Certigna

PC/DPC

POLITIQUE DE CERTIFICATION / DÉCLARATION DES PRATIQUES DE CERTIFICATION

CERTIGNA ROOT CA

Edité le :	19/03/2025	
Version :	5.1	
OID :	1.2.250.1.177.1.0.1	CERTIGNA
	1.2.250.1.177.2.0.1	CERTIGNA ROOT CA
Classification :	Publique	

1 INTRODUCTION

1.1 Nom et identification du document

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

- 1.2.250.1.177.1.0.1 CERTIGNA
- 1.2.250.1.177.2.0.1 CERTIGNA ROOT CA

1.2 Redirection

IMPORTANT : La présente PC/DPC décrivait les engagements et pratiques mises en œuvre pour les certificats émis par les Autorités de certification de CERTIGNA. Comme recommandé par le CA/Browser Forum (http://www.cabforum.org), cette PC/DPC a été divisée en plusieurs PC/DPC :

PC/DPC	OID	AC Racine	Type de certificats
CERTIGNA TLS	1.2.250.1.177.1.0.1 1.2.250.1.177.2.0.1 1.2.250.1.177.6.0.1.1 1.2.250.1.177.14.0.1.1	CERTIGNA CERTIGNA ROOT CA CERTIGNA SERVER AUTHENTICATION ROOT CA CERTIGNA SERVER AUTHENTICATION EU ROOT CA	Authentification web (SSL/TLS)
CERTIGNA EMAIL PROTECTION	1.2.250.1.177.1.0.1 1.2.250.1.177.2.0.1 1.2.250.1.177.8.0.1.1 1.2.250.1.177.17.0.1.1	CERTIGNA CERTIGNA ROOT CA CERTIGNA EMAIL PROTECTION ROOT CA CERTIGNA EMAIL PROTECTION EU ROOT CA	Signature de mails (S/MIME)
CERTIGNA CODE SIGNING	1.2.250.1.177.1.0.1 1.2.250.1.177.2.0.1 1.2.250.1.177.13.0.1.1	CERTIGNA CERTIGNA ROOT CA CERTIGNA CODE SIGNING ROOT CA	Cachet de code
CERTIGNA MULTIPURPOSE	1.2.250.1.177.1.0.1 1.2.250.1.177.2.0.1 1.2.250.1.177.7.0.1.1 1.2.250.1.177.15.0.1.1 1.2.250.1.177.9.0.1.1 1.2.250.1.177.16.0.1.1 1.2.250.1.177.10.0.1.1 1.2.250.1.177.11.0.1.1 1.2.250.1.177.12.0.1.1 1.2.250.1.177.18.0.1.1	CERTIGNA CERTIGNA ROOT CA CERTIGNA CLIENT AUTHENTICATION ROOT CA CERTIGNA CLIENT AUTHENTICATION EU ROOT CA CERTIGNA DOCUMENT SIGNING ROOT CA CERTIGNA DOCUMENT SIGNING EU ROOT CA CERTIGNA OTF DOCUMENT SIGNING ROOT CA CERTIGNA TIME STAMPING ROOT CA CERTIGNA ENCRYPTION ROOT CA CERTIGNA ENCRYPTION EU ROOT CA	 Authentification client Authentification client Signature de documents Signature de documents Signature de documents Cachet d'horodatage Chiffrement Chiffrement

Nous vous invitons à consulter ces PC/DPC à l'adresse suivante :

https://www.certigna.com/autorites-de-certification/

1.3 Révision du document

Le tableau ci-dessous présente l'historique de cette PC/DPC avant qu'elle ne soit divisée en plusieurs documents.

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	Précisions 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).
3.2	24/08/2020	Réduction de la durée de vie des certificats SSL/TLS (cf. 7.4.2, 7.4.3)
3.3	02/11/2020	Révision du document et précisions apportées sur : - Domaines applicables aux différents certificats (cf. 1.4) ; - Modalités de validation des PC/DPC/CGVU (cf. 1.5) ; - Rappel du face à face applicable pour certificats NCP+ (cf. 3.2.3.3.2) ; - Description de l'OID du SAN dans certificats de FR03 (cf. 7.5.3.2) ; - Ordonnancement des champs dans les DN des certificats (cf. 7.5).
3.4	14/06/2021	Révision du document et précisions apportées sur : - Le rôle de demandeur (cf. 1.3.3) ; - La durée de la validation des noms de domaine (cf. 3.2.2.4) ; - Les enregistrements DNS CAA de CERTIGNA (cf. 3.2.2.8) ; - Les méthodes démontrant la compromission d'une clé (cf. 4.9.12) ; - La stratégie des certificats QWAC (cf. 7.5.4.2) ; - La protection des données à caractère personnel (cf. 9.4.1) ; - Les obligations des RC et des Porteurs (cf. 9.6.3) ; - Les obligations des demandeurs de certificats (cf. 9.6.4).
3.5	01/12/2021	Révision du document et précisions apportées sur : - Les URLs d'accès aux documentations et services ; - Les fournisseurs et les exigences applicables (cf. 1.3.6.4) ; - Les méthodes autorisées pour les certificats wildcard (cf. 3.2.2.4.6) ; - Cause de révocation liée à perte de qualification support (cf. 4.9.1.1) ; - La stratégie des certificats QWAC (cf. 7.5.4.2) ; - Profil des LAR avec raison de révocation (cf. 7.9) ; - L'engagement à fournir des services non-discriminatoires (cf. 9.15).

3.6	01/09/2022	Révision du document et précisions apportées sur : - Les raisons de révocation (cf. 4.9.1.1) ; - La révocation de certificats présumant exister (cf. 4.9.3.2) ; - La publication des causes de révocation (cf. 4.9.3.2 et 7.8) ; - Les nouveaux gabarits de certificats en RSA 3072 (cf. 6.1.5.3 et 7.5) ; - Les nouveaux gabarits de certificats QNCP-w (cf. 7.5) ; - L'ajout de journaux pour les SCT (Cf. 7.5.4.3).
3.7	25/11/2022	Révision du document et précisions apportées sur : - Le lien entre CERTIGNA, DHIMYOTIS et TESSI (cf. 1.1) ; - Les URL utilisées dans le champ AIA (cf. 7).
3.8	22/05/2023	Révision du document et précisions apportées sur : - La conformité aux BR S/MIME à compter de 01/09/2023 (cf. 1.1) ; - Les exigences contractuelles avec les AE (cf. 1.3.2) ; - Les types de noms pour les certificats S/MIME (cf. 3.1.1) ; - La substitution des caractères non-ASCII (cf. 3.1.4) ; - La méthode « changement apporté au site web v2 » (cf. 3.2.2.4.18) ; - L'enregistrement CAA (cf. 3.2.2.8) ; - Les raisons de révocation (cf. 4.9.1.2) ; - Les exigences sur l'OCSP (cf. 4.9.10) ; - Les types d'évènements à enregistrer (cf. 5.4.1) ; - Les revues de PCA (cf. 5.7.1) ; - Les conditions de rejet d'une demande de certificat (cf. 6.1.1.3) ; - L'arrêt de la signature de hash SHA-1 (cf. 7.1) ; - Les caractéristiques des évaluations (cf. 8.1, 8.2, 8.4, 8.6, 8.7).
3.9	01/09/2023	Révision du document et précisions apportées sur : - La méthode d'autorisation du domaine sur jeton de demande (cf. 3.2.2.4) ; - L'ajout de journaux pour les SCT (cf. 7.1.4) ; - Le retrait de l'EKU « Email Protection » pour les certificats (cf. 7.1.4) ; - L'ajout du champ « OrganizationIdentifier » aux certificats (cf. 7.1.4) ;
4.0	12/09/2023	Révision du document et précisions apportées sur : - L'OID des certificats SSL Client (cf. 7.1.4) ; - L'EKU « Email Protection » des certificats ID et cachets (cf. 7.1.4) ; - Le retrait de l'Email dans le SAN des certificats ID et cachets (cf. 7.1.4).
4.1	11/10/2023	Révision du document et précisions apportées sur : - Liens vers la TSL et le site de LSTI pour l'état des qualifications (cf. 1.1) ; - Les contacts de FAQ et pour toute réclamation ou révocation (cf. 1.5.2) ; - Le délai où la réponse d'une CRL peut différer de l'OCSP (Cf. 4.10.1).
4.2	06/11/2023	Révision du document et précisions apportées sur : - La migration des certificats ID RGS **/eIDAS vers du S/MIME (cf. 7.1.4) ; - L'ajout de l'Email dans le SAN des certificats S/MIME (cf. 7.1.4) ; - Ajout des OID du CAB Forum dédiés aux certificats S/MIME (cf. 7.1.4) ; - Précision sur la vérification de l'email des certificats S/MIME (cf. 3.2.2.1.4.1).
4.3	04/03/2024	Révision du document et précisions apportées sur : - L'extension Basic Constraint des certificats TLS (cf. 7.1.4).
4.4	21/03/2024	Révision du document et précisions apportées sur : - L'ajout des AC ACME 2024 et ACME FR 2024 et de leurs certificats (cf. 7.1) ; - L'ajout des AC ACME et ACME FR et de leurs certificats (cf. 7.1).

4.5	27/03/2024	Révision du document et précisions apportées sur : - La révocation des AC ACME 2024 et ACME FR 2024 (cf. 7) ; - La révocation des AC ACME et ACME FR (cf. 7) ; - L'ajout des AC ACME G1 et ACME FR G1 et de leurs certificats (cf. 7.1) ; - L'ajout des AC ACME G2 et ACME FR G2 et de leurs certificats (cf. 7.1).
4.6	05/04/2024	Révision du document et précisions apportées sur : - Les certificats d'authentification client (cf. 7).
4.7	25/06/2024	Révision du document et précisions apportées sur : - La durée d'utilisation des documents pour l'enregistrement (cf. 4.1.2.2) ; - L'acceptation des certificats en utilisant le service ACME (cf. 4.4.1.2) ; - L'acceptation des CVGU en utilisant le service ACME (cf. 4.5.1) ; - La durée de rétention des dossiers de demande (cf. 9.4.1) ; - Les obligations des RC, Porteurs et demandeurs (cf. 9.6.3 et 9.6.4) ; - L'usage des certificats de test (cf. 9.17.1).
4.8	12/07/2024	Révision du document et précisions apportées sur : - La méthode « Changement apporté au site web – ACME » (cf. 3.2.2.4.19)
4.9	13/09/2024	Révision du document et précisions apportées sur : - Les sections structurées en alignement avec la RFC 3647 ; - La vérification de l'existence opérationnelle de l'entité (cf. 3.2.2.1.3) ; - Les enregistrements CAA (Cf. 3.2.2.8) ; - L'identification et l'authentification sur renouvellement (cf. 3.3.1.2 et 3.3.1.3) ; - Le délai d'utilisation des validations (cf. 4.2.1.2) ; - L'AC n'émet pas de certificat avec un nouveau gTLD (cf. 4.2.2).
5.0	24/09/2024	Révision du document et précisions apportées sur : - Le retrait de la méthode d'email au contact du domaine (cf. 3.2.2.4.2) ; - L'ajout de la méthode d'email au contact DNS TXT (cf. 3.2.2.4.14) ; - La corroboration de l'émission multi-perspective (cf. 3.2.2.9).
5.1	19/03/2025	Regroupement de la PC et DPC dans un même document. Transfert vers les PC/DPC découpées par usage.

www.certigna.com