal Code						
	State or Province Name						
	Country Name	Pays de domiciliation de l'entité					
	Business Category						
	Jurisd. Locality Name						
	Jurisd. State/Prov. Name						
	Jurisd. Country Name						

7.1.12.4.2 Extensions

CERTIGNA SERVER AUTHENTICATION		AUTO CA				AUTO FR CA	
Usage		Server authentication					
OID 1.2.250.1.177.6		.2.1.2.1	.2.1.2.2	.2.1.3.1	.2.1.3.2	.3.1.1.1	.3.1.1.2
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	OVCP	OVCP
RGS v2						RGS *	RGS *
Extension	**Crit.**	**Description**					
Authority Key Ident.	Non	Identifiant de la clé publique de l'AC					
Subject Key Ident.	Non	Identifiant de la clé publique du serveur					
Subject Alt. Name	Non	FQDN des différents domaines à protéger. Le caractère « _ » ne doit pas être présent aux entrées dNSName.					
Key Usage	**Oui**	Digital sign. / Key Enciph.					
Extended Key Usage	Non	id-kp-serverAuth / id-kp-clientAuth				id-kp-serverAuth	
Certificate Policies	Non	.2.1.2.1	.2.1.2.2	.2.1.3.1	.2.1.3.2	.3.1.1.1	.3.1.1.2
		2.23.140.1.2.2 (OVCP)					
		0.4.0.2042.1.7 (OVCP)					
		CPS= http://cps.certigna.com					
CRL Distribut. Points	Non	URL=http://crl.certigna.com/CertignaServerAuthenticationAutoCA.crl				URL=http://crl.certigna.com/CertignaServerAuthenticationAutoFRCA.crl	
Authority Info. Access	Non	URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/CertignaServerAuthenticationAutoCA.cer				URL=http://ocsp.certigna.com http://cert.certigna.com/CertignaServerAuthenticationAutoFRCA.cer	
Basic Constraints	**Oui**	cA = FALSE					
Cabf Organization. Identifier 2.23.140.3.1	Non						
Certif. Transparency	Non	Liste de SCTs. *Uniquement pour les certificats contenant un ou plusieurs FDQN.*					
QC Statement	Non						

7.1.12.5 Profils des certificats délivrés par Certigna Server Authentication OVCP EU CA & AUTO OVCP EU CA

7.1.12.5.1 Champs de base

Autorité		CERTIGNA SERVER AUTHENTICATION EU ROOT CA	
		CERTIGNA SERVER AUTHENTICATION OVCP EU CA	CERTIGNA SERVER AUTHENTICATION AUTO OVCP EU CA
Usage		Server authentication	
OID		1.2.250.1.177.14.1.1.1.1	1.2.250.1.177.14.2.1.1.1
ETSI 319 411		OVCP	OVCP
RGS v2		*	*
Champs		**Description**	
Version		V3	
Serial Number		Numéro de série unique délivré par un CSPRNG. Entre 128 et 160 bits	
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-256 minimum	
Subject Public Key Info		RSA 2048 minimum avant le 31/12/2025 / RSA 3072 minimum à compter du 31/12/2025	
Validity		398 jours maximum	
Issuer DN	CN =	Certigna Server Authentication OVCP EU CA	Certigna Server Authentication Auto OVCP EU CA
	OI =	NTRFR-48146308100036	NTRFR-48146308100036
	O =	Certigna	Certigna
	C =	FR	FR
Subject DN	Serial Number	Série de caractères constituée d'un aléa	
	Common Name	Un des FQDN de l'extension « Subject Alternative Name »	
	Organization Identifier		
	Organizat. Unit Name		
	Organization Name	Nom de l'entité à laquelle le serveur est rattaché	
	Street Address		
	Locality Name	Ville ou village de domiciliation de l'entité (2.5.4.7)	
	Postal Code		
	State or Province Name		
	Country Name	Pays de domiciliation de l'entité	
	Business Category		
	Jurisd. Locality Name		
	Jurisd. State/Prov. Name		
	Jurisd. Country Name		

7.1.12.5.2 Extensions

Autorité		CERTIGNA SERVER AUTHENTICATION EU ROOT CA	
		CERTIGNA SERVER AUTHENTICATION OVCP EU CA	CERTIGNA SERVER AUTHENTICATION AUTO OVCP EU CA
Usage		Server authentication	
OID		1.2.250.1.177.14.1.1.1.1	1.2.250.1.177.14.2.1.1.1
ETSI 319 411		OVCP	OVCP
RGS v2		*	*
Extension	**Crit.**	**Description**	
Authority Key Ident.	Non	Identifiant de la clé publique de l'AC	
Subject Key Ident.	Non	Identifiant de la clé publique du serveur	
Subject Alt. Name	Non	FQDN des différents domaines à protéger. Le caractère « _ » ne doit pas être présent aux entrées dNSName.	
Key Usage	**Oui**	Digital sign. / Key Enciph.	
Extended Key Usage	Non	id-kp-serverAuth	
Certificate Policies	Non	1.2.250.1.177.14.1.1.1.1	1.2.250.1.177.14.2.1.1.1
		2.23.140.1.2.2 (OVCP)	
		0.4.0.2042.1.7 (OVCP)	
		CPS= http://cps.certigna.com	
CRL Distribut. Points	Non	URL=http://crl.certigna.com/CertignaServerAuthentication OVCPEUCA.crl	http://crl.certigna.com/CertignaServerAuthenticationAuto OVCPEUCA.crl
Authority Info. Access	Non	caIssuers= http://cert.certigna.com/CertignaServerAuthentication OVCPEUCA.cer	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationAuto OVCPEUCA.cer
Basic Constraints	**Oui**	cA = FALSE	
Cabf Organization. Identifier 2.23.140.3.1	Non		
Certif. Transparency	Non	Liste de SCTs. *Uniquement pour les certificats contenant un ou plusieurs FDQN.*	
QC Statement	Non		

7.1.12.6 Profils des certificats délivrés par Certigna Services CA

7.1.12.6.1 Champs de base

CERTIGNA SERVICES CA										
Usage		Server authentication		Client authentication		Server authentication				
OID 1.2.250.1.177.2		.5.1.1.1	.5.1.1.2	.5.1.2.1	.5.1.2.2	.5.1.3.1	.5.1.4.1	.5.1.4.2	.5.1.5.1	5.1.5.2
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	QEVCP-w	QEVCP-w		QNCP-w	QNCP-w
RGS v2		RGS *	RGS *	RGS *	RGS *					
Champs		**Description**								
Version		V3								
Serial Number		Numéro de série unique délivré par un CSPRNG. Entre 128 et 160 bits								
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-256 RSA 4096								
Subject Public Key Info		RSA 2048	RSA >=3072	RSA 2048	RSA >=3072	RSA 2048	2048	3072	RSA 2048	RSA >=3072
Validity		Maximum 398 jours								
Issuer DN	CN =	Certigna Services CA								
	OU =	0002 48146308100036								
	OI =	NTRFR-48146308100036								
	O =	Dhimyotis								
	C =	FR								
Subject DN	Serial Number	Série de caractères constituée d'un aléa								
	Common Name	Un des FQDN de l'extension « Subject Alternative Name »								
	Organization Identifier					Numéro d'enregistrement de l'entité rattachée au certificat				
	Organizat. Unit Name			ICD + Identifiant de l'entité						
	Organization Name	Nom de l'entité à laquelle le serveur est rattaché								
	Street Address					N° et rue (2.5.4.9)				
	Locality Name	Ville ou village de domiciliation de l'entité (2.5.4.7)								
	Postal Code					Code postal (2.5.4.17)				
	State or Province Name					Département/région (2.5.4.8)				
	Country Name	Pays de domiciliation de l'entité								
	Business Category					Catégorie pro. (2.5.4.15)				
	Jurisd. Locality Name					Ville/village juridiction				
	Jurisd. State/Prov. Name					Département juridiction				
	Jurisd. Country Name					Pays juridiction				

7.1.12.6.2 Extensions

CERTIGNA SERVICES CA										
Usage		Server authentication		Client authentication		Server authentication				
OID 1.2.250.1.177.2		.5.1.1.1	.5.1.1.2	.5.1.2.1	.5.1.2.2	.5.1.3.1	.5.1.4.1	.5.1.4.2	.5.1.5.1	5.1.5.2
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	QEVCP-w	QEVCP-w		QNCP-w	QNCP-w
RGS v2		RGS *	RGS *	RGS *	RGS *					
Extension	**Crit.**	**Description**								
Authority Key Ident.	Non	Identifiant de la clé publique de l'AC								
Subject Key Ident.	Non	Identifiant de la clé publique du serveur								
Subject Alt. Name	Non	FQDN des différents domaines à protéger. Le caractère « _ » ne doit pas être présent aux entrées dNSName.								
Key Usage	**Oui**	Digital sign. / Key Enciph.		Digital signature		Digital signature / Key Encipherment				
Extended Key Usage	Non	id-kp-serverAuth		id-kp-clientAuth		id-kp-serverAuth / id-kp-clientAuth				
Certificate Policies	Non	.5.1.1.1	.5.1.1.2	.5.1.2.1	.5.1.2.2	.5.1.3.1	.5.1.4.1	.5.1.4.2	.5.1.5.1	5.1.5.2
		2.23.140.1.2.2 (OVCP)				2.23.140.1.1 (EVCP)			2.23.140.1.2.2	
				~~0.4.0.2042.1.7~~ ~~(OVCP)~~		0.4.0.194112.1.4 (QEVCP-w)	0.4.0.19495.3.1 (QCP-w-psd2)		0.4.0.194112.1.5 (QNCP-w)	
		CPS= https://www.certigna.fr/autorites/								
CRL Distribut. Points	Non	URL=http://crl.certigna.fr/servicesca.crl URL=http://crl.dhimyotis.com/servicesca.crl								
Authority Info. Access	Non	Si émis sous la racine « Certigna » (avant le 14/01/2026) caIssuers=http://autorite.certigna.fr/servicesca.der caIssuers=http://autorite.dhimyotis.com/servicesca.der URL=http://servicesca.ocsp.certigna.fr URL=http://servicesca.ocsp.dhimyotis.com				Si émis sous la racine « Certigna Root Ca » (à partir du 14/01/2026) caIssuers=https://autorite.certigna.fr/servicesca_rootca.der caIssuers=http://autorite.dhimyotis.com/servicesca_rootca.der URL=http://servicesca.ocsp.certigna.fr URL=http://servicesca.ocsp.dhimyotis.com				
Basic Constraints	**Oui**	cA = FALSE								
Cabf Org. Id. 2.23.140.3.1	Non					Info. Entité [2]	Info. Entité [2]		Info. Entité [2]	Info. Entité [2]
Certif. Transparency	Non	Liste de SCTs. *Uniquement pour les certificats contenant un ou plusieurs FDQN.*								
QC Statement	Non					QcCompliance				
						QcEuPDS				
						QcType 3 (web)				
							PSD2QcType [3]			

[1] Le champ « OrganizationIdentifier » (OI) est utilisé pour fournir le numéro d'enregistrement de l'entité rattachée au certificat. Si ce numéro est délivré par l'ACN, ce champ sera composé de la façon suivante :

- Les 3 caractères « PSD » en référence au type d'identité personne morale
- Les 2 caractères désignant le code du pays de l'ACN ;
- Le caractère de séparation « - » ;
- Les 2 à 8 caractères identifiant l'ACN sans le code pays ;
- Le caractère de séparation « - » et ;
- L'identifiant du PSP correspondant au numéro d'autorisation tel que spécifié par l'ACN (sans restriction sur les caractères employés)

Exemple : le champ « OI » contenant cette série de caractère « PSDFR-APCR-123456789 » signifie un certificat délivré à un PSP dont le numéro d'enregistrement est 123456789 et dont l'autorisation est fournie par une ACN française qui est l'Autorité de contrôle prudentiel et de résolution dont l'identifiant est « FR-APCR ». D'autres exemples peuvent inclure des caractères non alphanumériques tels que "PSDBE-NBB-1234.567.890" et "PSDFI-INFSA-1234567-8" et "PSDMT-MFSA-A 12345" (notez l'espace après le "A").

A noter : Le champ peut contenir également un préfixe incluant le type d'institution afin d'assurer l'unicité dans le cas où il existerait des schémas de numérotation pour différents types d'établissement avec la possibilité d'attribuer un même numéro à différentes institutions). Ce préfixe serait alors constitué d'une des chaines de caractères suivantes, suivi du caractère « : » :

- « CI » pour « Credit institution » ;
- « PI » pour « Payment institution » ;
- « EMI » pour « Electronic money institution » (or e-money institution);
- « RAISP » pour « Account information service provider » dispensé en vertu de l'article 33 de la DSP2.

[2] Extension liée au champ OrganizationIdentifier avec les informations sur l'entité sous la forme suivante :

r**egistrationSchemeIdentifier** = NTR / VAT / PSD
registrationCountry = Pays de domiciliation de l'entité
registrationStateOrProvince = Département ou région de domiciliation (si pertinent)
registrationReference = Identifiant unique assigné à l'entité légale

[3] Contenu du PSD2QcType :

- **rolesOfPSP**
  - **roleOfPspOid** = une ou plusieurs des valeurs suivantes :
    - 0.4.0.19495.1.1 (PSP_AS)
    - 0.4.0.19495.1.2 (PSP_PI)
    - 0.4.0.19495.1.3 (PSP_AI)
    - 0.4.0.19495.1.4 (PSP_IC)
  - **roleOfPspName** = une ou plusieurs des valeurs suivantes :
    - PSP_AS (Account Servicing Payment Service Provider)
    - PSP_PI (Payment Initiation Service Provider)
    - PSP_AI (Account Information Service Provider)
    - PSP_IC (Payment Service Provider issuing card-based payment

instruments)

- **nCAName** = Nom du NCA en anglais
- **nCAId** = Identifiant du NCA

Note : Les attributs du sujet présents dans le DN des certificats des serveurs ne peuvent pas contenir une unique métadonnée de type '.', '-' et ' ' (caractère espace), et/ou toute autre indication que la valeur est absente, incomplète ou non applicable. Les attributs présents dans le DN du sujet qui sont autres que ceux listés dans les « Baseline requirements » du CA/Browser Forum contiennent des attributs vérifiés par l'AC.

7.1.12.6.3 Pré-certificats

Dans le cadre de l'implémentation des exigences de la RFC 6962 relative au « Certificate Transparency », l'AC Certigna Services CA 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 dynamiquement parmi les journaux autorisés.

7.1.12.7 Profils des certificats délivrés par Certigna Wild CA

7.1.12.7.1 Champs de base

CERTIGNA WILD CA					
Usage		**multi-domains Server authentication**		**Wildcard multi-domains Server authentication**	
OID 1.2.250.1.177.2		.7.1.1.1	.7.1.1.2	.7.1.2.1	.7.1.2.2
ETSI 319 411		OVCP	OVCP	OVCP	OVCP
RGS v2					
Champs		**Description**			
Version		V3			
Serial Number		Numéro de série unique délivré par un CSPRNG. Entre 128 et 160 bits			
Signature		CA signing algorithm identifier / SHA-256 minimum			
Subject Public Key Info		RSA 2048	RSA >=3072	RSA 2048	RSA >=3072
Validity		398 days maximum			
Issuer DN	CN =	Certigna Wild CA			
	OU =	0002 48146308100036			
	OI =	NTRFR-48146308100036			
	O =	DHIMYOTIS			
	C =	FR			
Subject DN	CN =	Un des FQDN de l'extension « Subject Alternative Name »			
	OU =	ICD + Identifiant de l'entité liée au serveur (*Champ proscrit et absent à compter du 01/09/2022*)			
	O =	Nom de l'entité à laquelle le service de cachet est rattaché			
	L =	Ville où est implantée l'entité			
	C =	Pays de domiciliation de l'entité			

Les attributs du sujet présents dans le DN des certificats des serveurs ne peuvent pas contenir une unique métadonnée de type '.', '–' et ' ' (caractère espace), et/ou toute autre indication que la valeur est absente, incomplète ou non applicable. Les attributs présents dans le DN du sujet qui sont autres que ceux listés dans les « Baseline requirements » du CA/Browser Forum contiennent des attributs vérifiés par l'AC.

7.1.12.7.2 Extensions

CERTIGNA WILD CA					
Usage		**multi-domains Server authentication**		**Wildcard multi-domains Server authentication**	
OID 1.2.250.1.177.2		.7.1.1.1	.7.1.1.2	.7.1.2.1	.7.1.2.2
ETSI 319 411		OVCP	OVCP	OVCP	OVCP
RGS v2					
Champs	**Critique**	**Description**			
Authority Key Identifier	Non	Identifiant de la clé publique de l'AC			
Subject Key Identifier	Non	Identifiant de la clé publique du service de cachet			
Subject Alt. Name	Non	FQDN des différents domaines à protéger. Le caractère « _ » ne doit pas être présent dans les entrées dNSName.			
Key Usage	**Oui**	Digital signature / Key Encipherment			
Extended Key Usage	Non	id-kp-serverAuth / id-kp-clientAuth			
Certificate Policies	Non	OID=1.2.250.1.177.2.7.1.1.1 OID=2.23.140.1.2.2 (OVCP)	OID=1.2.250.1.177.2.7.1.1.2 OID=2.23.140.1.2.2 (OVCP)	OID=1.2.250.1.177.2.7.1.2.1 OID=2.23.140.1.2.2 (OVCP)	OID=1.2.250.1.177.2.7.1.2.2 OID=2.23.140.1.2.2 (OVCP)
		CPS= https://www.certigna.fr/autorites/			
CRL Distribut. Points	Non	URL=http://crl.certigna.fr/wildca.crl URL=http://crl.dhimyotis.com/wildca.crl			
Authority Info. Access	Non	Si émis sous la racine « Certigna » (avant le 14/01/2026) caIssuers=http://autorite.certigna.fr/wildca.der caIssuers=http://autorite.dhimyotis.com/wildca.der URL=http://wildca.ocsp.dhimyotis.com URL=http://wildca.ocsp.certigna.fr		Si émis sous la racine « Certigna Root Ca » (à partir du 14/01/2026) caIssuers=http://autorite.certigna.fr/wildca_rootca.der caIssuers=http://autorite.dhimyotis.com/wildca_rootca.der URL=http://wildca.ocsp.dhimyotis.com URL=http://wildca.ocsp.certigna.fr	
Basic Constraints	**Oui**	cA = FALSE			
Certificate Transparency	Non	Liste de SCTs. *Uniquement pour les certificats contenant un ou plusieurs FDQN.*			

7.1.12.7.3 Pre-certificates

Dans le cadre de l'implémentation des exigences de la RFC 6962 relative au « Certificate Transparency », l'AC Certigna Wild CA 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 dynamiquement parmi les journaux autorisés.

7.1.12.8 Profils des certificats délivrés par Certigna Server Authentication OVCP EU CA G1 & OVCP CA G1

7.1.12.8.1 Champs de base

Autorité		CERTIGNA	
		CERTIGNA SERVER AUTHENTICATION OVCP EU CA G1	CERTIGNA SERVER AUTHENTICATION OVCP CA G1
Usage		Server authentication	Server authentication
OID		1.2.250.1.177.1.23.1.1.1	1.2.250.1.177.1.22.1.1.1
ETSI 319 411		OVCP	OVCP
RGS v2		RGS *	
Champs		**Description**	
Version		V3	
Serial Number		Numéro de série unique délivré par un CSPRNG. Entre 128 et 160 bits	
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-256 minimum	
Subject Public Key Info		RSA 2048 Minimum avant le 31/12/2025 / RSA 3072 minimum à compter du 31/12/2025	
Validity		398 jours maximum	
Issuer DN	CN = OI = O = C =	Certigna Server Authentication OVCP EU CA G1 NTRFR-48146308100036 Certigna FR	Certigna Server Authentication OVCP CA G1 NTRFR-48146308100036 Certigna FR
Subject DN	Serial Number	Série de caractères constituée d'un aléa	
	Common Name	Un des FQDN de l'extension « Subject Alternative Name »	
	Organization Name	Nom de l'entité à laquelle le serveur est rattaché	
	Locality Name	Ville ou village de domiciliation de l'entité (2.5.4.7)	
	Country Name	Pays de domiciliation de l'entité	

7.1.12.8.2 Extensions

Autorité		CERTIGNA	
		CERTIGNA SERVER AUTHENTICATION OVCP EU CA G1	CERTIGNA SERVER AUTHENTICATION OVCP CA G1
Usage		Server authentication	Server authentication
OID		1.2.250.1.177.1.23.1.1.1	1.2.250.1.177.1.22.1.1.1
ETSI 319 411		OVCP	OVCP
RGS v2		RGS *	
Extension	**Crit.**	**Contenu**	
Authority Key Ident.	Non	Identifiant de la clé publique de l'AC	
Subject Key Ident.	Non	Identifiant de la clé publique du serveur	
Subject Alt. Name	Non	FQDN des différents domaines à protéger. Le caractère « _ » ne doit pas être présent aux entrées dNSName.	
Key Usage	**Oui**	Digital signature / Key Encipherment	
Extended Key Usage	Non	id-kp-serverAuth	id-kp-serverAuth / id-kp-clientAuth
Certificate Policies	Non	1.2.250.1.177.1.23.1.1.1	1.2.250.1.177.1.22.1.1.1
		2.23.140.1.2.2 (OVCP CAB FORUM) 0.4.0.2042.1.7 (OVCP ETSI)	
		CPS= http://cps.certigna.com	
CRL Distribut. Points	Non	http://crl.certigna.com/CertignaServerAuthenticationOVCPEUCAG1.crl	http://crl.certigna.com/CertignaServerAuthenticationOVCPCAG1.crl
Authority Info. Access	Non	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationOVCPEUCAG1.cer	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationOVCPCAG1.cer
Basic Constraints	**Oui**	cA = FALSE	
Certif. Transparency	Non	Liste de SCTs. *Uniquement pour les certificats contenant un ou plusieurs FDQN*	

7.1.12.9 Profils des certificats délivrés par Certigna Server Authentication ACME CA G1 & ACME CA FR G1

7.1.12.9.1 Champs de base

Autorité		CERTIGNA						
		CERTIGNA SERVER AUTHENTICATION ACME CA G1				CERTIGNA SERVER AUTHENTICATION ACME FR CA G1		
Usage		Server authentication				Server authentication		
OID 1.2.250.1.177		.1.20.1.1.1	.1.20.1.1.2	.1.20.1.1.3	.1.20.1.2.1	.1.21.1.1.1	.1.21.1.1.2	.1.21.1.1.3
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	OVCP	OVCP	OVCP
RGS v2						RGS *	RGS *	RGS *
Champs		**Description**						
Version		V3						
Serial Number		Numéro de série unique délivré par un CSPRNG. Entre 128 et 160 bits						
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-256 minimum						
Subject Public Key Info		RSA 2048	RSA 3072	RSA 4096	>= RSA 2048	RSA 2048	RSA 3072	RSA 4096
Validity		398 jours maximum						
Issuer DN	CN = OI = O = C =	Certigna Server Authentication ACME CA G1 NTRFR-48146308100036 Certigna FR				Certigna Server Authentication ACME FR CA G1 NTRFR-48146308100036 Certigna FR		
Subject DN	Serial Number	Série de caractères constituée d'un aléa						
	Common Name	Un des FQDN de l'extension « Subject Alternative Name »						
	Organization Name	Nom de l'entité à laquelle le serveur est rattaché						
	Locality Name	Ville ou village de domiciliation de l'entité (2.5.4.7)						
	Country Name	Pays de domiciliation de l'entité						

7.1.12.9.2 Extensions

Autorité		CERTIGNA						
		CERTIGNA SERVER AUTHENTICATION ACME CA G1				CERTIGNA SERVER AUTHENTICATION ACME FR CA G1		
Usage		Server authentication				Server authentication		
OID 1.2.250.1.177.1		.20.1.1.1	.20.1.1.2	.20.1.1.3	.20.1.2.1	.21.1.1.1	.21.1.1.2	.21.1.1.3
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	OVCP	OVCP	OVCP
RGS v2						RGS *	RGS *	RGS *
Extension	**Crit.**	**Contenu**						
Authority Key Ident.	Non	Identifiant de la clé publique de l'AC						
Subject Key Ident.	Non	Identifiant de la clé publique du serveur						
Subject Alt. Name	Non	FQDN des différents domaines à protéger. Le caractère « _ » ne doit pas être présent aux entrées dNSName.						
Key Usage	**Oui**	Digital signature / Key Encipherment						
Extended Key Usage	Non	id-kp-serverAuth / id-kp-clientAuth				id-kp-serverAuth		
Certificate Policies	Non	.1.20.1.1.1	.1.20.1.1.2	.1.20.1.1.3	.1.20.1.2.1	.1.21.1.1.1	.1.21.1.1.2	.1.21.1.1.3
		2.23.140.1.2.2 (OVCP CAB FORUM) 0.4.0.2042.1.7 (OVCP ETSI)						
		CPS= http://cps.certigna.com						
CRL Distribut. Points	Non	http://crl.certigna.com/CertignaServerAuthenticationACMECAG1.crl				http://crl.certigna.com/CertignaServerAuthentication ACMEFRCAG1.crl		
Authority Info. Access	Non	URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/CertignaServerAuthenticationACMECAG1.cer				URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/CertignaServerAuthentication ACMEFRCAG1.cer		
Basic Constraints	**Oui**	cA = FALSE						
Certif. Transparency	Non	Liste de SCTs. *Uniquement pour les certificats contenant un ou plusieurs FDQN.*						

7.1.12.10 Profils des certificats délivrés par Certigna Server Authentication ACME CA G2 & ACME CA FR G2

7.1.12.10.1 Champs de base

Autorité		CERTIGNA ROOT CA							
		CERTIGNA SERVER AUTHENTICATION ACME CA G2					CERTIGNA SERVER AUTHENTICATION ACME FR CA G2		
Usage		Server authentication			Server authent. Wildcard		Server authentication		
OID 1.2.250.1.177.2		.10.1.1.1	.10.1.1.2	.10.1.1.3	.10.1.2.1	.10.1.2.2	.11.1.1.1	.11.1.1.2	.11.1.1.3
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	OVCP	OVCP	OVCP	OVCP
RGS v2							RGS *	RGS *	RGS *
Champs		**Description**							
Version		V3							
Serial Number		Numéro de série unique délivré par un CSPRNG. Entre 128 et 160 bits							
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-256 minimum							
Subject Public Key Info		RSA 2048	RSA 3072	RSA 4096	RSA 3072	RSA 4096	RSA 2048	RSA 3072	RSA 4096
Validity		Maximum 398 jours							
Issuer DN	CN = OI = O = C =	Certigna Server Authentication ACME CA NTRFR-48146308100036 Certigna FR					Certigna Server Authentication ACME FR CA NTRFR-48146308100036 Certigna FR		
Subject DN	Serial Number	Série de caractères constituée d'un aléa							
	Common Name	Un des FQDN de l'extension « Subject Alternative Name »							
	Organization Name	Nom de l'entité à laquelle le serveur est rattaché							
	Locality Name	Ville ou village de domiciliation de l'entité (2.5.4.7)							
	Country Name	Pays de domiciliation de l'entité							

7.1.12.10.2 Extensions

Autorité		CERTIGNA ROOT CA							
		CERTIGNA SERVER AUTHENTICATION ACME CA G2					CERTIGNA SERVER AUTHENTICATION ACME FR CA G2		
Usage		Server authentication			Server authentication Wildcard		Server authentication		
OID 1.2.250.1.177.2		.10.1.1.1	.10.1.1.2	.10.1.1.3	.10.1.2.1	.10.1.2.2	.11.1.1.1	.11.1.1.2	.11.1.1.3
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	OVCP	OVCP	OVCP	OVCP
RGS v2							RGS *	RGS *	RGS *
Extension	**Crit.**	**Contenu**							
Authority Key Ident.	Non	Identifiant de la clé publique de l'AC							
Subject Key Ident.	Non	Identifiant de la clé publique du serveur							
Subject Alt. Name	Non	FQDN des différents domaines à protéger. Le caractère « _ » ne doit pas être présent aux entrées dNSName.							
Key Usage	**Oui**	Digital signature / Key Encipherment							
Extended Key Usage	Non	id-kp-serverAuth / id-kp-clientAuth					id-kp-serverAuth		
Certificate Policies	Non	.10.1.1.1	.10.1.1.2	.10.1.1.3	.10.1.2.1	.10.1.2.2	.11.1.1.1	.11.1.1.2	.11.1.1.3
		2.23.140.1.2.2 (OVCP CAB FORUM) 0.4.0.2042.1.7 (OVCP ETSI)							
		CPS= http://cps.certigna.com							
CRL Distribut. Points	Non	http://crl.certigna.com/CertignaServerAuthenticationACMECAG2.crl					http://crl.certigna.com/CertignaServerAuthenticationACMEFRCAG2.crl		
Authority Info. Access	Non	URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/CertignaServerAuthenticationACMECAG2.cer					URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/CertignaServerAuthenticationACMEFRCAG2.cer		
Basic Constraints	**Oui**	cA = FALSE							
Certif. Transparency	Non	Liste de SCTs. *Uniquement pour les certificats contenant un ou plusieurs FDQN.*							

7.2 Profils des LCR

7.2.1 Numéro(s) de version

Les listes de certificats révoqués sont de type X.509 v2.

7.2.2 LCR and extension de l'entrée de LCR

		CERTIGNA SERVER AUTHENTICATION ROOT CA						
		CA	AUTO CA	AUTO FR CA	OVCP CA	AUTO OVCP CA	QCP CA	AUTO QCP CA
Champs		**Description**						
Version		V2						
Signature		Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096						
Issuer DN	CN =	Certigna Server Authentication CA	Certigna Server Authentication Auto CA	Certigna Server Authentication Auto FR CA	Certigna Server Authentication OVCP CA	Certigna Server Authentication Auto OVCP CA	Certigna Server Authentication QCP CA	Certigna Server Authentication Auto QCP CA
	OI =	NTRFR-48146308100036						
	O =	Certigna						
	C =	FR						
This Update		Date de génération de la LCR						
Next Update		Date de prochaine mise à jour de la LCR [7 jours maximum]						
Revoked certificates		Liste des n° de série des certificats révoqués						
		ReasonCode [1]						
Extensions	**Crit.**	**Description**						
AKI	Non	Identifiant de la clé publique de l'AC						
CRL Nb	Non	Contient le numéro de série de la LCR						
Expired CertsOnCRL	Non	Date depuis laquelle les certificats révoqués et expirés sont maintenus dans la LCR.						

1 Une extension précisant la raison de révocation peut être présente conformément aux dispositions des chapitres 4.9.1 et 4.9.3.2.

		CERTIGNA & CERTIGNA ROOT CA		CERTIGNA		CERTIGNA SERVER AUTH. EU ROOT CA	
		SERVICES CA	WILD CA	SERVER AUTHENTICATION OVCP EU CA G1	SERVER AUTHENTICATION OVCP CA G1	SERVER AUTHENTICATION OVCP EU CA	SERVER AUTHENTICATION Auto OVCP EU CA
Champs		**Description**					
Version		V2					
Signature		Identifiant algorithme de signature de l'AC SHA-256 RSA 4096					
Issuer DN	CN =	Certigna Services CA	Certigna Wild CA	Certigna Server Authentication OVCP EU CA G1	Certigna Server Authentication OVCP CA G1	Certigna Server Authentication OVCP EU CA	Certigna Server Authentication Auto OVCP EU CA
	OU =	0002 48146308100036					
	OI =	NTRFR-48146308100036					
	O =	Dhimyotis		Certigna			
	C =	FR					
This Update		Date de génération de la LCR					
Next Update		Date de prochaine mise à jour de la LCR [7 jours maximum]					
Revoked certificates		Liste des n° de série des certificats révoqués					
		ReasonCode [1]					
Extensions	**Crit.**	**Description**					
AKI	Non	Identifiant de la clé publique de l'AC					
CRL Nb	Non	Contient le numéro de série de la LCR					
Expired CertsOnCRL	Non	Date depuis laquelle les certificats révoqués et expirés sont maintenus dans la LCR.					

[1] Une extension précisant la raison de révocation peut être présente conformément aux dispositions des chapitres 4.9.1 et 4.9.3.2.

		CERTIGNA		CERTIGNA ROOT CA	
		SERVER AUTHENTICATION ACME CA G1	SERVER AUTHENTICATION ACME FR CA G1	SERVER AUTHENTICATION ACME CA G2	SERVER AUTHENTICATION ACME FR CA G2
Champs		**Description**			
Version		V2			
Signature		Identifiant algorithme de signature de l'AC SHA-256 RSA 4096			
Issuer DN	CN =	Certigna Server Authentication ACME CA G1	Certigna Server Authentication ACME FR CA G1	Certigna Server Authentication ACME CA G2	Certigna Server Authentication ACME FR CA G2
	OU =				
	OI =	NTRFR-48146308100036			
	O =	Certigna			
	C =	FR			
This Update		Date de génération de la LCR			
Next Update		Date de prochaine mise à jour de la LCR [7 jours maximum]			
Revoked certificates		Liste des n° de série des certificats révoqués			
		ReasonCode [1]			
Extensions	**Crit.**	**Description**			
AKI	Non	Identifiant de la clé publique de l'AC			
CRL Nb	Non	Contient le numéro de série de la LCR			
Expired CertsOnCRL	Non	Date depuis laquelle les certificats révoqués et expirés sont maintenus dans la LCR.			

[1] Une extension précisant la raison de révocation peut être présente conformément aux dispositions des chapitres 4.9.1 et 4.9.3.2.

7.2.3 Profils des LAR des AC Racines

		Certigna Server Authentication Root CA	Certigna Server Authentication EU Root CA	Certigna Root CA	Certigna
Champs		**Description**			
Version		V2			
Signature		SHA-256 RSA 4096	SHA-384 RSA 4096	SHA-256 RSA 4096	
Issuer DN		CN = Certigna Server Authentication Root CA O = Certigna C = FR	CN = Certigna Server Authentication EU Root CA O = Certigna C = FR	CN = Certigna Root CA OU = 0002 48146308100036 O = Dhimyotis C = FR	CN = Certigna O = Dhimyotis C = FR
This Update		Date de génération de la LAR			
Next Update		Date de prochaine mise à jour de la LCR [1 an maximum]			
Revoked certificates		Liste des n° de série des certificats d'AC révoqués : - Numéro de série - Date de révocation - Cause de révocation (à compter du 30/09/2020)			
Extensions	**Crit.**	**Description**			
AKI	Non	Identifiant de la clé publique de l'AC			
CRL Nb	Non	Contient le numéro de série de la LAR			
Expired CertsOnCRL	Non	Date depuis laquelle les certificats révoqués et expirés sont maintenus dans la LAR.			

7.3 Profils des OCSP

7.3.1 Numéro(s) de version

Sant objet.

7.3.2 Extension OCSP

Les singleExtensions d'une réponse OCSP ne doivent pas contenir l'extension d'entrée de CRL reasonCode (OID 2.5.29.21).

Certigna Server Authentication Root CA		
Champs		**Description**
Version		V3
Signature		SHA-384 RSA 4096
Validity		15 years
Issuer DN		CN = Certigna Server Authentication Root CA O = Certigna C = FR
Subject DN		CN = Certigna Server Authentication Root OCSP OI = NTRFR-48146308100036 O = Certigna C = FR
Extensions	**Crit.**	**Description**
SKI	Non	Identifiant de la clé publique de l'AC
AKI	Non	Identifiant de la clé publique du répondeur OCSP
Key Usage	Oui	Digital signature
Extended Key Usage	Non	Signature OCSP (1.3.6.1.5.5.7.3.9)
Ocsp No Check	Non	
Basic Constraints	Oui	cA = FALSE

7.3.3 Profils des certificats OCSP pour les AC intermédiaires

Autorités		SERVER AUTHENTICATION CA	SERVER AUTHENTICATION AUTO CA	SERVER AUTHENTICATION AUTO FR CA
Champs		**Contenu**		
Version		V3		
Serial Number		Numéro de série unique délivré par un CSPRNG. Entre 128 et 160 bits		
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-256 minimum		
Subject Public Key Info		RSA 4096		
Validity		3 ans		
Issuer DN	CN =	Certigna Server Authentication CA	Certigna Server Authentication Auto CA	Certigna Server Authentication Auto FR CA
	OI =	NTRFR-48146308100036		
	O =	Certigna		
	C =	FR		
Subject DN	CN =	Certigna Server Authentication OCSP	Certigna Server Authentication Auto OCSP	Certigna Server Authentication Auto FR OCSP
	OI =	NTRFR-48146308100036		
	O =	DHIMYOTIS		
	C =	FR		
Extensions	**Crit.**	**Description**		
Authority Key Id.	Non	Identifiant de la clé publique de l'AC		
Subject Key Id.	Non	Identifiant de la clé publique du répondeur OCSP		
Key Usage	Oui	Digital signature		
Extended Key U.	Non	Signature OCSP (1.3.6.1.5.5.7.3.9)		
Ocsp No Check	Non			
Basic Constraints	Oui	cA = FALSE		

		SERVICES CA	WILD CA
Champs		**Contenu**	
Version		V3	
Serial Number		Numéro de série unique délivré par un CSPRNG. Entre 128 et 160 bits	
Signature		CA signing algorithm identifier / SHA-256 minimum	
Subject Public Key Info		RSA 3072	
Validity		3 ans	
Issuer DN	CN =	Certigna Services CA	Certigna Wild CA
	OU =	0002 48146308100036	
	OI =	NTRFR-48146308100036	
	O =	DHIMYOTIS	
	C =	FR	
Subject DN	CN =	OCSP Certigna Services CA	OCSP Certigna Wild CA
	OU =	0002 48146308100036	
	O =	DHIMYOTIS	
	C =	FR	
Extensions	**Crit.**	**Description**	
Authority Key Id.	Non	CA public key identifier	
Subject Key Id.	Non	OSCP responder public key identifier	
Key Usage	Oui	Digital signature	
Extended Key U.	Non	Signature OCSP (1.3.6.1.5.5.7.3.9)	
Ocsp No Check	Non		
Basic Constraints	Oui	cA = FALSE	

Autorité		SERVER AUTHENTICATION ACME CA G1	SERVER AUTHENTICATION ACME FR CA G1	SERVER AUTHENTICATION ACME CA G2	SERVER AUTHENTICATION ACME FR CA G2
Champs		**Description**			
Version		V3			
Serial Number		Numéro de série unique délivré par un CSPRNG. Entre 128 et 160 bits			
Signature		CA signing algorithm identifier / SHA-256 RSA 4096			
Subject Public Key Info		RSA 4096			
Validity		3 ans			
Issuer DN	CN = OI = O = C =	Certigna Server Authentication ACME CA G1 NTRFR-48146308100036 Certigna FR	Certigna Server Authentication ACME FR CA G1 NTRFR-48146308100036 Certigna FR	Certigna Server Authentication ACME CA G2 NTRFR-48146308100036 Certigna FR	Certigna Server Authentication ACME FR CA G2 NTRFR-48146308100036 Certigna FR
Subject DN	CN = OI = O = C =	Certigna Server Authentication ACME OCSP G1 NTRFR-48146308100036 DHIMYOTIS FR	Certigna Server Authentication ACME FR OCSP G1 NTRFR-48146308100036 DHIMYOTIS FR	Certigna Server Authentication ACME OCSP G2 NTRFR-48146308100036 DHIMYOTIS FR	Certigna Server Authentication ACME FR OCSP G2 NTRFR-48146308100036 DHIMYOTIS FR
Extensions	**Critiq**	**Description**			
Authority Key Id.	Non	CA public key identifier			
Subject Key Id.	Non	OSCP responder public key identifier			
Key Usage	Oui	Digital signature			
Extended Key U.	Non	Signature OCSP (1.3.6.1.5.5.7.3.9)			
Ocsp No Check	Non				
Basic Constraints	Oui	cA = FALSE			

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

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 et aux pratiques identifiées dans cette PC/DPC.

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 vise la conformité aux « Baseline Requirements documents (SSL/TLS Server Certificates) » et aux « EV Guidelines for TLS Server certificate » en vigueur du CA/Browser Forum (http://www.cabforum.org).

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 et les pratiques identifiés dans cette PC/DPC.

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 cette PC/DPC.

Ce contrôle est également effectué par l'AC à minima une fois par an. Un audit de qualification est réalisé chaque année, avec une période d'audit qui n'excède pas une durée d'un an, afin que la période pendant laquelle l'AC délivre les certificats soit divisée en une séquence ininterrompue de périodes d'audit. L'AC maintient un historique des audits de certifications et de qualifications annuels qui sont réalisés sans interruption.

Les certificats susceptibles d'être utilisés pour signer de nouveaux certificats sont, soit techniquement contraints et audités conformément à la section 8.7 uniquement, soit sans contrainte et entièrement audités conformément à toutes les exigences restantes de cette section. Un Certificat est considéré comme pouvant être utilisé pour signer de nouveaux certificats s'il contient une extension X.509v3 « basicConstraints », avec le booléen cA défini à « true » et est donc par définition un Certificat d'AC Racine ou un Certificat d'AC Subordonnée.

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 annuels de certifications et de qualifications sont réalisés par des auditeurs qualifiés. Un auditeur qualifié désigne une personne physique, une entité juridique ou un groupe de personnes physiques ou d'entités juridiques qui possèdent collectivement les qualifications et compétences suivantes :

- Indépendance vis-à-vis du sujet de l'audit ;
- La capacité à mener un audit répondant aux critères spécifiés dans un plan d'audit éligible ;
- Emploi des personnes compétentes dans l'examen de la technologie de l'infrastructure à clé publique, des outils et techniques de sécurité de l'information, de l'audit de la technologie et de la sécurité de l'information et de la fonction d'attestation par un tiers ;
- Pour les audits effectués conformément à l'une des normes ETSI, accrédité conformément à la norme ISO 17065 appliquant les exigences spécifiées dans la norme ETSI EN 319 403 ;
- Lié par la loi, la réglementation gouvernementale ou le code de déontologie professionnel ; et
- Sauf dans le cas d'une agence d'audit interne du gouvernement, maintient une assurance responsabilité professionnelle / erreurs et omissions avec des limites de couverture d'au moins un million de dollars américains.

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.

8.4 Sujets couverts par les évaluations

L'AC se soumet annuellement à un audit ETSI EN 319 411-1 qui inclut les références normatives à l'ETSI EN 319 401.

Pour les tiers délégués qui ne sont pas RA ou DRA, l'AC obtient un rapport d'audit, émis conformément aux normes d'audit, qui fournit une opinion indiquant si la performance du sous-traitant est conforme à la déclaration de pratiques énoncées du tiers délégué ou à la politique de certification et/ou des pratiques de certification de l'AC. Si l'opinion est que le tiers délégué ne se conforme pas, alors l'AC ne permet pas au tiers délégué de continuer à exercer les fonctions déléguées.

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

Une attestation d'audit est publiquement disponible sur le site de l'organisme de certification. Cette attestation est publiée au plus tard trois (3) mois après la fin de la période d'audit. Dans le cas d'un retard supérieur à trois (3) mois, l'AC fournira une lettre explicative signée par l'auditeur qualifié.

Le rapport d'audit contient au moins les informations suivantes :

- Le nom de l'organisation auditée ;
- Le nom et l'adresse de l'organisme réalisant l'audit ;
- L'empreinte digitale SHA-256 de tous les certificats d'autorité de certification racine et subordonnée, y compris les certificats croisés, qui étaient dans le champ de l'audit ;
- Les critères d'audit, avec le(s) numéro(s) de version, qui ont été utilisés pour auditer chacun des certificats (et les clés associées) ;
- Une liste des documents de politique de l'AC, avec les numéros de version, référencés lors de l'audit ;
- Si l'audit a évalué une période de temps ou un point précis dans le temps ;
- La date de début et la date de fin de la Période d'Audit, pour celles qui couvrent une période de temps ;
- La date du point dans le temps, pour ceux qui sont pour un point dans le temps ;
- La date à laquelle le rapport a été émis, qui sera nécessairement postérieure à la date de fin ou à la date de référence ; et
- Une déclaration indiquant si l'audit était un audit complet ou un audit de surveillance, et quelles parties des critères ont été appliquées et évaluées ;
- Une déclaration indiquant que l'auditeur a fait référence aux critères applicables du CA/Browser Forum et la version utilisée.

8.7 Audits internes

Les contrôles de conformité visent à vérifier le respect des engagements et pratiques définies dans la PC/DPC qui y répond, ainsi que des éléments qui en découlent (procédures opérationnelles, ressources 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/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.

À compter du 15/03/2025, l'AC utilise un processus de vérification pour contrôler l'exactitude technique des certificats à l'aide d'un échantillon sélectionné.

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 examine 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. L'AC audite en interne et annuellement la conformité de chaque tiers délégué.

Pendant la période au cours de laquelle une AC intermédiaire techniquement contrainte émet des certificats, l'AC qui a signé l'AC intermédiaire surveille le respect de la politique de certification de l'autorité de certification et de la déclaration des pratiques de certification de l'AC intermédiaire. Au moins une fois par trimestre, par rapport à un échantillon sélectionné au hasard d'au moins trois pour cent des demandes de certificats délivrés par l'AC intermédiaire, au cours de la période commençant immédiatement après le prélèvement de l'échantillon d'audit précédent, l'AC doit s'assurer que tous les PC applicables sont respectées.

Les résultats des audits de conformité effectués par l'équipe d'audit sont tenus à la disposition de l'organisme en charge de la certification et qualification de l'AC.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

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 la demande de certificat a été faite. Ainsi, tout certificat émis ne peut faire l'objet d'une demande de remboursement notamment suite à des difficultés de mise en œuvre liées notamment à l'environnement technique d'exploitation du certificat (ex : non-conformité des logiciels ou matériels stockant et utilisant le certificat avec les standards et normes en vigueur). Toutefois, dans l'hypothèse où le certificat ne correspond pas à la demande de certificat suite à une erreur exclusivement imputable à l'AC, l'AC s'engage à fournir un certificat conforme, ou le cas échéant s'il est dans l'incapacité de le faire, de procéder au remboursement des sommes déjà versées au titre de la commande du certificat.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

L'AC est titulaire d'une police d'assurance en matière de Responsabilité Civile Professionnelle, garantissant les dommages directs matériels ou immatériels consécutifs causés dans l'exercice de son activité professionnelle.

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 PC/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 RC ;
- Les causes de révocation des certificats.

9.3.2 Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3 Responsabilités en termes de protection des informations confidentielles

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

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

L'AC applique des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles au 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage. De plus, lorsque ces données sont échangées, l'AC en garantit l'intégrité.

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

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

En acceptant les CGVU, le Demandeur, le RC reconnaît avoir pris connaissance de la Politique d'utilisation des Données Personnelles de CERTIGNA disponible sur le Site https://www.certigna.com/politique-dutilisation-des-donnees-personnelles/.

Les données fournies par le Demandeur, le RC, lors de son inscription sur le Site https://www.certigna.com, lors de sa commande et lors de sa demande de certificats sont des Données Personnelles dont la collecte et le traitement sont régis par la Politique d'utilisation des Données Personnelles susvisée.

Les dossiers de demande de certificat électronique comportant les données personnelles sont archivés à minima pendant au moins sept ans après l'expiration des certificats associés 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. Les informations personnelles d'identité peuvent être utilisées comme données d'authentification lors d'une éventuelle demande de révocation ou d'informations.

Les journaux applicatifs liés au cycle de vie des certificats et comportant les données personnelles sont archivés à minima sept ans après l'expiration des certificats associés 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.

Par ailleurs, CERTIGNA conserve les données à caractère personnel pendant une durée de trois ans à compter de la fin des relations commerciales avec le client et 3 ans à compter du dernier contact émanant avec le prospect. Le délai commence à partir de la dernière connexion au compte client ou du dernier envoi d'un courriel au service client, ou d'un clic sur un lien hypertexte d'un courriel adressé par DHIMYOTIS, ou d'une réponse positive à un courriel demandant si le client souhaite continuer à recevoir de la prospection commerciale à l'échéance du délai de trois ans.

Afin de suivre la qualité de nos services, les appels réalisés auprès de notre service client sont susceptibles d'être enregistrés et conservés durant une période de 30 jours.

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@certigna.com, ou par courrier à l'adresse suivante :

CERTIGNA, 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 ;
- Les dossiers 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 pas 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.

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 web 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/DPC ;
- 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 l'émission d'un certificat, les exigences décrites au chapitre 3.2 et 3.3 pour vérifier que l'organisation rattachée au serveur web 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/DPC.
- Mettre en œuvre et suivre, lors de la délivrance d'un certificat, les exigences décrites aux chapitres 3.2 et 3.3 de la 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).

L'AC assume toute conséquence dommageable résultant du non-respect de sa PC/DPC par elle-même ou l'une de ses composantes. Elle a pris les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique. De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des RC à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

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

L'AC racine est responsable des performances et des garanties de chaque AC intermédiaire, de la conformité de l'AC intermédiaire aux exigences, ainsi que de toutes les responsabilités et obligations d'indemnisation de l'AC intermédiaire, comme si l'AC racine était l'AC intermédiaire délivrant les Certificats.

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 Demandeur et RC

Le RC a le devoir de :

- Effectuer sa demande de certificat en suivant toutes les étapes de la procédure figurant sur le site https://www.certigna.fr.
- Respecter les Conditions Générales de Vente et d'Utilisation (CGVU) du certificat demandé ;
- Avoir connaissance et accepter que l'AC a le pouvoir de révoquer le certificat immédiatement si le RC, ou le Demandeur ne respecte pas les CGVU ou si la révocation est requise par la PC/DPC ou les exigences applicables ;
- Communiquer des informations exactes, complètes et à jour pour la demande de certificat ou son renouvellement ;

- Transmettre à l'AE, le cas échéant à l'AED, ou à un MC de son entité, en main propre ou par voie postale, le formulaire d'inscription généré lors de la demande de certificat en ligne sur le site https://www.certigna.fr ou sur le site de l'AED le cas échéant, le paiement, ainsi que les pièces justificatives.
- Utiliser et générer le cas échéant, la bi-clé avec un modulus RSA de 2048 bits minimum et en respectant les spécifications de l'ETSI 119 312 ;
- Générer et utiliser la bi-clé associée au certificat dans un dispositif qui est conforme aux exigences de sécurité du chapitre 11 de la PC/DPC associée au certificat.
- Des justificatifs attestant de la conformité du dispositif pourront être demandés par l'AC lors de la demande de certificat (cas notamment d'un certificat de cachet). Ces justificatifs seront à minima la facture d'achat du dispositif et des photos/impressions d'écran des caractéristiques matérielles et logicielles du dispositif et du numéro de série associé. L'AC se réserve le droit de refuser la demande de certificat en l'absence de justificatifs ou s'il était avéré que ce dispositif ne réponde pas à ces exigences.
- Dans le cas où l'AC serait informée ou aurait identifié la perte de la conformité du dispositif, l'AC demandera au RC les preuves attestant que la bi-clé est toujours stockée dans un dispositif répondant aux exigences du chapitre 11 de la Politique de Certification associée au certificat. le le RC s'engage à fournir ces preuves (Ex : Facture d'achat d'un nouveau dispositif, Procès-verbal de cérémonie des clés en cas de migration des clés, Procès-verbal de mise à jour du dispositif pour le maintien de la certification, etc.) dans un délai de quinze (15) jours suivants la demande par l'AC. Dans le cas où aucune preuve ne seraient fournies ou que ces dernières ne permettraient pas de déterminer si les conditions de stockage de la bi-clé, et de transfert dans un autre dispositif le cas échéant, répondent aux exigences de la Politique de Certification, l'AC se donne le droit de révoquer le certificat.
- Informer l'AE en cas de non-réception d'un e-mail confirmant la prise en compte de la demande de certificat ou de révocation ;
- Suite à la réception d'un e-mail de l'AE signalant la non-conformité de la demande de certificat ou que le dossier est incomplet, d'effectuer les modifications sous sept (7) jours calendaires après la réception de cet e-mail ;
- Télécharger le certificat généré, mis à disposition sur son espace client le cas échéant, dans les trente (30) jours qui suivent la validation de la demande de certificat qui est notifiée par e-mail au RC. Au-delà de ce délai, le certificat est révoqué automatiquement par l'AE.
- Accepter le certificat après sa génération explicitement depuis son espace client CERTIGNA ou celui de son AED le cas échéant, ou tacitement lors de l'usage du service ACME. Cette acceptation peut également être opérée par l'envoi d'un courrier papier signé par le RC sur demande expresse de l'AE. En cas de non-acceptation explicite, le certificat est automatiquement révoqué par l'AE ;
- Protéger la clé privée associée au certificat dont il a la responsabilité par des moyens appropriés à son environnement et conformément aux exigences du chapitre 11 ;
- Protéger ses données d'activation et, le cas échéant, les mettre en œuvre ;
- Protéger l'accès à la base de certificats du serveur pour les certificats d'authentification serveur ;
- Respecter les conditions d'usages du certificat et de la clé privée associée citées au chapitre 4.5;
- Informer l'AC de toute modification concernant les informations contenues dans le certificat ;
- Faire, sans délai, une demande de révocation du certificat dont il est responsable auprès de l'AE, de l'AED auprès de laquelle la demande de certificat a été effectuée ou le cas échéant du MC de l'entité, en cas de perte, de vol, de compromission ou de suspicion de compromission de la clé privée correspondante, ou lorsque l'une des causes de révocation du chapitre 4.9.1 est rencontrée;
- Prendre toutes les mesures propres à assurer la sécurité du ou des dispositifs sur lesquels est installé le certificat. Le RC est le seul responsable de l'installation du certificat ;
- Installer un certificat d'authentification web uniquement sur les serveurs qui sont accessibles au(x) subjectAltName(s) listé(s) dans le certificat ;

- Répondre aux instructions de l'AC concernant une clé compromise ou un certificat mal utilisé sous 24 heures ;
- Ne plus utiliser immédiatement et de manière permanente un certificat et sa clé privée suite à l'expiration ou la révocation de ce certificat et à supprimer la bi-clé associée, sauf s'il s'agit d'une clé de déchiffrement ;
- Ne plus utiliser un certificat s'il a été révoqué ou si l'AC l'ayant délivré a été compromise ;
- Informer l'AE sans délai de son départ de l'entité ou de son changement de responsabilités et du besoin d'enregistrer un nouveau RC ;
- Vérifier l'adéquation à son besoin du certificat et de ses caractéristiques ;
- S'assurer que les prérequis matériels et/ou logiciels préconisés par l'AC sont remplis en vue de l'installation le cas échéant et de l'utilisation du certificat ;
- Disposer de toutes les compétences et moyens nécessaires pour utiliser les certificats ;
- Mettre en œuvre des mesures permettant d'empêcher toute personne non autorisée d'accéder physiquement au dispositif stockant la clé privée et le certificat ;
- Prévenir sans délai la personne en charge de la sécurité des systèmes d'information de son entité (exemple : RSSI) en cas de perte ou de vol du dispositif stockant les clés et le certificat ; et
- Pour les applications jugées les plus critiques au niveau métier, mettre en place des mesures permettant de détecter des transactions potentiellement frauduleuses (incohérence des données métiers signés, etc.) et de prévoir, le cas échéant, une procédure alternative.
- S'il s'agit d'un certificat d'authentification serveur et/ou client, et dans le cas où pour un ou plusieurs noms de domaine à intégrer dans le certificat, l'option « DNS CAA » est activée, le RC doit mettre à jour les enregistrements DNS associés afin d'y faire figurer l'AC, et ce préalablement à la demande de certificat.

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.

Le demandeur de certificat a le devoir de :

- Effectuer sa demande de certificat en suivant toutes les étapes de la procédure figurant sur le site https://www.certigna.fr ;
- Respecter les Conditions Générales de Vente et d'Utilisation (CGVU) du certificat demandé ;
- Avoir connaissance et accepter que l'AC a le pouvoir de révoquer le certificat immédiatement si le RC ou le Demandeur ne respecte pas les CGVU ou si la révocation est requise par la PC, la DPC ou les exigences applicables ;
- Communiquer des informations exactes, complètes et à jour pour la demande de certificat ou son renouvellement ;
- Confirmer que les informations à placer dans le certificat sont correctes ;
- Transmettre à l'AE, le cas échéant à l'AED, ou à un MC de son entité, en main propre ou par voie postale, le formulaire d'inscription généré lors de la demande de certificat en ligne sur le site https://www.certigna.fr ou sur le site de l'AED le cas échéant, le paiement, ainsi que les pièces justificatives.
- Respecter les conditions d'usages du certificat et de la clé privée associée citées au chapitre 4.5 et interdire tout utilisation non autorisée de la clé privée du serveur ;
- Utiliser et générer le cas échéant, la bi-clé avec un modulus RSA de 2048 bits minimum et en respectant les spécifications de l'ETSI 119 312 ;
- Générer le cas échéant, la bi-clé associé au CERTIFICAT dans un dispositif qui est conforme aux exigences de sécurité du chapitre 11 ;
- Des justificatifs attestant de la conformité du dispositif pourront être demandés par l'AC lors de la demande de certificat (cas notamment d'un certificat de cachet). Ces justificatifs seront à

minima la facture d'achat du dispositif et des photos/impressions d'écran des caractéristiques matérielles et logicielles du dispositif et du numéro de série associé. L'AC se réserve le droit de refuser la demande de certificat en l'absence de justificatifs ou s'il était avéré que ce dispositif ne réponde pas à ces exigences.

- Maintenir la clé privée du serveur sous le seul contrôle de la personne morale associée ;
- Informer sans délai l'AC de toute perte, vol ou compromission de la clé privée du serveur ;
- Informer sans délai l'AC si le contrôle de la clé privée du serveur a été perdu en raison de la compromission des données d'activation (par exemple, le code PIN) ou d'autres raisons ;
- Informer sans délai l'AC de toute modification concernant les informations contenues dans le certificat ;
- Informer l'AE en cas de non-réception d'un e-mail confirmant la prise en compte de la demande de certificat ou de révocation ;
- Suite à la réception d'un e-mail de l'AE signalant la non-conformité de la demande de certificat ou que le dossier est incomplet, d'effectuer les modifications sous sept (7) jours calendaires après la réception de cet e-mail ;
- S'assurer que le certificat du serveur n'est plus utilisé suite à l'expiration ou la révocation de ce certificat (Excepté pour les clés de déchiffrement) ;
- Répondre aux instructions de l'AC concernant une clé compromise ou un certificat mal utilisé sous 24 heures.

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 d'entité finale 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 présente PC/DPC.

9.6.5 Autres participants

Sans objet.

9.6.6 Résiliation

En cas de manquement par l'AC ou le RC à l'une de ses obligations au titre de cette PC, l'autre partie sera autorisée, trente (30) jours après mise en demeure envoyée par lettre recommandée avec avis de réception restée sans effet, à mettre fin à ses obligations de plein droit par lettre recommandée avec avis de réception sans préjudice de tous dommages et intérêts auxquels elle pourrait prétendre du fait des manquements invoqués.

9.7 Livraison et garantie

Tout certificat commandé doit être accepté par le RC sur l'espace client qu'il s'est créé depuis le site de l'AC ou de l'un de ses AED. Avant la génération du certificat, le RC doit vérifier que les informations

énoncées dans la demande de certificat sont exactes. A défaut, le RC doit prendre contact avec un membre du personnel de l'AC ou de l'AED. S'il s'agit de l'AC, soit par téléphone au 0 806 115 115 (service gratuit coût d'un appel local), soit par email à l'adresse suivante : contact@certigna.fr. Le support téléphonique est disponible du lundi au vendredi, sauf jours fériés, de 9h à 18h sans interruption. Le RC est conscient qu'en cas d'erreur lors de la commande dans la nature même du certificat, aucune modification ne pourra être faite par l'AC et une nouvelle demande de certificat devra être réalisée par le RC. Si un paiement avait déjà été effectué, l'AC ne serait tenue à aucun remboursement.

Une fois la demande de certificat validée, le certificat est généré. Le RC est alors amené à confirmer l'exactitude desdites informations, ce qui vaut acceptation du certificat. A ce stade, aucune modification des informations ne peut être effectuée par l'AC. Il est donc de la responsabilité du RC de bien vérifier l'exactitude de ses informations la première fois que cela lui est demandé. A défaut, le RC devra faire une nouvelle demande de certificat et le certificat généré ne donnera lieu à aucun remboursement.

Une fois le certificat accepté, celui-ci est mis à la disposition du RC soit depuis son espace client, soit sur un support cryptographique. L'installation du certificat se fait sous la seule responsabilité du RC. En cas de difficulté quelconque pendant cette dernière phase, le RC peut contacter l'AC ou l'AED au numéro de téléphone et l'adresse email de l'AC indiqués précédemment ou aux coordonnées disponibles sur le site de l'AED. L'AC ne garantit pas le fonctionnement du certificat dans le cas d'une utilisation en dehors des usages prévus au chapitre 1.5 de la présente DPC.

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

9.8 Limite de responsabilité

L'AC est soumise à une obligation générale de moyens. L'AC ne pourra voir sa responsabilité engagée à l'égard du RC ou du Demandeur que pour les dommages directs qui pourraient lui être imputés au titre des prestations qui lui sont confiées dans le cadre de la présente PC et des CGVU associées.

La responsabilité de l'AC ne pourra pas être recherchée pour tout préjudice indirect, tel que notamment, la perte de chiffre d'affaires, la perte de bénéfice, la perte de commandes, la perte de données, la perte d'une chance, le trouble à l'image ou tout autre dommage spécial ou évènements en dehors de son contrôle ou de tout fait ne lui étant pas imputable.

L'AC n'est responsable que des tâches expressément mises à sa charge. L'AC ne saurait être tenue responsable de quelque manière que ce soit de l'utilisation faite par le RC du certificat, ni du contenu des documents et des données qui lui sont remis par le RC, ou le Demandeur.

En aucun cas, la responsabilité de l'AC ne saurait être recherchée pour :

- Faute, négligence, omission ou défaillance de l'AC, qui constituerait la cause exclusive de survenance du dommage,
- Dysfonctionnement ou d'indisponibilité d'un bien matériel ou immatériel dans le cas où celui-ci a été fourni par le RC,
- Retard dans la fourniture des données à traiter dû au RC ;

- Perte de la qualification d'un tiers prestataire qui est indépendant de la volonté de CERTIGNA (Ex : le fournisseur du support cryptographique du certificat).

De convention expresse entre l'AC et le RC, la responsabilité de l'AC est limitée, tous préjudices confondus, à la somme de deux (2) fois le montant réglé au titre de la commande du certificat.

9.9 Indemnités

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

L'AC comprend 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 dégage 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 lorsqu'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).

9.9.1 Indemnisation par le RC

Sans objet.

9.9.2 Indemnisation par un tiers

Sans objet.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

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

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/DPC 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/DPC 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/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/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 une mise à jour de la PC/DPC sont effectuées annuellement et si nécessaire.

9.12.2 Mécanisme et période d'information sur les amendements

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

9.12.3 Circonstances selon lesquelles l'OID doit être changé

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

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

9.13 Dispositions concernant la résolution de conflits

La validité de la PC/DPC et toute autre question ou litiges relatifs à son interprétation, à son exécution ou à sa résiliation seront régis par le droit français.

L'AC et le RC s'engagent à consacrer leurs meilleurs efforts à la résolution amiable de toutes les questions ou de tous les litiges qui pourraient les diviser, préalablement à la saisie de la juridiction ci-après désignée.

L'AC et le RC conviennent, pour le cas où un accord amiable serait impossible à arrêter, que les juridictions de Lille auront compétences exclusives pour connaître de tout différend résultant de la validité, de l'interprétation, de l'exécution ou de la résiliation des présentes, et plus généralement de tout litige procédant des présentes qui pourrait les diviser, nonobstant pluralités des défendeurs ou appel en garantie.

Pour porter une réclamation à la connaissance de CERTIGNA, veuillez utiliser le formulaire de contact disponible à l'adresse suivante https://www.certigna.com/contactez-nous/ et sélectionner le motif « Réclamation ».

Vous pouvez également porter réclamation à notre service client aux coordonnées suivantes :

- Contact mail **:** contact@certigna.fr ;
- Téléphone : 0 806 115 115 (Service gratuit) disponible du lundi au vendredi de 09h00 à 18h00 ;
- Chat sur le site https://www.certigna.com et disponible du lundi au vendredi de 09h00 à 18h00 ;
- Courrier adressé à :

CERTIGNA
20 allée de la Râperie
Zone de la plaine
59650 Villeneuve d'Ascq, France

Les informations relatives au traitement de vos données personnelles sont disponibles dans la Politique d'utilisation des données personnelles accessible à l'adresse suivante : https://www.certigna.com/politique-dutilisation-des-donnees-personnelles/.

9.14 Juridictions compétentes

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

9.15 Conformité aux législations et réglementations

La présente PC/DPC est soumise au droit français et aux textes législatifs applicables à la présente DPC. Les pratiques de services de confiance en vertu desquelles l'AC opère sont non-discriminatoires.

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

9.16.4 Application et renonciation

Aucune renonciation à se prévaloir de l'un de ses droits ne saurait intervenir tacitement. Pour être opposable à l'AC une renonciation doit avoir été formulée par écrit. Une telle renonciation ne saurait constituer une renonciation pour l'avenir aux dits droits.

9.16.5 Force majeure

L'AC ne pourra être tenue pour responsable de tout retard ou manquement dans l'exécution de l'une quelconque de ses obligations au titre de la présente DPC, si ledit retard ou manquement est dû à la survenance d'un cas de force majeure habituellement reconnu par la jurisprudence des cours et tribunaux français.

9.17 Autres dispositions

9.17.1 Tests supplémentaires

Les certificats émis sur son environnement de production à des fins de test sont conformes aux exigences de ce document, et ne sont pas utilisés pour des usages autres que les tests. L'AC réduit notamment la durée de vie des certificats de test à la durée des tests ou révoque les certificats de test à l'issue de la réalisation des tests.

10 ANNEXE 1 : EXIGENCE DE SECURITE 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 UTILISÉ PAR LE SERVEUR

11.1 Exigences sur les objectifs de sécurité

RGS *
Le dispositif utilisé par le service de cachet 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 service de cachet ou d'authentification web 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 un cachet qui ne peut être falsifié sans la connaissance de la clé privée ; - Détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de 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

Sans objet.

Certigna

www.certigna.com

© Certigna, Services de confiance numérique