CERTIGNA
Services de confiance numérique

DECLARATION DES PRATIQUES DE CERTIFICATION

CERTIGNA

Edité le :	05/06/2020
Version :	3.1
OID :	1.2.250.1.177.2.0.1
Auteurs :	J. Allemandou
Classification :	Publique

tessi

SOMMAIRE

1 INTRODUCTION 5

1.1 Présentation générale 5

1.2 Nom et identification du document 6

1.3 Entités intervenant dans l'IGC 7

1.4 Usage des certificats 12

1.5 Gestion de la PC 13

1.6 Définitions et acronymes 14

2 RESPONSABILITE CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS 20

2.1 Publication 20

2.2 Publication de la documentation 20

2.3 Délais et fréquences de publication 23

2.4 Contrôle d'accès aux informations publiées 23

2.5 Signaler un certificat malveillant ou dangereux 23

3 IDENTIFICATION ET AUTHENTIFICATION 24

3.1 Nommage 24

3.2 Validation initiale de l'identité 26

3.3 Identification et authentification d'une demande de renouvellement des clés 45

3.4 Identification et authentification d'une demande de révocation 46

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS 48

4.1 Demande de certificat 48

4.2 Traitement d'une demande de certificat 49

4.3 Délivrance du certificat 51

4.4 Acceptation du certificat 52

4.5 Usages de la bi-clé et du certificat 53

4.6 Renouvellement d'un certificat 53

4.7 Délivrance d'un nouveau certificat suite au changement du bi-clé 54

4.8 Modification du certificat 55

4.9 Révocation et suspension des certificats 56

4.10 Fonction d'information sur l'état des certificats 63

4.11 Fin de la relation entre le Porteur et l'AC 64

4.12 Séquestre de clé et recouvrement 65

5 MESURES DE SECURITE NON TECHNIQUES 67

5.1 Mesures de sécurité physique 67
5.2 Mesures de sécurité procédurales 69
5.3 Mesures de sécurité vis-à-vis du personnel 70
5.4 Procédures de constitution des données d'audit 73
5.5 Archivage des données 75
5.6 Renouvellement d'une clé de composante de l'IGC 77
5.7 Reprise suite à compromission et sinistre 78
5.8 Fin de vie de l'IGC 79

6 MESURES DE SECURITE TECHNIQUES 81
6.1 Génération et installation de bi-clés 81
6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques 84
6.3 Autres aspects de la gestion des bi-clés 88
6.4 Données d'activation 89
6.5 Mesures de sécurité des systèmes informatiques 90
6.6 Mesures de sécurité des systèmes durant leur cycle de vie 90
6.7 Mesures de sécurité réseau 91
6.8 Horodatage et Système de datation 91

7 PROFIL DES CERTIFICATS ET DES LCR 92
7.1 Hiérarchie de confiance 92
7.2 Profils des certificats des AC Racines 93
7.3 Profils des certificats des AC intermédiaires pour personne morale 94
7.4 Profils des certificats des AC intermédiaires pour personne physique 95
7.5 Profils des certificats OCSP des AC intermédiaires pour personne morale 113
7.6 Profils des certificats OCSP des AC intermédiaires pour personne physique 114
7.7 Profils des LCR des AC intermédiaires 115
7.8 Traitement des extensions de certificats par les applications 116

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS 118
8.1 Fréquences et/ou circonstances des évaluations 118
8.2 Identités/qualifications des évaluateurs 118
8.3 Relations entre évaluateurs et entités évaluées 118
8.4 Sujets couverts par les évaluations 118
8.5 Actions prises suite aux conclusions des évaluations 119
8.6 Communication des résultats 119

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES 120

9.1 Tarifs....120
9.2 Responsabilité financière....120
9.3 Confidentialité des données professionnelles....121
9.4 Protection des données personnelles....121
9.5 Droits sur la propriété intellectuelle et industrielle....123
9.6 Interprétations contractuelles et garanties....123
9.7 Livraison et garantie....125
9.8 Limite de responsabilité....126
9.9 Indemnités....127
9.10 Durée et fin anticipée de validité de la PC....127
9.11 Notifications individuelles et communications entre les participants....128
9.12 Amendements à la PC....128
9.13 Dispositions concernant la résolution de conflits....129
9.14 Juridictions compétentes....129
9.15 Conformité aux législations et réglementations....129
9.16 Dispositions diverses....129
9.17 Autres dispositions....130

10 ANNEXE 1 : EXIGENCE DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC....131
10.1 Exigences sur les objectifs de sécurité....131
10.2 Exigences sur la qualification....131

11 ANNEXE 2 : EXIGENCES DE SÉCURITÉ DU DISPOSITIF UTILISÉ PAR LE SERVICE, SERVEUR OU PORTEUR....132
11.1 Exigences sur les objectifs de sécurité....132
11.2 Exigences sur la qualification....133

1 INTRODUCTION

1.1 Présentation générale

CERTIGNA s'est dotée de plusieurs autorités de certifications (AC) pour délivrer des certificats électroniques à des personnes morales et des personnes physiques. La présente Déclaration des Pratiques de Certification (DPC) expose les pratiques que CERTIGNA applique dans le cadre de la fourniture de ses services de certification électronique aux usagers en conformité avec sa Politique de Certification (PC) qu'elle s'est engagée à respecter. L'attention du lecteur est attirée sur le fait que la compréhension de la présente DPC suppose qu'il soit familiarisé avec les notions liées à la technologie des Infrastructures de Gestion de Clés (IGC). La présente DPC vise la conformité aux standards et niveaux de sécurité suivants :

CERTIGNA ROOT CA	OID		
Signature	1.2.250.1.177.2.0.1		
CERTIGNA ENTITY CA		RGS	ETSI
Cachet mails et documents	1.2.250.1.177.2.6.1.1.1	*	EN 319 411-1 LCP
Cachet mails et documents	1.2.250.1.177.2.6.1.4.1	**	EN 319 411-2 QCP-l-qscd
Cachet mails et documents	1.2.250.1.177.2.6.1.42.1	**	
Cachet mails et documents	1.2.250.1.177.2.6.1.41.1		EN 319 411-2 QCP-l-qscd
Cachet mails et documents	1.2.250.1.177.2.6.1.7.1		EN 319 411-2 QCP-l
Cachet mails et documents	1.2.250.1.177.2.6.1.8.1		EN 319 411-2 QCP-l / TS 119 495 DSP2
Cachet jetons d'horodatage	1.2.250.1.177.2.6.1.9.1		EN 319 411-2 QCP-l
Cachet jetons d'horodatage	1.2.250.1.177.2.6.1.3.1	*	EN 319 411-1 LCP
Cachet jetons d'horodatage	1.2.250.1.177.2.6.1.6.1	**	EN 319 411-2 QCP-l-qscd
CERTIGNA ENTITY CODE SIGNING CA		RGS	ETSI
Cachet de code	1.2.250.1.177.2.8.1.1.1	*	EN 319 411-1 LCP
Cachet de code	1.2.250.1.177.2.8.1.2.1	**	EN 319 411-2 QCP-l-qscd
FR03		RGS	ETSI
Cachet de 2D-DOC	1.2.250.1.177.2.2.1.1	*	EN 319 411-1 NCP+
CERTIGNA SERVICES CA		RGS	ETSI
Authentification serveur	1.2.250.1.177.2.5.1.1.1	*	EN 319 411-1 OVCP
Authentification client	1.2.250.1.177.2.5.1.2.1	*	EN 319 411-1 OVCP
Authentification client/serveur	1.2.250.1.177.2.5.1.3.1		EN 319 411-2 QCP-w
Authentification client/serveur	1.2.250.1.177.2.5.1.4.1		EN 319 411-2 QCP-w / TS 119 495 DSP2
CERTIGNA WILD CA		RGS	ETSI
Authentification client/serveur	1.2.250.1.177.2.7.1.1.1		EN 319 411-1 OVCP
Authentification wildcard	1.2.250.1.177.2.7.1.2.1		EN 319 411-1 OVCP
CERTIGNA IDENTITY CA		RGS	ETSI
Chiffrement	1.2.250.1.177.2.3.1.1.1	*	EN 319 411-1 LCP
Chiffrement	1.2.250.1.177.2.3.1.3.1	*	EN 319 411-1 LCP
Authentification & signature	1.2.250.1.177.2.3.1.2.1	*	EN 319 411-1 LCP
Authentification & signature	1.2.250.1.177.2.3.1.4.1	*	EN 319 411-1 LCP
CERTIGNA IDENTITY PLUS CA		RGS	ETSI
Authentification & signature	1.2.250.1.177.2.4.1.1.1	**	EN 319 411-2 QCP-n-qscd
Authentification	1.2.250.1.177.2.4.1.2.1	***	EN 319 411-1 NCP+
Signature	1.2.250.1.177.2.4.1.3.1	***	EN 319 411-2 QCP-n-qscd
Authentification & signature	1.2.250.1.177.2.4.1.4.1	**	EN 319 411-2 QCP-n-qscd
Authentification	1.2.250.1.177.2.4.1.5.1	***	EN 319 411-1 NCP+
Signature	1.2.250.1.177.2.4.1.6.1	***	EN 319 411-2 QCP-n-qscd
Authentification & signature	1.2.250.1.177.2.4.1.7.1		EN 319 411-2 QCP-n
Authentification & signature	1.2.250.1.177.2.4.1.8.1		EN 319 411-2 QCP-n-qscd

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

1.2 Nom et identification du document

La présente DPC peut être identifiée par le nom de l'AC « Certigna Root CA » ainsi que par son OID : 1.2.250.1.177.2.0.2. Elle décrit les dispositions mises en œuvre pour répondre aux engagements formulés dans la PC ayant l'OID suivant : 1.2.250.1.177.2.0.1. Les certificats d'AC intermédiaires et finaux délivrés sous cette AC racine disposent également d'un OID permettant d'identifier clairement les pratiques de cette DPC qui lui sont applicables.

1.2.1 Révision du document

Cette DPC est un regroupement de toutes les DPC des AC intermédiaires émises sous cette AC racine. Afin de faciliter l'accès à l'information, il a été décidé de regrouper l'ensemble de ces documents en une seule DPC. Le tableau ci-dessous présente l'historique de cette DPC, et l'historique des anciennes versions des DPC d'AC intermédiaires à la page suivante : https://www.certigna.com/autorite-crl

Ver.	Date	Modifications apportées
1.0	03/11/2008	Création
1.1	01/02/2019	Révision de la charte graphique et des engagements.
3.0	30/03/2020	Regroupement des DPC des AC intermédiaire sous cette unique DPC. Nouvelle charte graphique TESSI. Précisions apportées sur : - Conformité aux spécifications ETSI 319 412 applicables (cf. 1.1, 7), - Causes possible de révocation des certificats d'AC (cf. 4.9.1), - Conservation des dossiers de demandes (cf. 5.5.2.1, 5.5.2.3, 9.4.1), - Mise en ligne ponctuelles des AC racines pour LAR (cf. 6.2.7), - Politique de remboursement (9.1.5), - Couverture des assurances (9.2.1), - Résiliation (9.6.6), - Livraison et garantie (9.7), - Limite de responsabilité (9.8), - Dispositions concernant la résolution de conflits (9.13), - Modalités de renonciation, force majeure (9.16).
3.1	05/06/2020	Précision apportées sur : - L'authentification d'un RC et d'un MC (cf. 3.2.3.2.1 et 3.2.3.4), - Le champ SAN des certificats FR03 (cf. 7.4.1.2).

1.2.2 Versions précédentes des DPC regroupées dans ce document

Version précédente	Autorité de Certification associée à la PC
1.5	Certigna Root CA
1.7	Certigna Entity CA
1.5	Certigna Entity Code Signing CA
1.7	FR03
2.4	Certigna Services CA
2.0	Certigna Wild CA
1.9	Certigna Identity CA
1.7	Certigna Identity Plus CA

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

L'AC assure ces fonctions directement ou en les sous-traitant, tout ou partie. Dans tous les cas, l'AC en garde la responsabilité. L'AC s'engage à respecter les obligations décrites dans la PC associée. 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 DPC :
- La prise en compte et la vérification des informations du futur Responsable de Certificat (RC) ou Porteur 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, du Porteur 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 en garde la responsabilité.

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

(*) : L'AE offre la possibilité à l'entité cliente d'utiliser un Mandataire de Certification (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.

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

1.3.3 Responsable de certificat ou Porteur

Deux termes différents sont utilisés dans cette DPC lorsqu'il s'agit d'évoquer la personne qui se voit délivrer un certificat et gérer ce dernier :

- 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.
- On parlera du « Porteur » lorsque le certificat délivré est destiné à une personne physique, pour signer, s'authentifier ou chiffrer des données. Le porteur est alors la personne physique désignée explicitement dans le certificat.

Le RC ou le Porteur doit respecter les conditions et obligations de cette PC et des CGVU.

1.3.3.1 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.

1.3.3.2 Responsable du certificat d'un service applicatif ou d'un serveur web

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
FR03	*Cachet 2D-DOC*
SERVICES CA	*Authentification web*
WILD CA	*Authentification 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 service applicatif ou 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 service applicatif ou 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.	

FR03	*Cachet 2D-DOC*
Les émetteurs de 2D-DOC doivent être référencés par l'ANTS. D'après la norme 2D-DOC, un émetteur référencé correspond à un participant (personne morale signant les 2D-DOC) référencé qui s'appuie sur la solution d'un éditeur (fournisseur de la solution technique) référencé. L'émetteur de 2D-DOC doit désigner au moins un RC afin d'obtenir un certificat. L'ANTS ne contrôle pas les consommateurs de 2D-DOC.	

1.3.3.3 Porteur d'un certificat de personne physique

CERTIGNA IDENTITY CA	*Authentification/signature/chiffrement*
CERTIGNA IDENTITY PLUS CA	*Authentification/signature*
Un porteur de certificat ne peut être qu'une personne physique, acteur du secteur privé ou du secteur public. Cette personne utilise sa clé privée et le certificat correspondant dans le cadre de ses activités personnelles ou en relation avec l'entité identifiée dans le certificat et avec laquelle il a un lien contractuel, hiérarchique ou réglementaire.	

1.3.4 Utilisateurs de certificats

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

1.3.4.1 Certificat d'AC

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.	

1.3.4.2 Certificat de personne morale

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
FR03	*Cachet 2D-DOC*
Un utilisateur de certificat électronique de cachet peut être : - Un usager destinataire de données signées par un service applicatif de cachet et qui utilise le certificat électronique du cachet ainsi qu'un module de vérification de cachet afin d'authentifier l'origine des données transmises. - Un service applicatif destinataire de données provenant d'un autre service applicatif et qui utilise le certificat électronique de cachet et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises. - Un service applicatif qui signe des données électroniques.	

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
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.	

1.3.4.3 Certificat de personnes physique

CERTIGNA IDENTITY CA	*Authentification/signature/chiffrement*
CERTIGNA IDENTITY PLUS CA	*Authentification/signature*
Authentification et Signature	
Un utilisateur de certificat d'authentification et de signature peut être notamment : - Un service en ligne qui utilise un certificat et un dispositif de vérification d'authentification soit pour valider une demande d'accès faite par le porteur du certificat dans le cadre d'un contrôle d'accès, soit pour authentifier l'origine d'un message ou de données transmises par le porteur du certificat ; - Un service en ligne qui utilise un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le porteur du certificat ; - Un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification d'authentification afin d'en authentifier l'origine. - Un usager qui signe électroniquement un document ou un message ; - Un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le porteur du certificat sur ce message ou sur ces données.	
Authentification	
Un utilisateur de certificat d'authentification peut être notamment : - Un service en ligne qui utilise un certificat et un dispositif de vérification d'authentification soit pour valider une demande d'accès faite par le porteur du certificat dans le cadre d'un contrôle d'accès, soit pour authentifier l'origine d'un message ou de données transmises par le porteur du certificat ; - Un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification d'authentification afin d'en authentifier l'origine.	
Signature	
Un utilisateur de certificat de signature peut être notamment : - Un service en ligne qui utilise un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le porteur du certificat ; - Un usager qui signe électroniquement un document ou un message ; - Un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le porteur du certificat sur ce message ou sur ces données.	
Chiffrement	
Un utilisateur de certificat de chiffrement peut être notamment : - Un service en ligne qui utilise un dispositif de chiffrement pour chiffrer des données ou un message à destination du Porteur du certificat ; - Une personne qui émet un message chiffré à l'intention du Porteur du certificat électronique.	

1.3.5 Autres participants

1.3.5.1 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, Porteurs 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 ou Porteurs, et respecter les parties de la PC et de la présente DPC lui incombant.

1.3.5.2 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 ou Porteurs 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 ou Porteurs, et respecter les parties de la PC et de la présente 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 ou Porteur.

1.3.5.3 Autorité compétente nationale

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
SERVICES CA	*Authentification web*
TS 119 495 DSP2	
Conformément à la directive DSP2 et à la directive (UE) 2015/2366, l'Autorité Compétente Nationale (ACN) responsable des services de paiement approuve ou refuse l'autorisation des prestataires de services de paiement dans leur propre pays. Si l'autorisation est accordée, l'ACN inscrit le Prestataire de Services de Paiement (PSP) correspondant dans le registre public national, ainsi qu'un numéro d'identification, qui peut être, mais n'est pas nécessairement, un numéro d'autorisation. Sous réserve de l'approbation de l'ACN, le PSP peut exercer le droit d'établir et de fournir librement des services dans d'autres États membres. Ceci s'appelle le passeport. Les informations sur le passeport sont publiées dans le registre public du pays d'origine du PSP ou du registre DSP2 de l'Autorité Bancaire Européenne. Les certificats délivrés conformément aux exigences énoncées dans le présent document ne comportent aucune caractéristique en matière de passeport.	

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

RGS ***
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.
RGS **
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 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

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
FR03	*Cachet 2D-DOC*
Cachet pour la signature de mails et de documents	
Les usages sont la signature électronique de données et la vérification de signatures électroniques. Ces données peuvent être, par exemple, un accusé de réception suite à la transmission d'informations par un usager à un service applicatif, une réponse automatique à une demande formulée par un usager, les données d'un code 2D par exemple de type Datamatrix, un mail, un document, ou encore une archive.	
Cachet pour la signature de code	
Les usages sont la signature électronique de code d'application et la vérification de signatures électroniques.	
Cachet pour la signature de jetons d'horodatage	
Les usages sont la signature électronique de jetons d'horodatage et la vérification de signatures électroniques.	

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
Authentification de type serveur et/ou client TLS/SSL	
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).	

1.4.1.3 Certificat de personne physique

CERTIGNA IDENTITY CA	*Authentification/signature/chiffrement*
CERTIGNA IDENTITY PLUS CA	*Authentification/signature*
Authentification	
L'authentification des Porteurs auprès de serveurs distants ou auprès d'autres personnes. Il peut s'agir d'authentification dans le cadre d'un contrôle d'accès à un serveur ou une application, ou de l'authentification de l'origine de données dans le cadre de la messagerie électronique.	
Signature	
La signature électronique de données. Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.	
Authentification et Signature	
L'ensemble des usages identifiés ci-dessus pour les usages séparés d'authentification et de signature.	
Chiffrement	
- Déchiffrement : à l'aide de sa clé privée, un Porteur déchiffre les données qui lui ont été transmises dans le cadre d'échanges dématérialisés, chiffrées à partir de sa clé publique ; - Chiffrement : à l'aide de la publique du destinataire, une personne chiffre des données.	

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, les Porteurs et les utilisateurs de certificats. A cette fin, elle publie à destination des RC, des Porteurs, 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, de la modification et de la validation de la PC et de la DPC. Il statue sur toute modification nécessaire à apporter à la PC à échéance régulière.

1.5.2 Point de contact

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

Contact mail : contact@certigna.fr
Téléphone : 0 806 115 115 (Service gratuit)

1.5.3 Entité déterminant la conformité de la DPC avec la PC

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

1.5.4 Procédures d'approbation de la conformité de la DPC

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

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

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

1.6 Définitions et acronymes

1.6.1 Définitions

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

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

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

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification.

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

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

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

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

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

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

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

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

Dispositif de protection des éléments secrets - Désigne un dispositif de stockage des éléments secrets remis au porteur ou 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.

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.

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.

Norme Technique Réglementaire (RTS) - Norme Technique Règlementaire pour l'authentification forte du client PSD2 et des normes ouvertes de communication communes et sécurisées.

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 porteurs et les utilisateurs de certificats.

Porteur de certificat – Personne identifiée dans le certificat de personne physique et qui est la détentrice de la clé privée correspondant à la clé publique.

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 porteurs et utilisateurs de ces certificats.

Prestataire de service de paiement (PSP) - Prestataire autorisé par l'Autorité nationale compétente (ANC) à assurer un ou plusieurs des rôles suivants :
- Gestion de comptes (PSP_AS) ;
- Initiation de paiement (PSP_PI) ;
- Informations de comptes (PSP_AI) ;
- Délivrance d'instruments de paiement par carte (PSP_IC).

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.

Registre de l'Autorité Bancaire Européenne DSP2 - Registre des établissements de paiement et des établissements de monnaie électronique mis au point, exploité et tenu à jour par l'ABE en vertu de l'article 15 de la directive (UE) 2015/2366.

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).

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

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

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
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
CGVU	Conditions Générales de Vente et d'Utilisation
CNIL	Commission Nationale de l'Informatique et des Libertés
CSR	Certificate Signature Request
DSP2	Directive européenne sur les services de Paiement 2
DN	Distinguished Name
DNS	Domain Name System
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
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
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
RTS	Norme technique règlementaire pour le DSP2
SCT	Signed Certificate Timestamp
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

2 RESPONSABILITE CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS

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, des Porteurs et des utilisateurs de certificats :

- La PC ;
- La 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 ou Porteur 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 de la documentation

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

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

2.2.2 Publication de la DPC

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

2.2.3 Publication des certificats d'AC

Les RC, les Porteurs et les utilisateurs de certificat peuvent accéder aux certificats d'AC qui sont à l'adresse suivante https://www.certigna.com/autorite-crl ou directement via les adresses listées dans le tableau suivant. 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.

CERTIGNA ROOT CA	
Certificat d'AC	http://autorite.certigna.fr/certignarootca.der http://autorite.dhimyotis.com/certignarootca.der
CERTIGNA ENTITY CA	
Certificat d'AC	http://autorite.certigna.fr/entityca_rootca.der http://autorite.dhimyotis.com/entityca_rootca.der
CERTIGNA ENTITY CODE SIGNING CA	
Certificat d'AC	http://autorite.certigna.fr/entitycsca_rootca.der http://autorite.dhimyotis.com/entitycsca_rootca.der
FR03	
Certificat d'AC	http://autorite.certigna.fr/2ddoc.der http://autorite.dhimyotis.com/2ddoc.der
CERTIGNA SERVICES CA	
Certificat d'AC	http://autorite.certigna.fr/servicesca_rootca.der http://autorite.dhimyotis.com/servicesca_rootca.der
CERTIGNA WILD CA	
Certificat d'AC	http://autorite.certigna.fr/wildca_rootca.der http://autorite.dhimyotis.com/wildca_rootca.der
CERTIGNA IDENTITY CA	
Certificat d'AC	http://autorite.certigna.fr/identca_rootca.der http://autorite.dhimyotis.com/identca_rootca.der
CERTIGNA IDENTITY PLUS CA	
Certificat d'AC	http://autorite.certigna.fr/identityplusca_rootca.der http://autorite.dhimyotis.com/identityplusca_rootca.der

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 SERVICES CA	
EN 319 411-1 OVCP	
Test certificat valide Test certificat expire Test certificat révoqué	https://valid.servicesca.certigna.com https://expired.servicesca.certigna.com https://revoked.servicesca.certigna.com
EN 319 411-2 QCP-w	
Test certificat valide Test certificat expire Test certificat révoqué	https://valid.ev-servicesca.certigna.com https://expired.ev-servicesca.certigna.com https://revoked.ev-servicesca.certigna.com

TS 119 495 DSP2	
Test certificat valide Test certificat expire Test certificat révoqué	https://valid.psd2-servicesca.certigna.com https://expired. psd2-servicesca.certigna.com https://revoked. psd2-servicesca.certigna.com
CERTIGNA WILD CA	
EN 319 411-1 OVCP	
Test certificat valide Test certificat expire Test certificat révoqué	https://valid.wildca.certigna.com https://expired.wildca.certigna.com https://revoked.wildca.certigna.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 ROOT CA et AC intermédiaires	
LAR	http://crl.certigna.fr/certignarootca.crl http://crl.dhimyotis.com/certignarootca.crl

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 ENTITY CA	
LCR	http://crl.certigna.fr/entityca.crl http://crl.dhimyotis.com/entityca.crl
CERTIGNA ENTITY CODE SIGNING CA	
LCR	http://crl.certigna.fr/entitycsca.crl http://crl.dhimyotis.com/entitycsca.crl
FR03	
LCR	http://crl.certigna.fr/2ddoc.crl http://crl.dhimyotis.com/2ddoc.crl
CERTIGNA SERVICES CA	
LCR	http://crl.certigna.fr/servicesca.crl http://crl.dhimyotis.com/servicesca.crl
CERTIGNA WILD CA	
LCR	http://crl.certigna.fr/wildca.crl http://crl.dhimyotis.com/wildca.crl
CERTIGNA IDENTITY CA	
LCR	http://crl.certigna.fr/identca.crl http://crl.dhimyotis.com/identca.crl
CERTIGNA IDENTITY PLUS CA	
LCR	http://crl.certigna.fr/identityplusca.crl http://crl.dhimyotis.com/identityplusca.crl

2.3 Délais et fréquences de publication

2.3.1 Publication de la documentation

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

2.3.2 Publication des certificats d'AC

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

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

2.5 Signaler un certificat malveillant ou dangereux

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

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 service applicatif, du serveur ou du Porteur 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 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

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

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. Par défaut, le format du « serialNumber » est défini avec un numéro aléatoire.

3.1.5.1 Certificat d'AC

CERTIGNA ROOT CA & AC intermédiaires	*AC racine & intermédiaires*
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

FR03	*Cachet 2D-DOC*
L'ANTS est garante de l'unicité des noms des AC qu'elle référence dans le cadre de la norme 2D-DOC. La combinaison de l'identité de l'AC (4 caractères) et de l'identifiant du certificat (4 caractères) identifie de manière univoque les cachets serveurs émis.	

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
La combinaison du pays, de l'entité et de l'identité du service de création de cachet identifie de manière univoque le titulaire du certificat. Le champ « serialNumber » est également utilisé pour assurer l'unicité du DN. Durant toute la durée de vie de l'AC, le nom du service de création de cachet rattaché à une entité ne peut être attribué à une autre entité. L'attribut « serialNumber » 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 : - "T" pour « Cachet de jetons d'horodatage » ; - "TT" pour « Cachet de jetons d'horodatage » sur support physique ; - "S" pour « Cachet de mails et de documents » ; - "ST" pour « Cachet de mails et de documents » sur support physique ; - "C" pour « Cachet de code » ; - "CT" pour « Cachet de code » sur support physique.	

SERVICES CA	*Authentification web*
CERTIGNA WILD CA	*Authentification web*
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 » uniquement ; - "S" pour « Authentification de serveur » uniquement.	
EN 319 411-2 QCP-w	
L'attribut « serialNumber » est constitué du numéro d'immatriculation/d'enregistrement de l'entité.	

3.1.5.3 Certificat de personne physique

CERTIGNA IDENTITY CA	*Authentification/signature/chiffrement*
CERTIGNA IDENTITY PLUS CA	*Authentification/signature*
La combinaison du pays, du nom et de l'adresse e-mail du Porteur de certificat identifie de manière univoque le titulaire du certificat. L'attribut « *serialNumber* », valeur unique attribuée à chaque certificat émis par l'AC et présente dans le DN, assure également l'unicité du DN. Ce champ est constitué à partir d'un numéro aléatoire unique géré par l'AC précédé d'une ou plusieurs lettres indiquant le(s) usage(s) du certificat : - "I" pour « Authentification » et « Signature » ; - "A" pour "Authentification" uniquement ; - "S" pour "Signature" uniquement ; - "C" pour "Chiffrement" uniquement.	

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 ou d'un Porteur 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 ou du Porteur est vérifiée au travers de l'envoi de plusieurs emails qui permettent au RC ou Porteur 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 ou le Porteur et les cosignataires. La demande peut également être communiquée à l'AE ou l'AED au format électronique sous les conditions suivantes :

EN 319 411-1 NCP+ EN 319 411-2 QCP-n EN 319 411-2 QCP-n-qscd EN 319 411-2 QCP-l EN 319 411-2 QCP-l-qscd EN 319 411-2 QCP-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.
RGS ***
Au format électronique si signée à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau RGS **. La signature et le certificat associé doivent être valides lors de l'enregistrement par l'AE.
RGS **
Au format électronique si signée à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau RGS **. La signature et le certificat associé doivent être valides lors de l'enregistrement par l'AE.
EN 319 411-1 LCP 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 ou le Porteur avant de certifier la clé publique. Pour cela, l'AE, le RC ou le Porteur 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.

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
FR03	*Cachet 2D-DOC*
EN 319411-2 QCP-l-qscd RGS **	
Des justificatifs attestant que le dispositif est bien conforme aux exigences du chapitre 11 (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) doivent être fournis lors de la demande par le RC permettant d'attester de la détention du dispositif par le RC. L'AC 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 consigne les caractéristiques du dispositif, qu'il soit ou non élaboré par l'AC et contrôle mensuellement jusqu'au terme de la période de validité du certificat de l'entité, le maintien du statut de certification du dispositif. En cas de perte de la certification du dispositif, l'AC demandera au RC les preuves attestant que la bi-clé est stockée dans un dispositif répondant aux exigences du chapitre 11. Le RC s'engage à fournir ces preuves (Ex : Facture d'achat d'un nouveau dispositif qualifié QSealCD, 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 15 jours suivants la demande. Dans le cas où aucune preuve ne serait fournie 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 PC, l'AC se donne le droit de révoquer le certificat.	
EN 319411-2 QCP-l-qscd	
Dans le cas où le dispositif est géré par un Prestataire de Service de Confiance autre que CERTIGNA et l'entité sujet du certificat, le RC devra fournir lors de la demande, les justificatifs (Ex : Attestation de qualification en tant qu'Opérateur de certification, attestation de qualification en tant que PSCE pour le niveau QCP-l-qscd et accord contractuel signée associé entre l'entité désignée dans le certificat et ce prestataire, etc.) attestant que ce prestataire est en capacité de répondre aux exigences de la PC et notamment du chapitre 11.	

3.2.2 Authentification de l'organisation

3.2.2.1 Identité

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.

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.

3.2.2.1.4 Vérification des moyens de communication de l'entité

Lors de la demande de certificat, l'adresse email du demandeur est contrôlée via l'envoi d'un lien d'activation.

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
EN 319 411-2 QCP-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.	

3.2.2.1.5 Vérification du numéro d'autorisation DSP2

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
SERVICES CA	*Authentification web*
TS 119 495 DSP2	
Pour les certificats DSP2, l'identification du PSP par l'opérateur d'AE est réalisé également à l'aide du numéro d'autorisation DSP2 du PSP disponible dans le registre de l'ACN. Dans le cas où aucun numéro d'autorisation DSP2 n'est disponible, une autre forme du numéro d'enregistrement reconnu par l'ACN peut être utilisée à la place du numéro d'autorisation DSP2. Si nécessaire, pour s'assurer de l'unicité, le numéro d'autorisation ou d'enregistrement peut contenir un préfixe incluant le type d'institution. Les informations relatives au PSP et à l'ACN à positionner dans le certificat sont vérifiées par l'AE en contrôlant les informations officielles publiées sur l'un des registres suivants : - Le registre de l'ACN national en lien avec le PSP. A titre d'exemple, en France, l'ACN qui est l'APCR met à disposition un Registre des Agents Financiers (REGAFI) permettant de vérifier ces informations notamment à l'adresse suivante : https://www.regafi.fr ; - Le registre de l'ABE, nommé « Payment Institutions Register » accessible à l'adresse suivante https://euclid.eba.europa.eu/register/pir/disclaimer.	

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.

3.2.2.3 Vérification du pays

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
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

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
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.	

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

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
L'AC confirme le contrôle du demandeur sur le FQDN en envoyant une valeur aléatoire par mail, puis en recevant une réponse de confirmation en utilisant la valeur aléatoire. La valeur aléatoire est envoyée par CERTIGNA à l'une des adresses e-mail identifiée comme contact pour le domaine sur le site du registraire. Chaque e-mail peut confirmer le contrôle de plusieurs noms de domaine. L'AC pourra envoyer à l'e-mail identifié dans cette section à plusieurs destinataires à condition que chaque destinataire soit identifié par le registraire de nom de domaine comme représentant le registrant de nom de domaine pour chaque FQDN vérifié à l'aide de l'email. La valeur aléatoire est unique pour chaque FQDN et reste valide jusqu'à 30 jours après sa création. L'AC pourra renvoyer le mail dans son intégralité, y compris la réutilisation de la valeur aléatoire, à condition que le contenu et les destinataires de la communication restent inchangés. Remarque : Une fois que le FQDN a été validé à l'aide de cette méthode, l'AC pourra également émettre des certificats pour d'autres FQDN qui se terminent par tous les labels du FQDN validé. Cette méthode convient à la validation des noms de domaine Wildcard.	

3.2.2.4.3 Contact téléphonique avec le contact du domaine

Sans objet.

3.2.2.4.4 Email construit pour le contact du domaine

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

La valeur aléatoire est unique pour chaque FQDN et reste valide jusqu'à 30 jours après sa création. Le mail pourra être renvoyé dans son intégralité, intégrant la réutilisation de la valeur aléatoire, 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.

3.2.2.4.5 Document d'autorisation du domaine

Sans objet.

3.2.2.4.6 Changement apporté au site web

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*

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

La valeur aléatoire est unique pour chaque FQDN et reste valide jusqu'à 30 jours après sa création. Le mail peut être renvoyé mais un fichier avec une nouvelle valeur aléatoire sera fourni pour chaque FQDN, rendant invalide le fichier fourni précédemment.

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

3.2.2.4.7 Changement DNS

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*

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

La valeur aléatoire est unique pour chaque FQDN et reste valide jusqu'à 30 jours après sa création. Le mail peut être renvoyé mais un enregistrement avec une nouvelle valeur aléatoire sera fourni pour chaque FQDN, rendant invalide l'enregistrement fourni précédemment. Si plusieurs FQDNs sont concernés par une même demande, un seul mail est envoyé au demandeur contenant les enregistrements associés. Le demandeur doit ajouter tous les enregistrements dans la configuration DNS du site web afin de permettre le contrôle de chaque FQDN.

3.2.2.4.8 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

Sans objet.

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.

3.2.2.5 Authentification pour une adresse IP

Sans objet.

3.2.2.6 Validation d'un domaine Wildcard

WILD 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

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
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

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
EN 319 411-2 QCP-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

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
EN 319 411-2 QCP-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

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
EN 319 411-2 QCP-w	
Les dossiers de demandes de certificats qualifiés (QCP-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 (QCP-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

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
Conformément à la RFC 6844, des contrôles sont réalisés par l'autorité d'enregistrement pour chaque nom de domaine présent dans l'extension « subjectAltName » du certificat à émettre et dont l'option « DNS CAA » est activée dans l'enregistrement DNS associé. 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 » ou « issuewild » 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.	

3.2.3 L'authentification de l'identité d'un individu

La vérification de l'identité d'un individu cible :
- Un Responsable de Certificat de personne morale ;
- Un Porteur de certificat de personne physique ;
- Le représentant légal de l'organisation rattachée au certificat, le cas échéant ;
- Le mandataire de certification associée à l'organisation, le cas échéant.

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'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

CERTIGNA ROOT CA et AC intermédiaires	*AC racine et intermédiaires*
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

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
FR03	*Cachet 2D-DOC*
SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
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

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
FR03	*Cachet 2D-DOC*
SERVICES CA	*Authentification web*
WILD CA	*Authentification web*

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

TS 119 495 DSP2
Pour un certificat DSP2, un document doit être fourni listant les caractéristiques du PSP et son référencement dans le registre de l'ACN ou de l'ABE le cas échéant.
EN 319 411-2 QCP-l EN 319 411-2 QCP-l-qscd EN 319 411-1 NCP+
L'authentification du RC par l'AE est réalisée via l'un des moyens suivants : - Authentification en face à face physique avec le porteur 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 QCP-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 : o Une carte bancaire de crédit avec une date d'expiration et qui n'est pas expirée ; o Une carte bancaire de retrait d'un établissement bancaire règlementé contenant une date d'expiration et qui n'est pas expirée ; o Un relevé de compte bancaire d'un établissement bancaire règlementé datant de moins de 6 mois ; o Une facture originale récente (facture télécom pour une ligne fixe ou une facture EDF/GDF) désignant le nom et l'adresse fixe du RC ; o Une copie d'une quittance de loyer datant de moins de 6 mois ; o Une facture de taxe locale pour l'année en cours (taxe foncière, taxe d'habitation) ; o Un extrait d'acte de naissance.
EN 319 411-1 LCP 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 Porteur par l'AE est réalisée lors d'un face-à-face physique ou sous forme dématérialisée à condition que la demande soit signée par le Porteur à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau ** que la signature soit vérifiée et valide au moment de l'enregistrement.
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 Certificat de personne physique

3.2.3.3.1 Enregistrement d'un Porteur [Particulier]

CERTIGNA IDENTITY CA	*Authentification/signature/chiffrement*
CERTIGNA IDENTITY PLUS CA	*Authentification/signature*

Le dossier de demande de certificat est à compléter depuis les formulaires disponibles sur le site de CERTIGNA ou de l'AED. Une fois complétés, les éléments suivants sont transmis à l'AE :

Formulaire de demande du certificat	
Objet	Désignation du futur Porteur habilité et de ses coordonnées
	Désignation des CGVU applicables (Incluant l'obligation du Porteur sur l'utilisation d'un dispositif conforme aux exigences du chapitre 11)
Date	Signature du formulaire de moins de 3 mois
Signature	Signature du futur Porteur pour accepter le rôle de Porteur et les CGVU

Pièce d'identité officielle du Porteur	
Objet	La photocopie d'un document officiel d'identité en cours de validité du futur Porteur comportant une photographie d'identité. *Exemple : carte nationale d'identité, passeport ou carte de séjour*
Date	Pièce valide au moment de l'enregistrement

QCP-n
QCP-n-qscd

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

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

RGS ***

L'authentification du Porteur par l'AE est réalisée lors d'un face-à-face physique.

RGS **

L'authentification du Porteur par l'AE est réalisée lors d'un face-à-face physique ou sous forme dématérialisée à condition que la demande soit signée par le Porteur à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau RGS **, que la signature soit vérifiée et valide au moment de l'enregistrement.

RGS *

L'authentification du futur Porteur 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).

3.2.3.3.2 Enregistrement d'un Porteur [Entreprise][Administration]

CERTIGNA IDENTITY CA	*Authentification/signature/chiffrement*
CERTIGNA IDENTITY PLUS CA	*Authentification/signature*

Le dossier de demande de certificat est à compléter depuis les formulaires disponibles sur le site de CERTIGNA ou de l'AED. Une fois complétés, les éléments suivants sont 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 Porteur habilité et de ses coordonnées
	Désignation de l'identité de l'entité à laquelle est rattaché le Porteur
	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 Porteur Signature du futur Porteur pour accepter le rôle de Porteur et les CGVU

Pièce d'identité officielle du Porteur	
Objet	La photocopie d'un élément d'identification du Porteur 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

QCP-n QCP-n-qscd
L'authentification du Porteur par l'AE est réalisée via l'un des moyens suivants : - Authentification en face-à-face physique avec le porteur avec présentation d'une pièce d'identité valide lors du face-à-face (Carte nationale d'identité, Passeport ou Carte de séjour). - Authentification du porteur à distance à l'aide d'un moyen d'identification électronique qualifié au niveau substantiel ou élevé au sens du règlement eIDAS. - Authentification du porteur 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 porteur à l'aide d'un certificat de signature électronique qualifié au sens du Règlement eIDAS.
RGS ***
L'authentification du porteur par l'AE ou le MC est réalisée lors d'un face-à-face physique.
RGS **
L'authentification du Porteur par l'AE ou le MC est réalisée lors d'un face-à-face physique ou sous forme dématérialisée à condition que la demande soit signée par le Porteur à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau **, que la signature soit vérifiée et valide au moment de l'enregistrement, et que le certificat sur lequel repose cette signature électronique soit un certificat qualifié au titre du règlement eIDAS.
RGS *
L'authentification du futur Porteur 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).

3.2.3.4 Enregistrement d'un Mandataire de Certification

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
FR03	*Cachet 2D-DOC*
SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
CERTIGNA IDENTITY CA	*Authentification/signature/chiffrement*
CERTIGNA IDENTITY PLUS CA	*Authentification/signature*

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 QCP-l EN 319 411-2 QCP-l-qscd EN 319 411-2 QCP-w
L'authentification du MC par l'AE est réalisée lors d'un face-à-face physique ou sous forme dématérialisée à condition que la demande soit signée par le Porteur à l'aide d'une signature électronique vérifiée et valide au moment de l'enregistrement, et que le certificat sur lequel repose cette signature électronique soit un certificat qualifié au titre du règlement eIDAS.
RGS **
L'authentification du MC par l'AE est réalisée lors d'un face-à-face physique ou sous forme dématérialisée à condition que la demande soit signée par le Porteur à l'aide d'un procédé de signature électronique conforme au minimum aux exigences du niveau RGS ** que la signature soit vérifiée et valide au moment de l'enregistrement.
EN 319 411-1 LCP 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 du RC ou Porteur

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 ou Porteur (directement par l'AE ou par le MC).

3.2.6 Critères d'interopérabilité ou de certification

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

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
FR03	*Cachet 2D-DOC*
SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
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.	
EN 319 411-1 OVCP EN 319 411-2 QCP-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.	

3.3.1.3 Certificat de personne physique

CERTIGNA IDENTITY CA	*Authentification/signature/chiffrement*
CERTIGNA IDENTITY PLUS CA	*Authentification/signature*
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 Porteur, et l'entité le cas échéant, selon la même procédure que pour l'enregistrement initial.	

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 ou le Porteur, 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.fr en sélectionnant le certificat à révoquer.

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 Porteur concerné ou le nom du service ou serveur concerné ;
- L'adresse e-mail du Porteur le cas échéant ;
- La raison de la révocation.

Si le RC ou Porteur 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.

3.4.2.2 Demande émanant d'une ACN

Une ACN authentifiée est autorisée à demander la révocation du certificat d'un PSP présent dans son registre. Cette demande doit être formulée par mail à security@certigna.com en joignant une demande de révocation en Français ou en Anglais. Cette demande de révocation doit être signée électroniquement à l'aide d'un procédé de signature ou de cachet avancé reposant sur un certificat qualifié au sens du règlement eIDAS et dont l'organisation désignée en tant que sujet du certificat est l'ACN.

La demande de révocation de certificat devra préciser les informations suivantes :
- Identifiant de l'ACN ;
- Coordonnées du demandeur ;
- Identifiant du PSP objet de la demande de révocation ;
- Raison pour laquelle le certificat doit être révoqué :
    - L'autorisation du PSP a été révoquée ;
    - Un ou plusieurs rôles du PSP figurant dans son certificat a été révoqué.

Sur demande de l'ACN et confirmation par CERTIGNA, l'AC pourra mettre à disposition un certificat conformément à ses processus de délivrance et permettant d'authentifier les demandes de l'ACN.

L'un des cas suivants peut conduire l'AC à rejeter la demande de révocation réceptionnée ou à demander des compléments d'informations :
- Si l'authenticité de la demande n'est pas vérifiable ;
- Si la demande n'indique pas clairement la raison de révocation du certificat ;
- Si la raison de révocation du certificat n'est pas de la responsabilité de l'ACN demandeuse.

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 ou Porteur.

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
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 ou Porteur à partir des éléments fournis par son entité le cas échéant, soit par son entité et signé par le futur RC ou Porteur. 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 ou Porteur, 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 ou Porteurs. Le dossier de demande de certificat doit contenir les éléments décrits au chapitre 3.2.3. L'adresse mail du RC ou Porteur, 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.

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 service, serveur ou Porteur ;
- Validation de l'identité de l'entité ;
- Validation de l'identité des signataires de la demande (RC ou Porteur, représentant légal ou MC) ;
- Validation de l'autorisation d'émettre un certificat pour ce service, serveur ou Porteur ;
- Validation du contrôle du domaine pour un serveur ;
- Validation du dossier et de la cohérence des justificatifs présentés ;
- Assurance que le futur RC ou Porteur a pris connaissance des modalités applicables pour l'utilisation du certificat.

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 ou Porteur a pris connaissance des CGVU, en complément de leur diffusion opérée par l'AC ;
- Vérifier l'identité du RC ou du Porteur 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 ou Porteur et du représentant légal est approuvée si les pièces justificatives fournies sont valides à la date de réception.

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
SERVICES CA	*Authentification web*
TS 119 495 DSP2	
L'AC vérifie les informations du PSP et de l'ACN associée (identifiant du PSP et ses rôles, identifiant et pays de l'ACN) grâce aux informations fournies officiellement par l'ACN sur son registre ou sur le registre de l'ABE. Dans le cas où l'ACN associée préconise des validations spécifiques à opérer, ces dernières seront réalisées par l'AC le cas échéant.	

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
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 6844, 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.

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 ou Porteur, 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 ou Porteur pour effectuer l'acceptation du certificat et la récupération de données d'activation.

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*

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

En complément, la vérification du propriétaire de nom de domaine réalisée par l'AE conduira, dans tous les cas, au rejet de la demande puisqu'il est impossible d'identifier le propriétaire d'un nom de domaine de type « *.tld ». Les demandes avec un TLD invalide ou sans domaine (Ex : *.co.uk) seront systématiquement rejetées.

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

Lorsqu'un gTLD est délégué via son inclusion dans la base de données « Root zone » de l'IANA, le nom interne devient un nom de domaine, et à ce moment-là, un certificat avec

ce gTLD, qui peut avoir respecté ces exigences au moment de l'émission, sera en violation avec ces exigences, à moins que l'AC ait vérifié les droits du demandeur sur le nom de domaine. Les dispositions ci-dessous visent à empêcher une telle violation.

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

EN 319 411-2 QCP-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 ou physique

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

4.3.1.1 Certificat d'AC

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 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 Certificat de personne morale ou physique

Suite à la validation par l'AE, l'AC déclenche le processus de génération du certificat destiné au RC ou au Porteur. Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres 5 et 6 ci-dessous, notamment la séparation des rôles de confiance. (Cf. chapitre 5.2).

Les opérations de validation de demande sur l'AE et de génération de certificat sur l'AC sont détaillées dans la « Procédure opérationnelle de demande de certificat ».

4.3.2 Notification par l'AC de la délivrance du certificat

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 ou physique

Le certificat complet et exact est mis à disposition de son RC ou Porteur depuis l'espace client ou sur le dispositif remis par l'AC le cas échéant. Le RC ou Porteur 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 ou le Porteur, 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 ou le Porteur choisit explicitement d'accepter ou non le certificat et la notification d'acceptation ou de refus est transmise automatiquement à l'AC. En cas de détection d'incohérence entre les informations figurant dans l'accord contractuel et le contenu du certificat, le RC ou le Porteur 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 ou physique

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

FR03	*Cachet 2D-DOC*
Tous les certificats émis par l'AC FR03 sont publiés dans un annuaire après l'acceptation du certificat par le RC. Le RC est informé de cette publication.	

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

L'AE est informée de la génération du certificat par l'AC 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, le RC ou le Porteur 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 ou du Porteur 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, ou le cas échéant jusqu'à l'acceptation et la signature par le RC ou le Porteur de nouvelles conditions générales émises et portées à sa connaissance par l'AC via le site https://www.certigna.com. Les nouvelles conditions signées doivent être transmises par le RC ou le Porteur à l'AC pour être applicables.

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

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats 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 ou le Porteur 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, des Porteurs, des services 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 ou du Porteur (pas d'existence de processus automatisé). L'entité, via son MC le cas échéant, peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un Porteur ou 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, de Porteur, de service 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 ou physique

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat :

- Le RC ou le Porteur, 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 représentant légal de l'entité à laquelle le service, le serveur ou le Porteur appartient le cas échéant, informe l'AC 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 correspondant à la clé publique du certificat est suspectée de compromission, est compromise, est perdue ou volée (ou éventuellement les données d'activation associées à la clé privée),

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
- 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.	

L'AC révoquera un certificat sous 5 jours dans une ou plusieurs des situations suivantes :

- Le certificat n'est plus conforme aux exigences des chapitres 6.1.5 et 6.1.6 de cette PC ;
- L'AC obtient la preuve que l'usage du certificat est détourné ;
- L'AC est informée que le RC ou le Porteur n'a pas respecté toute ou partie des dispositions du contrat ou a violé une ou plusieurs de ses obligations en vertu des CGVU ;
- Les informations du porteur, du service de cachet ou 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 porteur, du service de cachet ou du serveur), ceci avant l'expiration normale du certificat ;
- L'AC est informée que le certificat n'a pas été émis en conformité avec les exigences et pratiques formulées dans cette DPC ou la PC associée ;
- L'AC détecte ou est informée que les informations apparaissant dans le certificat sont inexactes ou trompeuses ;
- 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 ou la DPC correspondante ;
- 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 (telle que la clé vulnérable de Debian, cf. http://wiki.debian.org/SSLkeys),
- Le RC ou le Porteur, l'entité, le cas échéant le MC ou l'opérateur d'AED, n'a pas respecté ses obligations découlant de la PC ou de la DPC ;
- L'AC 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.
- L'arrêt définitif du service ou du serveur ou la cessation d'activité de l'entité du RC ;
- Le départ de la société du Porteur ou la cessation d'activité de l'entité de rattachement du Porteur ;
- 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, …).

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
- L'AC est informée de toute circonstance indiquant que l'utilisation d'un nom de domaine dans le certificat n'est plus autorisée légalement (Ex : un tribunal ou un arbitre a révoqué le droit d'un titulaire de nom de domaine d'utiliser le nom de domaine, une licence ou un accord de services entre le titulaire et le demandeur est terminée, ou le titulaire n'a pas pu renouveler le nom de domaine).	

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
SERVICES CA	*Authentification web*
TS 119 495 DSP2	
- Les informations figurant dans le registre public ont été modifiées de manière à influer considérablement sur la validité des attributs DSP2 du certificat ; - Le statut d'autorisation accordé par l'ACN a changé (par exemple, le PSP n'est plus autorisé).	

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

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 ou la DPC associée ;
- 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 ou physique

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

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
SERVICES CA	*Authentification web*
TS 119 495 DSP2	
- Une ACN authentifiée. Cf. chapitre 3.4.2.2	

Le RC ou le Porteur 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 ou Porteurs 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 ou physique

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 ou du Porteur ;
- L'adresse email du RC ou du Porteur ;
- La raison de la révocation.

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

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

L'AC ne publie pas dans la LCR les causes de révocation des certificats.

4.9.4 Délai accordé pour formuler la demande de révocation

Dès que le RC, le Porteur 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 ou physique

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.

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
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 1 heure ; - Par mois de 4 heures.

RGS **
La durée maximale d'indisponibilité de la fonction de gestion des révocations est : - Par interruption (panne ou maintenance) de 2 heures ; - Par mois de 8 heures.
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 service, de serveur ou de Porteur 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 LAR/LCR

La LAR est émise au minimum tous les ans. En outre, une nouvelle LAR est systématiquement et immédiatement publiée 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.

4.9.8 Délai maximum de publication d'une LAR/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.

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.

4.9.10 Exigences sur la vérification en ligne de la révocation

Le répondeur OCSP opéré par l'AC support la méthode http GET, telle que décrite dans la RFC 6960 et/ou la RFC 5019. En complément de la publication des LCR sur les sites en ligne, l'AC met à disposition un répondeur OCSP accessible aux adresses fournies dans le tableau suivant.

CERTIGNA ENTITY CA	
OCSP	http://entityca.ocsp.certigna.fr http://entityca.ocsp.dhimyotis.com
CERTIGNA ENTITY CODE SIGNING CA	
OCSP	http://entitycsca.ocsp.certigna.fr http://entitycsca.ocsp.dhimyotis.com
FR03	
OCSP	http://2ddoc.ocsp.certigna.fr http://2ddoc.ocsp.dhimyotis.com
CERTIGNA SERVICES CA	
OCSP	http://servicesca.ocsp.certigna.fr http://servicesca.ocsp.dhimyotis.com
CERTIGNA WILD CA	
OCSP	http://wildca.ocsp.certigna.fr http://wildca.ocsp.dhimyotis.com
CERTIGNA IDENTITY CA	
OCSP	http://identca.ocsp.certigna.fr http://identca.ocsp.dhimyotis.com
CERTIGNA IDENTITY PLUS CA	
OCSP	http://identityplusca.ocsp.certigna.fr http://identityplusca.ocsp.dhimyotis.com

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

Le répondeur OCSP supporté la méthode « http GET », telle que décrite dans la RFC 6960 et/ou la RFC 5019.

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

4.9.11 Autres moyens disponibles d'information sur les révocations

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
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, le RC ou le Porteur 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 ».

CERTIGNA IDENTITY PLUS CA	Authentification/signature
RGS ***	
En cas de compromission de sa clé privée ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le Porteur s'oblige à interrompre immédiatement et définitivement l'usage du certificat et de la clé privée qui lui est associée. Pour rappel, cet engagement est pris lors de l'acceptation des CGVU.	

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).

Les activités relatives au service de publication sont définies dans la « Procédure de gestion du service publication ».

4.10.2 Disponibilité de la fonction

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

RGS ***
La durée maximale d'indisponibilité de la fonction d'information de l'état des certificats est : - Par interruption (panne ou maintenance) de 2 heures ; - Par mois de 8 heures.
RGS **
La durée maximale d'indisponibilité de la fonction d'information de l'état des certificats est : - Par interruption (panne ou maintenance) de 4 heures ; - Par mois de 16 heures.
RGS *
La durée maximale d'indisponibilité de la fonction d'information de l'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 Porteur et l'AC

En cas de fin de relation contractuelle ou réglementaire entre l'AC et l'entité de rattachement du service, serveur ou Porteur avant la fin de validité du certificat, le certificat est révoqué.

4.12 Séquestre de clé et recouvrement

CERTIGNA ROOT CA et AC intermédiaire	*AC racine et intermédiaires*
CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
FR03	*Cachet 2D-DOC*
SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
CERTIGNA IDENTITY CA	Authentification/signature
CERTIGNA IDENTITY PLUS CA	Authentification/signature
Le séquestre des clés privées est interdit.	

CERTIGNA IDENTITY CA	*Chiffrement*
Chiffrement	
Les clés privées de chiffrement des Porteurs sont séquestrées.	

4.12.1 Politique et pratiques de séquestre de clé et de recouvrement

Le séquestre des clés privées est interdit hormis pour les clés de chiffrement.

4.12.1.1 Demande de séquestre

CERTIGNA IDENTITY CA	*Chiffrement*
Chiffrement	
Le séquestre du certificat et la bi-clé sont opérés automatiquement et pour une durée de dix (10) ans à partir de la date d'émission du certificat. Le porteur, peut demander, lors de la commande à faire évoluer la durée de rétention ou bien à ne pas bénéficier du séquestre.	

4.12.1.2 Traitement d'une demande de séquestre

CERTIGNA IDENTITY CA	*Chiffrement*
Chiffrement	
Le certificat de chiffrement et la clé privée associée font l'objet d'un séquestre permettant leur recouvrement en cas de perte. La durée du séquestre est de dix (10) ans à partir de la date d'émission du certificat sauf demande explicite du porteur lors de la commande du certificat. Chaque clé privée séquestrée est identifiée de manière unique et non équivoque par le numéro de série du certificat correspondant.	

4.12.1.3 Origine d'une demande de recouvrement

CERTIGNA IDENTITY CA	*Chiffrement*
Chiffrement	
Outre le Porteur et les entités autorisées par la loi à accéder aux clés privées séquestrées par une AC, seul le représentant légal de l'entité ou une personne explicitement désignée (nominativement ou par sa fonction) par le représentant légal de l'entité peut demander le recouvrement d'une clé privée d'un Porteur donné.	

4.12.2 Identification et validation d'une demande de recouvrement

CERTIGNA IDENTITY CA	*Chiffrement*
Chiffrement	
L'identité du demandeur d'un recouvrement doit être validée, sauf cas particulier des entités autorisées par la loi, par l'AE suivant les mêmes exigences que la validation initiale de l'identité d'un demandeur de certificat (cf. 3.2). La demande de recouvrement doit comporter au moins le motif du recouvrement de la clé privée et les informations permettant d'identifier la clé privée à recouvrer. L'AE s'assure que le demandeur est bien l'une des personnes autorisées à demander le recouvrement de la clé concernée.	

4.12.2.1 Traitement d'une demande de recouvrement

CERTIGNA IDENTITY CA	*Chiffrement*
Chiffrement	
Suite à l'identification et la validation de la demande de recouvrement, un opérateur d'AE procède à la remise de la clé privée au demandeur, avec une sécurité équivalente à la remise de la clé privée lors de la génération du certificat du porteur. Les pièces du dossier de recouvrement sont archivées par l'AE.	

4.12.2.2 Destruction des clés séquestrées

CERTIGNA IDENTITY CA	*Chiffrement*
Chiffrement	
Dès la fin de la période de conservation d'une clé séquestrée, tout exemplaire de cette clé détenue par l'AC est détruit de manière fiable.	

4.12.2.3 Disponibilité des fonctions liées au séquestre et au recouvrement

CERTIGNA IDENTITY CA	*Chiffrement*
Chiffrement	
La fonction de gestion des recouvrements est disponible aux heures ouvrées. Dans tous les cas, le délai maximum de traitement d'une demande de recouvrement est de 72 heures. Ce délai s'entend entre la réception de la demande de recouvrement authentifiée et la mise à disposition de la clé privée auprès du demandeur.	

4.12.3 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. Sa 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 ».

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 services, serveurs et Porteurs.
- **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.

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

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

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

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 ».

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 d'événements

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

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

Sans objet.

5.4.8 Evaluation des vulnérabilités

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

Les journaux sont analysés dans leur totalité à la fréquence d'au moins 1 fois 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 logiciels (exécutables) constitutifs de l'IGC ;
- Les fichiers de configuration des équipements informatiques ;
- Les journaux d'événement des différentes composantes de l'IGC ;
- La PC ;
- La DPC ;
- Les demandes de certificats électroniques ;
- Les dossiers d'enregistrement des MC ;
- Les dossiers d'enregistrement des opérateurs d'AED ;
- Les dossiers de demande de certificat, avec les justificatifs d'identité ;
- Les certificats émis ;
- Les demandes de révocation ;
- Les LCR émises ;
- Les réponses OCSP.

5.5.2 Période de conservation des archives

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

Les réponses OCSP produites sont archivées pendant au moins trois mois 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. Au-delà des 11 premières années d'exploitation de l'AC, une procédure manuelle d'effacement des archives est exécutée sur les différents centres de production.

5.5.3 Protection des archives

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

5.5.4 Procédure de sauvegarde des archives

Le procédé de « réplication » (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

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. L'exploitation d'un moniteur de supervision garantit une détection et une prise en compte en temps réel des incidents sur les deux sites de production.

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

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

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

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

- Informera tous les RC et Porteurs 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.

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, Porteurs, 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.

5.8.1.1 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 et Porteurs 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.

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

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

Le contact identifié sur le site de l'ANSSI (http://www.ssi.gouv.fr) est immédiatement informé en cas de cessation d'activité de l'AC.

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

6 MESURES DE 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.

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 pour authentifier son personnel et sécuriser ses services.

6.1.1.3 Génération des bi-clés de personne morale ou physique

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 ou si elle est associée à une clé privée connue comme vulnérable.

Le RC ou le Porteur 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 et se réserve le droit de refuser la demande de certificat s'il était avéré que ce dispositif ne réponde pas à ces exigences. Dans le cas où l'AC génère la bi-clé, la génération s'effectue dans un dispositif conforme aux exigences du chapitre 11.

6.1.2 Transmission de la clé privée à son propriétaire

Lorsque que l'AC génère la clé privée au nom du service, serveur ou Porteur, l'authentification du RC ou du Porteur par l'AE est réalisée préalablement à la remise de la bi-clé au format chiffré. La clé privée est transmise soit sous forme de téléchargement protégé par une donnée d'activation définie par le RC ou le Porteur, soit dans un dispositif conforme au chapitre 11 et envoyé par courrier sécurisé au RC ou Porteur, ou remis en face-à-face par un opérateur d'AE, un opérateur d'AED, ou un MC.

Si l'AC ou l'AE est informée que la clé privée destinée au RC ou au Porteur 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 service de cachet, du serveur web ou du Porteur, est transmise à l'AC par le RC ou le Porteur. 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 ou le Porteur 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 Type d'algorithme et 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,
- Taille modulus RSA (bits) : 4096

6.1.5.3 Certificat de personne morale ou physique

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
CERTIGNA IDENTITY CA	Authentification/signature
CERTIGNA IDENTITY PLUS CA	Authentification/signature
- Algorithme de hachage : SHA-256, - Taille modulus RSA (bits) : 2048	

FR03	*Cachet 2D-DOC*
- Algorithme de hachage : SHA-256, - Courbe ECC : NIST P-256	

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 ou physique

L'équipement de génération de bi-clés employé par le RC ou le Porteur 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

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 et Porteurs 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 ou le Porteur pour protéger la clé privée est conforme avec les exigences du chapitre 11. Dans le cas où l'AC fournit le dispositif au RC ou au Porteur, directement ou indirectement, l'AC s'assure que :

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

6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC est assuré par du personnel de confiance et via un outil mettant en œuvre le partage des secrets (systèmes où n exploitants parmi m doivent s'authentifier, avec n au moins égal à 2). La « Procédure de gestion des HSM » et la « Procédure de gestion des clés cryptographiques » décrivent les mesures mises en œuvre.

6.2.3 Séquestre de la clé privée

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

CERTIGNA ROOT CA et AC intermédiaire	*AC racine et intermédiaires*
CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
FR03	*Cachet 2D-DOC*
SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
CERTIGNA IDENTITY CA	Authentification/signature
CERTIGNA IDENTITY PLUS CA	Authentification/signature
Le séquestre des clés privées est interdit.	

CERTIGNA IDENTITY CA	*Chiffrement*
Chiffrement	
Les clés privées de chiffrement des Porteurs sont séquestrées.	

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 ou physique

CERTIGNA ROOT CA et AC intermédiaire	*AC racine et intermédiaires*
CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
FR03	*Cachet 2D-DOC*
SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
CERTIGNA IDENTITY CA	Authentification/signature
CERTIGNA IDENTITY PLUS CA	Authentification/signature
Les clés privées des services de cachet, serveur web ou Porteurs ne font pas l'objet de copies de secours.	

CERTIGNA IDENTITY CA	*Chiffrement*
Chiffrement	
Les clés privées des porteurs séquestrées font l'objet de copies de secours moyennant le respect des exigences de sécurité pour le séquestre des clés.	

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 ou physique

La clé privée du service de cachet, du serveur web ou du Porteur n'est en aucun cas archivée.

Pour une clé privée générée dans un module cryptographique, il est techniquement impossible d'effectuer une copie de cette clé hors HSM.

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.

6.2.6.2 Clé privée de personne morale ou physique

La clé privée du service de cachet, du serveur web ou du Porteur est générée sous la responsabilité de l'opérateur d'AE, d'AED, du MC ou du Porteur.

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 ou physique

La clé privée du service de cachet, du serveur web ou du Porteur 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 ou physique

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 ou physique

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

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 cette procédure. Les mesures mises en œuvre sont décrites dans la « Procédure de gestion des clés cryptographiques ».

6.2.10.2 Clé privée de personne morale ou physique

Le RC ou le Porteur 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 ou physique

Le niveau d'évaluation du dispositif utilisé par le RC ou Porteur 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

Pour l'IGC CERTIGNA, la durée de validité du certificat de l'AC Racine est de 20 ans, et celle des certificats intermédiaires d'AC est de 18 ans. La fin de validité d'un certificat d'AC est postérieure à la fin de vie des certificats qu'elle émet.

6.3.2.2 Bi-clé et certificat de personne morale ou physique

Certificat	OID	Durée de vie
CERTIGNA ENTITY CA		
Cachet mails et documents	1.2.250.1.177.2.6.1.1.1	1 à 3 ans maximum
Cachet mails et documents	1.2.250.1.177.2.6.1.4.1	1 à 3 ans maximum
Cachet mails et documents	1.2.250.1.177.2.6.1.42.1	1 à 3 ans maximum
Cachet mails et documents	1.2.250.1.177.2.6.1.41.1	1 à 3 ans maximum
Cachet mails et documents	1.2.250.1.177.2.6.1.7.1	1 à 3 ans maximum
Cachet mails et documents	1.2.250.1.177.2.6.1.8.1	1 à 3 ans maximum
Cachet mails et documents	1.2.250.1.177.2.6.1.9.1	1 à 3 ans maximum
Cachet jetons d'horodatage	1.2.250.1.177.2.6.1.3.1	1 à 5 ans maximum
Cachet jetons d'horodatage	1.2.250.1.177.2.6.1.6.1	1 à 5 ans maximum
CERTIGNA ENTITY CODE SIGNING CA		
Cachet de code	1.2.250.1.177.2.8.1.1.1	1 à 3 ans maximum
Cachet de code	1.2.250.1.177.2.8.1.2.1	1 à 3 ans maximum
FR03		
Cachet de 2D-DOC	1.2.250.1.177.2.2.1.1	1 à 3 ans maximum
CERTIGNA SERVICES CA		
Authentification serveur	1.2.250.1.177.2.5.1.1.1	1 à 3 ans maximum
Authentification client	1.2.250.1.177.2.5.1.2.1	1 à 3 ans maximum
Authentification client/serveur	1.2.250.1.177.2.5.1.3.1	1 à 3 ans maximum
Authentification client/serveur	1.2.250.1.177.2.5.1.4.1	1 à 3 ans maximum
CERTIGNA WILD CA		
Authentification client/serveur	1.2.250.1.177.2.7.1.1.1	1 à 3 ans maximum
Authentification wildcard	1.2.250.1.177.2.7.1.2.1	1 à 3 ans maximum
CERTIGNA IDENTITY CA		
Chiffrement	1.2.250.1.177.2.3.1.1.1	1 à 3 ans maximum
Chiffrement	1.2.250.1.177.2.3.1.3.1	1 à 5 ans maximum
Authentification & signature	1.2.250.1.177.2.3.1.2.1	1 à 3 ans maximum
Authentification & signature	1.2.250.1.177.2.3.1.4.1	1 à 5 ans maximum

CERTIGNA IDENTITY PLUS CA		
Authentification & signature	1.2.250.1.177.2.4.1.1.1	1 à 3 ans maximum
Authentification	1.2.250.1.177.2.4.1.2.1	1 à 3 ans maximum
Signature	1.2.250.1.177.2.4.1.3.1	1 à 3 ans maximum
Authentification & signature	1.2.250.1.177.2.4.1.4.1	1 à 5 ans maximum
Authentification	1.2.250.1.177.2.4.1.5.1	1 à 5 ans maximum
Signature	1.2.250.1.177.2.4.1.6.1	1 à 5 ans maximum
Authentification & signature	1.2.250.1.177.2.4.1.7.1	1 à 3 ans maximum
Authentification & signature	1.2.250.1.177.2.4.1.8.1	1 à 3 ans 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 ou physique

Dans le cas où l'AC génère la bi-clé, les données d'activation sont transmises :

- Dans le cas d'une carte à puce/token, via l'espace client du RC ou Porteur après authentification de ce dernier ;
- Dans le cas d'un module cryptographique avec différentes formes de données d'activation (cartes, secrets, etc.) via différents canaux de communication (mail, courrier, téléphone/SMS) et à différents moments.

EN 319 411-2 QCP-n EN 319 411-2 QCP-l
- Dans le cas d'un autre type d'équipement matériel ou logiciel, via un canal de communication distinct de la plateforme sur laquelle est proposé le certificat (mail, courrier, téléphone/SMS).

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 ou physique

Si la bi-clé est générée par l'AE, elle génère également les données d'activation qui sont envoyées par les moyens décrit au chapitre 6.4.1. Ces données d'activation ne sont pas sauvegardées par l'AE et sont modifiées par le RC ou Porteur lors de l'acceptation du certificat ou dans le cas d'un module cryptographique, après réception du module.

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

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

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

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 ».

6.6.2 Mesures liées à la gestion de la sécurité

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

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

Sans objet.

6.7 Mesures de sécurité réseau

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

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

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.

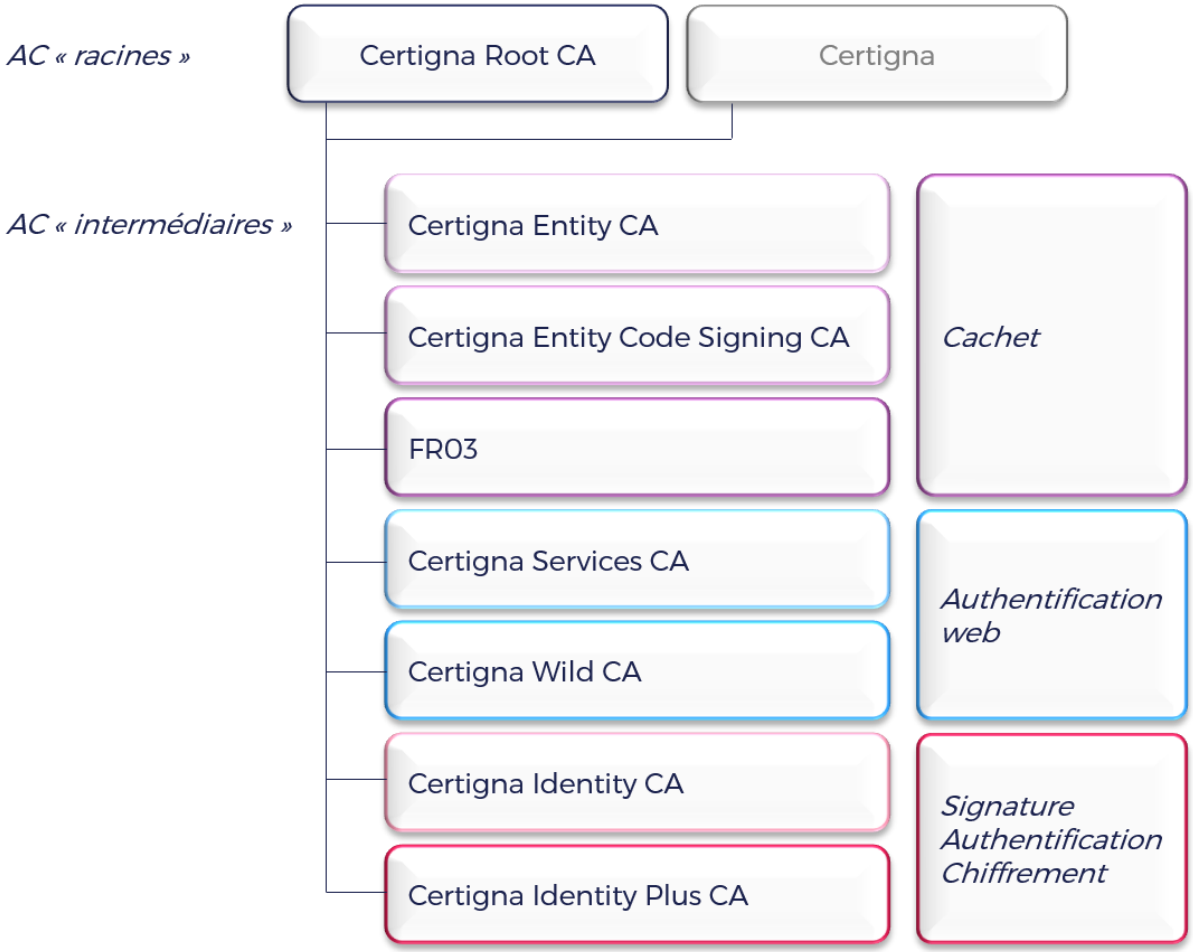
CERTIGNA dispose de deux AC racines :

- L'ancienne AC racine « Certigna » ;
- La nouvelle AC racine « Certigna Root CA » prévu en remplacement de l'ancienne racine « Certigna ».

Les certificats d'AC intermédiaires couvertes par cette PC ont été signés par les deux AC racines afin d'assurer la transition des certificats de l'ancienne racine vers la nouvelle.

7.1 Hiérarchie de confiance

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



7.2 Profils des certificats des AC Racines

7.2.1 Champs de base

Champs	Certigna Root CA	Certigna
Version	V3	
Serial Number	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-256 RSA 4096	SHA-128 RSA 2048
Subject Public Key Info	RSA 4096 bits	RSA 2048 bits
Validity	Dates et heures d'activation et d'expiration du Certificat	
Issuer DN	CN = Certigna Root CA OU = 0002 48146308100036 O = Dhimyotis C = FR	CN = Certigna O = Dhimyotis C = FR
Subject DN	CN = Certigna Root CA OU = 0002 48146308100036 O = Dhimyotis C = FR	CN = Certigna O = Dhimyotis C = FR

7.2.2 Extensions

Extensions	Critique	Certigna Root CA	Certigna
SKI	Non	Identifiant de la clé publique de l'autorité	
AKI	Non	Identifiant de la clé publique de l'autorité Racine	
Certificate Policies	Non	**CPS**=https://www.certigna.fr/autorites/	
CRL Distribution Points	Non	**URL**=http://crl.certigna.fr/certignarootca.crl **URL**=http://crl.dhimyotis.com/certignarootca.crl	
Netscape Cert type	Non		Autorité de certification SSL Autorité de certification SMIME Autorité de certification de signature
Basic Constraints	**Oui**	**cA** = TRUE	
Key Usage	**Oui**	Signature de certificat Signature de CRL	

7.3 Profils des certificats des AC intermédiaires pour personne morale

Autorité		ENTITY CA	ENTITY CODE SIGNING CA	FR03	SERVICES CA	WILD CA
Champs		**Contenu**				
Version		V3				
Serial Number		Numéro de série unique.				
Signature		Identifiant de l'algorithme de signature de l'AC / 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 Entity CA	Certigna Code Signing CA	FR03	Certigna Services CA	Certigna Wild CA
	OI =	NTRFR-0002 48146308100036			NTRFR-0002 48146308100036	
	OU =	0002 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	Signature de certificat Signature de CRL				

7.4 Profils des certificats des AC intermédiaires pour personne physique

Autorité		IDENTITY CA	IDENTITY PLUS CA
Champs		**Contenu**	
Version		V3	
Serial Number		Numéro de série unique.	
Signature		Identifiant de l'algorithme de signature de l'AC / 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 Identity CA	Certigna Identity Plus CA
	OI =	NTRFR-48146308100036	
	OU =	0002 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	Signature de certificat Signature de CRL	

7.4.1 Profils des certificats émis par Certigna Entity CA

7.4.1.1 Champs de base

CERTIGNA ENTITY CA										
Usage		Cachet de documents et mails						Cachet de jetons d'horodatage		
OID 1.2.250.1.177.2		.6.1.1.1	.6.1.7.1	.6.1.8.1	.6.1.4.1	.6.1.41.1	.6.1.42.1	.6.1.3.1	.6.1.9.1	.6.1.6.1
ETSI 319 411		LCP	QCP-l	QCP-l-psd2	QCP-l-qscd	QCP-l-qscd		LCP	QCP-l	QCP-l-qscd
RGS v2		RGS *			RGS **		RGS **	RGS *		RGS **
Champs		**Contenu**								
Version		V3								
Serial Number		Numéro de série unique délivré par un CSPRNG (Cryptographically secure pseudorandom number generator) 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								
Validity		1 à 3 ans						1 à 5 ans		
Issuer DN	CN = OI = OU = O = C =	Certigna Entity CA NTRFR-48146308100036 0002 48146308100036 Dhimyotis FR								
Subject DN	SN =	Série de caractères constitué en partie d'un aléa pour l'unicité								
	CN =	<Identité de l'entité> - <Nom du service>								
	OI =	Informations sur le justificatif d'identité de l'entité								
	OU =	ICD + Identifiant de l'entité liée au service enregistré conformément à la législation et réglementation en vigueur								
	O =	Nom de l'entité à laquelle le service de cachet est rattaché								
	C =	Pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée								

7.4.1.2 Extensions

CERTIGNA ENTITY CA										
Usage		Cachet de documents et mails						Cachet de jetons d'horodatage		
OID 1.2.250.1.177.2		.6.1.1.1	.6.1.7.1	.6.1.8.1	.6.1.4.1	.6.1.41.1	.6.1.42.1	.6.1.3.1	.6.1.9.1	.6.1.6.1
ETSI 319 411		LCP	QCP-l	QCP-l-psd2	QCP-l-qscd	QCP-l-qscd		LCP	QCP-l	QCP-l-qscd
RGS v2		RGS *			RGS **		RGS **	RGS *		RGS **
Extension	**Crit.**	**Contenu**								
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	Nom RFC822=Adresse e-mail du service de cachet								
Key Usage	Oui	Digital signature / Non repudiation								
Extended Key Usage	Non/ Oui	Email Protection [Non critique]						id-kp-timeStamping [Critique]		
Certificate Policies	Non	.6.1.1.1	.6.1.7.1	.6.1.8.1	.6.1.4.1	.6.1.41.1	.6.1.42.1	.6.1.3.1	.6.1.9.1	.6.1.6.1
		CPS= https://www.certigna.fr/autorites/								
CRL Distribut. Points	Non	URL=http://crl.certigna.fr/entityca.crl URL=http://crl.dhimyotis.com/entityca.crl								
Authority Info. Access	Non	calssuers=http://autorite.certigna.fr/entityca.der calssuers=http://autorite.dhimyotis.com/entityca.der URL=http://entityca.ocsp.certigna.fr URL=http://entityca.ocsp.dhimyotis.com								
Basic Constraints	Non	cA = FALSE								
QC Statement	Non		QcCompliance						QcCompliance	
					QcSSCD					QcSSCD
			QcEuPDS						QcEuPDS	
			QcType 2						QcType 2	
				PSD2QcType						

7.4.1 Profils des certificats émis par Certigna Entity Code Signing CA

7.4.1.1 Champs de base

CERTIGNA ENTITY CODE SIGNING CA			
Usage		Cachet de signature de code	
OID 1.2.250.1.177.2		.8.1.1.1	.8.1.2.1
ETSI 319 411		LCP	QCP-l-qscd
RGS v2		RGS *	RGS *
Champs		**Contenu**	
Version		V3	
Serial Number		Numéro de série unique délivré par un CSPRNG (Cryptographically secure pseudorandom number generator) 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	
Validity		1 à 3 ans	
Issuer DN	CN = OI = OU = O = C =	Certigna Entity Code Signing CA NTRFR-48146308100036 0002 48146308100036 Dhimyotis FR	
Subject DN	SN =	Série de caractères constitué en partie d'un aléa pour l'unicité	
	CN =	<Identité de l'entité> - <Nom du service>	
	OI =	Informations sur le justificatif d'identité de l'entité	
	OU =	ICD + Identifiant de l'entité liée au service enregistré conformément à la législation et réglementation en vigueur	
	O =	Nom de l'entité à laquelle le service de cachet est rattaché	
	C =	Pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée	

7.4.1.2 Extensions

CERTIGNA ENTITY CODE SIGNING CA			
Usage		Cachet de signature de code	
OID 1.2.250.1.177.2		.8.1.1.1	.8.1.2.1
ETSI 319 411		LCP	QCP-l-qscd
RGS v2		RGS *	RGS *
Champs	**Critique**	**Contenu**	
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	
Key Usage	**Oui**	Digital signature	
Extended Key Usage	Non	id-kp-codeSigning	
Certificate Policies	Non	OID=1.2.250.1.177.2.8.1.1.1	OID=1.2.250.1.177.2.8.1.2.1
		CPS= https://www.certigna.fr/autorites/	
CRL Distribut. Points	Non	URL=http://crl.certigna.fr/entitycsca.crl URL=http://crl.dhimyotis.com/entitycsca.crl	
Authority Info. Access	Non	calssuers=http://autorite.certigna.fr/entitycsca.der calssuers=http://autorite.dhimyotis.com/entitycsca.der URL=http://entitycsca.ocsp.certigna.fr URL=http://entitycsca.ocsp.dhimyotis.com	
Basic Constraints	Non	cA = FALSE	
QC Statement			QcCompliance
			QcSSCD
			QcEuPDS
			QcType 2 (eseal)

7.4.1 Profils des certificats émis par FR03

7.4.1.1 Champs de base

FR03		
Usage		**Cachet de signature de 2D-DOC**
OID 1.2.250.1.177.2		.2.1.1
ETSI 319 411		NCP +
RGS v2		RGS *
Champs		**Contenu**
Version		V3
Serial Number		Numéro de série unique délivré par un CSPRNG (Cryptographically secure pseudorandom number generator) Entre 128 et 160 bits
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-256 RSA 4096
Subject Public Key Info		NIST P-256
Validity		1 à 3 ans
Issuer DN	CN = OU = O = C =	FR03 0002 48146308100036 Dhimyotis FR
Subject DN	CN =	XXXY [1]
	OU =	ICD + Identifiant de l'entité liée au service enregistré conformément à la législation et réglementation en vigueur
	O =	Nom de l'entité à laquelle le service de cachet est rattaché
	C =	Pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée

[1] Nom codé sur 4 caractères alphanumériques majuscules et composé d'un code client sur les 3 premiers caractères et du numéro d'ordre chronologique du certificat cachet (de 0 à 9 puis de A à Z).

7.4.1.2 Extensions

FR03		
Usage		**Cachet de signature de 2D-DOC**
OID 1.2.250.1.177.2		.2.1.1
ETSI 319 411		NCP +
RGS v2		RGS *
Champs	**Critique**	**Contenu**
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	Type de document signé (OID + Description)
Key Usage	**Oui**	Digital signature / Non repudiation
Extended Key Usage	Non	anyExtendedKeyUsage
Certificate Policies	Non	OID=1.2.250.1.177.2.2.1.1
		CPS= https://www.certigna.fr/autorites/
CRL Distribut. Points	Non	URL=http://crl.certigna.fr/2ddoc.crl URL=http://crl.dhimyotis.com/2ddoc.crl
Authority Info. Access	Non	caIssuers=http://autorite.certigna.fr/2ddoc.der caIssuers=http://autorite.dhimyotis.com/2ddoc.der URL=http://2ddoc.ocsp.certigna.fr URL=http://2ddoc.ocsp.dhimyotis.com
Basic Constraints	Non	cA = FALSE

7.4.2 Profils des certificats émis par Certigna Services CA

7.4.2.1 Champs de base

CERTIGNA SERVICES CA					
Usage		Authentification Serveur	Authentification Client	Authentification Serveur/Client	
OID 1.2.250.1.177.2		.5.1.1.1	.5.1.2.1	.5.1.3.1	.5.1.4.1
ETSI 319 411		OVCP	OVCP	QCP-w	QCP-w
RGS v2		RGS *	RGS *		
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 RSA 4096			
Subject Public Key Info		RSA 2048			
Validity		825 jours			
Issuer DN	CN = OU = OI = O = C =	Certigna Services CA 0002 48146308100036 NTRFR-48146308100036 Dhimyotis FR			
Subject DN	Common Name	Un des FQDN de l'extension « Subject Alternative Name »			
	Organization Identifier				Identifiant fourni par ACN [1]
	Organization Unit Name	ICD + Identifiant de l'entité liée au serveur			
	Organization	Nom de l'entité à laquelle le serveur est rattaché			
	Street Address			N° et rue de domiciliation de l'entité (2.5.4.9)	
	Locality Name	Ville ou village de domiciliation de l'entité (2.5.4.7)			
	Postal Code			Code postal de domiciliation de l'entité (2.5.4.17)	
	State or Province Name			Département ou région de domiciliation (2.5.4.8)	
	Country Name	Pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée			
	Business Category			Catégorie professionnelle de l'entité (2.5.4.15)	
	Jurisd. Locality Name			Ville/village de juridiction de l'entité (si pertinent)	
	Jurisd. State/Prov. Name			Département de juridiction de l'entité (si pertinent)	
	Jurisd. Country Name			Pays de la juridiction de l'entité (1.3.6.1.4.1.311.60.2.1.3)	
	Serial Number	Série de caractères constitué d'un aléa		Identifiant de l'entité liée au service enregistré	

7.4.2.2 Extensions

CERTIGNA SERVICES CA					
Usage		Authentification Serveur	Authentification Client	Authentification Serveur/Client	
OID 1.2.250.1.177.2		.5.1.1.1	.5.1.2.1	.5.1.3.1	.5.1.4.1
ETSI 319 411		OVCP	OVCP	QCP-w	QCP-w
RGS v2		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 dans les 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 2.23.140.1.2.2 (OVCP)	.5.1.2.1 2.23.140.1.2.2 (OVCP)	.5.1.3.1 0.4.0.194112.1.4 (QCP-w) 2.23.140.1.1 (EV Guidelines)	.5.1.4.1 0.4.0.19495.3.1 (QCP-w-psd2) 2.23.140.1.1 (EV Guidelines)
		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	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			
Basic Constraints	Non	cA = FALSE			
Cabf Organization. Identifier 2.23.140.3.1	Non				Informations sur l'entité [2]
Certif. Transparency	Non	Liste de SCTs. *Uniquement pour les certificats contenant un ou plusieurs FDQN.*			
QC Statement	Non			QcCompliance	QcCompliance
				QcEuPDS	QcEuPDS
				QcType 3 (web)	QcType 3 (web)
					PSD2QcType [3]

[1] Le champ « OrganizationIdentifier » (OI) est utilisé pour fournir le numéro d'enregistrement de l'entité rattachée au certificat. Dans le cas où 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] Informations sur l'entité sous la forme suivante :

registrationSchemeIdentifier = 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.

7.4.2.3 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 à minima auprès des journaux suivants :

- mammoth.ct.comodo.com
- ct.googleapis.com/logs/argon*20XX* (où *20XX* est l'année d'expiration du certificat)
- yeti*20XX*.ct.digicert.com (où *20XX* est l'année d'expiration du certificat)
- ct.cloudflare.com/logs/nimbus*20XX* (où *20XX* est l'année d'expiration du certificat)

7.4.3 Profils des certificats émis par Certigna Wild CA

7.4.3.1 Champs de base

CERTIGNA WILD CA			
Usage		Authentification serveur/client multi-domaines	Authentification serveur/client Wildcard multi-domaines
OID 1.2.250.1.177.2		.7.1.1.1	.7.1.2.1
ETSI 319 411		LCP	LCP
RGS v2			
Champs		**Contenu**	
Version		V3	
Serial Number		Numéro de série unique délivré par un CSPRNG (Cryptographically secure pseudorandom number generator) 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	
Validity		825 jours	
Issuer DN	CN = OU = OI = O = C =	Certigna Wild CA 0002 48146308100036 NTRFR-48146308100036 Dhimyotis FR	
Subject DN	CN =	Un des FQDN de l'extension « Subject Alternative Name »	
	OU =	ICD + Identifiant de l'entité liée au service enregistré conformément à la législation et réglementation en vigueur	
	O =	Nom de l'entité à laquelle le service de cachet est rattaché	
	L =	Ville où est implantée l'entité	
	C =	Pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée	

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.

7.4.3.2 Extensions

CERTIGNA WILD CA			
Usage		Authentification serveur/client multi-domaines	Authentification serveur/client Wildcard multi-domaines
OID 1.2.250.1.177.2		.7.1.1.1	.7.1.2.1
ETSI 319 411		LCP	LCP
RGS v2			
Champs	**Critique**	**Contenu**	
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=1.2.250.1.177.2.7.1.2.1 OID=2.23.140.1.2.2 (OVCP)
		CPS= https://www.certigna.fr/autorites/	
CRL Distribut. Points	Non	URL=http://crl.certigna.fr/entitycsca.crl URL=http://crl.dhimyotis.com/entitycsca.crl	
Authority Info. Access	Non	calssuers=http://autorite.certigna.fr/entitycsca.der calssuers=http://autorite.dhimyotis.com/entitycsca.der URL=http://entitycsca.ocsp.certigna.fr URL=http://entitycsca.ocsp.dhimyotis.com	
Basic Constraints	Non	cA = FALSE	
Certificate Transparency	Non	Liste de SCTs. *Uniquement pour les certificats contenant un ou plusieurs FDQN.*	

7.4.3.3 Pré-certificats

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 à minima auprès des journaux suivants :

- mammoth.ct.comodo.com
- ct.googleapis.com/logs/argon*20XX* (où *20XX* est l'année d'expiration du certificat)
- yeti*20XX*.ct.digicert.com (où *20XX* est l'année d'expiration du certificat)
- ct.cloudflare.com/logs/nimbus*20XX* (où *20XX* est l'année d'expiration du certificat)

7.4.4 Profils des certificats émis par Certigna Identity CA

7.4.4.1 Champs de base

CERTIGNA IDENTITY CA					
OID 1.2.250.1.177.2		.3.1.1.1	.3.1.2.1	.3.1.3.1	.3.1.4.1
Usage		Chiffrement	Authentification/Signature	Chiffrement	Authentification/Signature
ETSI 319 411		LCP	LCP	LCP	LCP
RGS v2		RGS *	RGS *	RGS *	RGS *
Champs		**Contenu**			
Version		V3			
Serial Number		Numéro de série unique délivré par un CSPRNG (Cryptographically secure pseudorandom number generator) 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			
Validity		1 à 3 ans	1 à 3 ans	1 à 5 ans	1 à 5 ans
Issuer DN	CN = OU = OI = O = C =	Certigna Identity CA 0002 48146308100036 NTRFR-48146308100036 Dhimyotis FR			
Subject DN	CN =	<Prénom> <NOM> CHIF	<Prénom> <NOM> ID	<Prénom> <NOM> CHIF	<Prénom> <NOM> ID
	GN =	<Prénom>			
	SN =	<NOM>			
	OU =	ICD + identifiant [1]	ICD + identifiant [1]		
	O =	Nom de l'entité à laquelle le porteur est rattaché			
	C =	Pays auprès de laquelle **l'entité** est enregistrée		Pays auprès de laquelle **le Porteur** est enregistrée	
	SN =	Série de caractères constitué en partie d'un aléa pour l'unicité			

[1] Identifiant de l'entité à laquelle appartient le porteur enregistré conformément à la législation et aux réglementations en vigueur

7.4.4.2 Extensions

CERTIGNA IDENTITY CA					
OID 1.2.250.1.177.2		.3.1.1.1	.3.1.2.1	.3.1.3.1	.3.1.4.1
Usage		Chiffrement	Authentification/signature	Chiffrement	Authentification/signature
ETSI 319 411		LCP	LCP	LCP	LCP
RGS v2		RGS *	RGS *	RGS *	RGS *
Extension	**Critique**	**Contenu**			
Authority Key Identifier	Non	Identifiant de la clé publique de l'AC			
Subject Key Identifier	Non	Identifiant de la clé publique du Porteur			
Subject Alt. Name	Non	Nom RFC822=Adresse e-mail du Porteur			
Key Usage	Oui	key Encipherment	Digital signature / Non repudiation	Key Encipherment	Digital signature / Non repudiation
Extended Key Usage	Non	Email Protection / msEFS	Client Auth / Email Protection	Email Protection / msEFS	Client Auth / Email Protection
Certificate Policies	Non	.3.1.1.1	.3.1.2.1	.3.1.3.1	.3.1.4.1
		CPS= https://www.certigna.fr/autorites/			
CRL Distribut. Points	Non	URL=http://crl.certigna.fr/identityca.crl URL=http://crl.dhimyotis.com/identityca.crl			
Authority Info. Access	Non	calssuers=http://autorite.certigna.fr/identityca.der calssuers=http://autorite.dhimyotis.com/identityca.der URL=http://identityca.ocsp.certigna.fr URL=http://identityca.ocsp.dhimyotis.com			
Basic Constraints	Non	cA = FALSE			

7.4.5 Profils des certificats émis par Certigna Identity Plus CA

7.4.5.1 Champs de base

CERTIGNA IDENTITY PLUS CA									
OID 1.2.250.1.177.2		.4.1.1.1	.4.1.7.1	.4.1.8.1	.4.1.4.1	.4.1.3.1	.4.1.6.1	.4.1.2.1	.4.1.5.1
Usage		Auth + Sign	Auth + Sign	Auth + Sign	Auth + Sign	Signature	Signature	Authent.	Authent.
ETSI 319 411		QCP-n-qscd	QCP-n	QCP-n-qscd	QCP-n-qscd	QCP-n-qscd	QCP-n-qscd	NCP+	NCP+
RGS v2		RGS **			RGS **	RGS ***	RGS ***	RGS ***	RGS ***
Champs		**Contenu**							
Version		V3							
Serial Number		Numéro de série unique délivré par un CSPRNG (Cryptographically secure pseudorandom number generator) 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							
Validity		1 à 3 ans	1 à 3 ans	1 à 3 ans	1 à 5 ans	1 à 3 ans	1 à 5 ans	1 à 3 ans	1 à 5 ans
Issuer DN	CN = OU = OI = O = C =	Certigna Identity Plus CA 0002 48146308100036 NTRFR-48146308100036 Dhimyotis FR							
Subject DN	CN =	<Prénom> <NOM> ID				<Prénom> <NOM> SIGN		<Prénom> <NOM> AUTH	
	GN =	<Prénom>							
	SN =	<NOM>							
	OU =	ICD + id. [1]				ICD + ident.[1]		ICD + id. [1]	
	O =	Nom entité [2]				Nom entité [2]		Nom entité [2]	
	C =	Pays de l'autorité compétente auprès de laquelle **l'entité** ou le **Porteur** est officiellement enregistrée							
	SN =	Série de caractères constitué en partie d'un aléa pour l'unicité							

[1] Identifiant de l'entité liée au Porteur enregistré conformément à la législation et aux réglementations en vigueur

[2] Nom de l'entité à laquelle le Porteur est rattaché

7.4.5.2 Extensions

CERTIGNA IDENTITY PLUS CA									
OID 1.2.250.1.177.2		.4.1.1.1	.4.1.7.1	.4.1.8.1	.4.1.4.1	.4.1.3.1	.4.1.6.1	.4.1.2.1	.4.1.5.1
Usage		Auth + Sign	Auth + Sign	Auth + Sign	Auth + Sign	Signature	Signature	Authent.	Authent.
ETSI 319 411		QCP-n-qscd	QCP-n	QCP-n-qscd	QCP-n-qscd	QCP-n-qscd	QCP-n-qscd	NCP+	NCP+
RGS v2		RGS **			RGS **	RGS ***	RGS ***	RGS ***	RGS ***
Extension	**Critique**	**Contenu**							
Authority Key Identifier	Non	Identifiant de la clé publique de l'AC							
Subject Key Identifier	Non	Identifiant de la clé publique du Porteur							
Subject Alt. Name	Non	Nom RFC822=Adresse e-mail du Porteur							
Key Usage	Oui	Digital signature / Non repudiation				Non repudiation		Digital signature	
Extended Key Usage	Non	Client Auth / Email Protection				Email Protection		Client Auth	
Certificate Policies	Non	OID.4.1.1.1	OID.4.1.7.1	OID.4.1.8.1	OID.4.1.4.1	OID.4.1.3.1	OID.4.1.4.1	OID.4.1.2.1	OID.4.1.5.1
		CPS= https://www.certigna.fr/autorites/							
CRL Distribut. Points	Non	URL=http://crl.certigna.fr/identityplusca.crl URL=http://crl.dhimyotis.com/identityplusca.crl							
Authority Info. Access	Non	calssuers=http://autorite.certigna.fr/identityplusca.der calssuers=http://autorite.dhimyotis.com/identityplusca.der URL=http://identityplusca.ocsp.certigna.fr URL=http://identityplusca.ocsp.dhimyotis.com							
Basic Constraints	Non	cA = FALSE							
QC Statement	Non	QcCompliance							
		QcSSCD		QcSSCD					
		QcEuPDS							
		QcType 1							

7.5 Profils des certificats OCSP des AC intermédiaires pour personne morale

Autorité		ENTITY CA	ENTITY CODE SIGNING CA	FR03	SERVICES CA	WILD CA
Champs		**Contenu**				
Version		V3				
Serial Number		Numéro de série unique.				
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-256 RSA 4096				
Subject Public Key Info		RSA 2048				
Validity		3 ans				
Issuer DN	CN =	Certigna Entity CA	Certigna Entity Code Signing CA	FR03	Certigna Services CA	Certigna Wild CA
	OU =					
	OI =	0002 48146308100036				
	O =	NTRFR-48146308100036			NTRFR-48146308100036	
	C =	Dhimyotis				
		FR				
Subject DN	CN =	OCSP Entity CA	OCSP Entity Code Signing CA	2D-Doc	OCSP Services CA	OCSP Wild CA
	OU =					
	O =	0002 48146308100036				
	C =	Dhimyotis				
		FR				
Extensions	**Critiq.**	**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				
Authority Informat. Access	Non	calssuers=http://autorite.certigna.fr/ <Nom AC>.der calssuers=http://autorite.dhimyotis.com/<Nom AC>.der URL=http://<Nom AC>.ocsp.certigna.fr URL=http:// <Nom AC>.ocsp.dhimyotis.com				
CRL Distribution Points	Non	URL=http://crl.certigna.fr/XXXX.crl URL=http://crl.dhimyotis.com/wildca.crl				
Ocsp No Check	Non					
Basic Constraints	Non	cA = FALSE				

7.6 Profils des certificats OCSP des AC intermédiaires pour personne physique

Autorité		IDENTITY CA	IDENTITY PLUS CA
Champs		**Contenu**	
Version		V3	
Serial Number		Numéro de série unique.	
Signature		Identifiant de l'algorithme de signature de l'AC / SHA-256 RSA 4096	
Subject Public Key Info		RSA 2048	
Validity		3 ans	
Issuer DN	CN =	Certigna Identity CA	Certigna Identity Plus CA
	OU =	0002 48146308100036	
	OI =	NTRFR-48146308100036	
	O =	Dhimyotis	
	C =	FR	
Subject DN	CN =	OSCP Identity CA	OCSP Identity Plus CA
	OU =	0002 48146308100036	
	O =	Dhimyotis	
	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	
Authority Informat. Access	Non	caIssuers=http://autorite.certigna.fr/ <Nom AC>.der caIssuers=http://autorite.dhimyotis.com/<Nom AC>.der URL=http://<Nom AC>.ocsp.certigna.fr URL=http:// <Nom AC>.ocsp.dhimyotis.com	
CRL Distribution Points	Non	URL=http://crl.certigna.fr/XXXX.crl URL=http://crl.dhimyotis.com/wildca.crl	
Ocsp No Check	Non		
Basic Constraints	Non	cA = FALSE	

7.7 Profils des LCR des AC intermédiaires

		ENTITY CA	ENTITY CODE SIGNING CA	FR03	SERVICES CA	WILD CA	IDENTITY CA	IDENTITY PLUS CA
Champs		**Contenu**						
Version		V2						
Signature		Identifiant de l'algorithme de signature de l'AC. SHA-256 RSA 4096						
Issuer DN	CN =	Certigna Entity CA	Certigna Entity Code Signing CA	FR03	Certigna Services CA	Certigna Wild CA	Certigna Identity CA	Certigna Identity Plus CA
	OU =	0002 48146308100036						
	OI =	NTRFR-48146308100036			NTRFR-48146308100036			
	O =	Dhimyotis						
	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						
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.						

7.8 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.

7.8.1 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.

7.8.2 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 ».

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 affichés dans cette PC et aux pratiques identifiées dans la DPC correspondante.

Les chapitres suivants ne concernent que les audits et évaluations de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

L'AC peut réaliser des audits auprès des opérateurs d'AED ou des mandataires de certification au même titre que le personnel de son IGC. Il s'assure entre autres que les opérateurs d'AED ou les MC respectent les engagements vis-à-vis de cette PC et les pratiques correspondantes.

8.1 Fréquences et/ou circonstances des évaluations

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

Ce contrôle est également effectué par l'AC à minima une fois par an.

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 qualifications sont réalisés par des auditeurs qualifiés.

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

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

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

L'AC contrôle strictement la qualité du service des certificats délivrés ou contenant des informations vérifiées par un tiers délégué en demandant à un spécialiste de la validation employé par l'AC d'effectuer des vérifications trimestrielles en cours sur un échantillon sélectionné au hasard d'au moins trois pour cent des Certificats vérifiés par le tiers délégué dans la période commençant immédiatement après la prise du dernier échantillon.

L'autorité de certification examinera les pratiques et les procédures de chaque tiers délégué afin de s'assurer que le tiers délégué est en conformité avec les exigences de cette PC et de la DPC associée.

8.5 Actions prises suite aux conclusions des évaluations

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

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

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

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

8.6 Communication des résultats

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

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

La délivrance de certificats aux Porteurs 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 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 Porteurs ;
- Les causes de révocation des certificats.

9.3.2 Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3 Responsabilités en termes de protection des informations confidentielles

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

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

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

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

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

Les dossiers de demande de certificat électronique 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. Les informations personnelles d'identité peuvent être utilisées comme données d'authentification lors d'une éventuelle demande de révocation ou d'informations.

Par ailleurs, DHIMYOTIS 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@dhimyotis.com, ou par courrier à l'adresse suivante :

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

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

9.4.2 Informations à caractère personnel

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

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

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

9.4.5 Notification et consentement d'utilisation des données personnelles

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les Porteurs à l'AC ne doivent pas être divulguées ni

transférées à un tiers sauf dans les cas suivants : consentement préalable du Porteur, décision judiciaire ou autre autorisation légale.

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

La divulgation des informations confidentielles n'est effectuée qu'aux autorités 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 service de cachet, un serveur web ou un Porteur donné et que le RC ou le Porteur correspondant a accepté le certificat, conformément aux exigences du chapitre 4.4 ;
- Garantir et maintenir la cohérence de sa DPC avec sa PC ;
- Prendre toutes les mesures raisonnables pour s'assurer que les Porteurs 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 ou un Porteur 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 service de cachet, au serveur web ou au Porteur a autorisé la délivrance du certificat, et que le RC ou le Porteur 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 ou du Porteur 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.

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
- Mettre en œuvre et suivre, lors de la délivrance d'un certificat, les exigences décrites aux chapitres 3.2 et 3.3 de la présente PC pour vérifier que le RC a le droit d'utiliser ou de contrôler le(s) nom(s) de domaine indiqué(s) dans les champs « commonName » et « subjectAltName » du certificat (ou uniquement dans le cas où les droits d'utilisation ou de contrôle des noms de domaine ont été délégués par une personne disposant de ces droits).	

L'AC assume toute conséquence dommageable résultant du non-respect de sa PC par elle-même ou l'une de ses composantes. Elle a pris les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la 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 Porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

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

9.6.2 Service d'enregistrement

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

9.6.3 RC et Porteur

Le RC ou le Porteur a le devoir de :
- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- Protéger la clé privée dont il a la responsabilité par des moyens appropriés à son environnement ;
- Protéger ses données d'activation et, le cas échéant, les mettre en œuvre ;
- Protéger l'accès à la base de certificats du RC ou du Porteur ;
- Respecter les conditions d'utilisation de la clé privée et du certificat correspondant ;
- Informer l'AC de toute modification concernant les informations contenues dans le certificat du service de cachet, du serveur web ou du Porteur ;
- Faire, sans délai, une demande de révocation du certificat dont il est responsable auprès de l'AE, ou le cas échéant du MC de son entité, en cas de compromission ou de suspicion de compromission de la clé privée correspondante.

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

9.6.4 Utilisateurs de certificats

Les tiers utilisateurs doivent :
- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Pour chaque certificat de la chaîne de certification, du certificat 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.

9.6.5 Autres participants

Sans objet.

9.6.6 Résiliation

En cas de manquement par l'AC, le RC ou le Porteur 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 ou le Porteur 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 ou le Porteur doit vérifier que les informations énoncées dans la demande de certificat sont exactes. A défaut, le RC ou le Porteur 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 ou le Porteur 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 ou le Porteur. 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 ou le Porteur 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 ou du Porteur de bien vérifier l'exactitude de ses informations la première fois que cela lui est demandé. A défaut, le RC ou le Porteur 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 ou du Porteur soit depuis son espace client, soit sur un support cryptographique. L'installation du certificat se fait sous la seule responsabilité du RC ou du Porteur. En cas de difficulté quelconque pendant cette dernière phase, le RC ou le Porteur 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 PC.

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 Porteur 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 ou le Porteur du certificat, ni du contenu des documents et des données qui lui sont remis par le RC, le Porteur 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 Porteur,
- Retard dans la fourniture des données à traiter dû au RC ou au Porteur ;
- 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 Porteur, 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 CM ou le Porteur

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.

9.10.2 Fin anticipée de validité

La publication d'une nouvelle version des documents cités au chapitre 1.1 peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC

correspondante. Dans ce cas, cette mise en conformité n'imposera pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

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

9.10.3 Effets de la fin de validité et clauses restant applicables

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

9.11 Notifications individuelles et communications entre les participants

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

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

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

L'AC procède à toute modification des spécifications stipulées dans la PC et la DPC et/ou des composantes de l'AC qui lui apparaît nécessaire pour l'amélioration de la qualité des services de certification et de la sécurité des processus, en restant toutefois conforme aux exigences citées au chapitre 1.1.

L'AC procède également à toute modification des spécifications stipulées dans la PC et la DPC et/ou des composantes de l'AC qui est rendue nécessaire par une législation, réglementation en vigueur ou par les résultats des Contrôles. Une révision et mise à jour si nécessaire de la PC et DPC sont effectuées à minima 1 fois par an.

9.12.2 Mécanisme et période d'information sur les amendements

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

9.12.3 Circonstances selon lesquelles l'OID doit être changé

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

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

9.13 Dispositions concernant la résolution de conflits

La validité de la présente PC 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 ou le Porteur 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 ou le Porteur 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.

9.14 Juridictions compétentes

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

9.15 Conformité aux législations et réglementations

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

9.16 Dispositions diverses

9.16.1 Accord global

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

9.16.2 Transfert d'activités

Cf. chapitre 5.8.

9.16.3 Conséquences d'une clause non valide

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

En cas de conflit entre les exigences de cette 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 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 et 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

Sans objet.

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 SERVICE, SERVEUR OU PORTEUR

11.1 Exigences sur les objectifs de sécurité

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
FR03	*Cachet 2D-DOC*
RGS * 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 la fonction de génération des cachets électroniques et protéger la clé privée contre toute utilisation par des tiers.	

SERVICES CA	*Authentification web*
WILD CA	*Authentification web*
RGS * 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.	

CERTIGNA IDENTITY CA	Authent./signature/Chiffrement
CERTIGNA IDENTITY PLUS CA	Authentification/signature
RGS * RGS ** 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 Porteur 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 publique lors de son export hors du dispositif.	
Chiffrement	
- Assurer la fonction de déchiffrement, de clés symétriques de fichier ou de message, pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ; - Permettre de garantir l'authenticité et l'intégrité de la clé symétrique de fichier ou de message, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données ; - Le cas échéant, permettre de garantir la confidentialité, l'authenticité et l'intégrité de la clé privée lors de son export hors du dispositif, à destination d'une fonction de séquestre ou d'archivage des clés privées.	

11.2 Exigences sur la qualification

CERTIGNA ENTITY CA	*Cachet mails/docs/horodatage*
CERTIGNA ENTITY CODE SIGNING CA	*Cachet code*
FR03	*Cachet 2D-DOC*
EN 319 411-2 QCP-l-qscd	
Le dispositif de protection des clés privées fourni par l'AC ou utilisé par le RC est qualifié « Qualified Seal Creation Device » (QSCD).	
RGS * RGS **	
Le dispositif de protection des clés privées fourni par l'AC ou utilisé par le RC est : - Soit un dispositif matériel de type carte à puce ou module cryptographique qualifié par l'ANSSI ; - Soit une solution logicielle respectant les exigences du chapitre 11.1 via la mise en place de mesures de sécurité additionnelles propres à l'environnement dans lequel est déployé la clé privée. Cet environnement dans lequel est déployée la clé privée doit avoir fait l'objet d'un audit de sécurité.	

CERTIGNA IDENTITY CA	Authent./signature/Chiffrement
CERTIGNA IDENTITY PLUS CA	Authentification/signature
EN 319 411-2 QCP-n-qscd	
Le dispositif de protection des clés privées fourni par l'AC ou utilisé par le Porteur est qualifié « Qualified Signature Creation Device » (QSCD).	
RGS ***	
Le dispositif de protection des clés privées fourni par l'AC ou utilisé par le Porteur est qualifié au minimum au niveau « Renforcé » par l'ANSSI.	
RGS **	
Le dispositif de protection des clés privées fourni par l'AC ou utilisé par le Porteur est qualifié au minimum au niveau « Standard » par l'ANSSI.	
RGS *	
Le dispositif de protection des clés privées fourni par l'AC ou utilisé par le Porteur est qualifié au minimum au niveau « Elémentaire » par l'ANSSI.	

CERTIGNA

www.certigna.com | www.dhimyotis.com

© 2019 Certigna, Services de confiance numérique

tessi