Certigna

CP/CPS

CERTIFICATE POLICY / CERTIFICATION PRACTICE STATEMENT

CERTIGNA ROOT CA

Last update:	2025-03-19	
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: Public

1 INTRODUCTION

1.1 Document Name and Identification

This CP/CPS can be identified by several OID linked to the root CAs grouped in this 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: This CP/CPS describes the commitments and practices implemented for certificates issued by CERTIGNA Certification Authorities. As recommended by the CA/Browser Forum (http://www.cabforum.org), this CP/CPS has been divided into several CP/CPS:

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	Web authentication (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	Mail signature (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	Code signing
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	 Client authentication Authentification client Document signing Document signing Document signing Time Stamping Encryption Encryption

We invite you to consult these CP/CPS at the following address:

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

1.3 Révision du document

The table below shows the history of this CP/CPS before it was split into several documents.

Ver.	Date	Document change
1.0	03/11/2008	Creation
1.1	01/02/2019	Revision of the graphic chart and commitments.
3.0	03/24/2020	Grouping of CPS from intermediate CAs under this single CPS. New TESSI graphic chart: Precisions about: - Compliance with 319 412 ETSI specifications (see 1.1, 7), - Possible causes for a certificate's revocation (see 4.9.1), - Retention of application files (see 5.5.2.1, 5.5.2.3, 9.4.1), - Punctual uploading of root CAs for LAR (see 6.2.7), - Reimbursement policy (see 9.1.5), - Insurance coverage (see 9.2.1), - Termination (see 9.6.6), - Delivery and Guarantee (see 9.7), - Limitations of liability (see 9.8), - Dispute resolution procedure (see 9.13), - Renunciation and force majeure (see 9.16).
3.1	06/05/2020	Precisions about: - Authentication of CM or Certification Agent (see 3.2.3.2.1 and 3.2.3.4), - SAN field of FR03 certificates (see 7.4.1.2).
3.2	08/24/2020	Reduction of the SSL/TLS certificates lifespan (see 7.4.2 and 7.4.3)
3.3	11/02/2020	Revision of the document and clarifications on: - Areas applicable to the different certificates (see 1.4). - Procedures for validating PC / DPC / CGVU (see 1.5). - Reminder of the face to face applicable for NCP+ certificates (see 3.2.3.3.2). - Description of the SAN OID in FR03 certificates (see 7.5.3.2). - Ordering of fields in the DN of certificates (see 7.5).
3.4	06/14/2021	Revision of the document and clarifications on: - Role of Subscriber (see 1.3.3); - Validation period for domain names (see 3.2.2.4); - CAA DNS records of CERTIGNA (see 3.2.2.8); - Methods for demonstrating the compromise of a key (see 4.9.12); - Strategy for QWAC certificates (see 7.5.4.2); - Protection of personal data (see 9.4.1); - Obligations for CMs and Subjects (see 9.6.3); - Obligations for Subscribers (see 9.6.4).
3.5	12/01/2021	Revision of the document and clarifications on: - URLs for accessing documentations and services, - Suppliers and applicable requirements (see 1.3.6.4), - Methods authorized for wildcard certificates (see 3.2.2.4.6), - Revocation reason for the loss of support qualification (see 4.9.1.1), - QWAC certificate strategy (see 7.5.4.2), - Profile of ARLs with reason for revocation (see 7.9), - The commitment to provide non-discriminatory services (see 9.15).

3.6	09/01/2022	Revision of the document and clarifications on: - Reasons for revocation (see 4.9.1.1), - Revocation of certificates presuming to exist (cf. 4.9.3.2), - Publication of the reasons for revocation (see 4.9.3.2 and 7.8), - New certificate templates in RSA 3072 (see 6.1.5.3 and 7.5), - New QNCP-w certificate templates (see 7.5), - Addition of logs for the SCTs (see 7.5.4.3 and 7.5.5.3).
3.7	11/25/2022	Revision of the document and clarifications on: - Link between CERTIGNA, DHIMYOTIS and TESSI (see 1.1), - URLs used in AIA field (Cf. 7).
3.8	05/22/2023	Revision of the document and clarifications on: - Compliance with S/MIME BR from 09/01/2023 (see 1.1); - Contractual requirements with RA (see 1.3.2) ; - Types of names for S/MIME certificates (see 3.1.1); - Non-ASCII character substitution (see 3.1.4); - Method Agreed-Upon Change to Website v2 (see 3.2.2.4.18); - CAA Records (see 3.2.2.8); - Revocation Reasons (see 4.9.1.2); - OCSP Requirements (see 4.9.10); - Types of events recorded (see 5.4.1); - Incident and compromise handling procedures (see 5.7.1); - The conditions for rejecting a certificate request (see 6.1.1.3); - Stopping the SHA-1 hash signature (see 7.1); - The characteristics of assessments (see 8.1, 8.2, 8.4, 8.6, 8.7).
3.9	09/01/2023	Revision of the document and clarification on: - The method of authorising the domain on a request token (see 3.2.2.4), - The addition of logs for SCTs (see 7.1.4), - Removal of the "Email Protection" ECU for certificates (see 7.1.4), - Addition of the "OrganizationIdentifier" field in certificates (see 7.1.4),
4.0	09/12/2023	Revision of the document and clarification on: - The OID for SSL/TLS client certificates (see 7.1.4), - The "Email Protection" EKU for ID and seal certificates (see 7.1.4), - Removal of the Email of the SAN for ID and seal certificates (see 7.1.4).
4.1	10/11/2023	Revision of the document and clarification on: - Links to the TSL and the LSTI website for the status of qualifications (see 1.1); - FAQ contacts and for any complaints or revocations (see 1.5.2); - Delay within which the response from a CRL differ from the OCSP (see 4.10.1).
4.2	11/06/2023	Revision of the document and clarification on: - The migration of ID RGS**/eIDAS certificates to S/MIME (see 7.1.4), - The addition of the Email to SAN extension for S/MIME certificates (see 7.1.4). - The addition of OIDs dedicated to S/MIME certificates (see 7.1.4), - The method for verifying an e-mail address (see 3.2.2.1.4.1).
4.3	03/04/2024	Revision of the document and clarification on: - Basic Constraint extension of TLS certificates (see 7.1.4).
4.4	03/21/2024	Revision of the document and clarification on: - The addition of ACME CA G1 and ACME FR CA G1 certificates (see 7.1), - The addition of ACME CA and ACME FR CA certificates (see 7.1).

4.5	03/27/2024	Revision of the document and clarification on: - The revocation of ACME 2024 CA and ACME FR CA 2024 certificates (see 7), - The revocation of ACME CA and ACME FR CA certificates (see 7), - The addition of ACME CA G1 and ACME FR CA G1 certificates (see 7.1), - The addition of ACME CA G2 and ACME FR CA G2 certificates (see 7.1).
4.6	04/05/2024	Revision of the document and clarification on: - Client authentication certificates (see 7).
4.7	06/25/2024	Revision of the document and clarification on: - Duration of use of registration documents (see 4.1.2.2); - Acceptance of certificates using ACME service (see 4.4.1.2); - TCSU acceptance using the ACME service (see 4.5.1); - Application file retention period (see 9.4.1); - Obligations of CMs, Subjects and applicants (see 9.6.3 and 9.6.4); - Use of test certificates (see 9.17.1).
4.8	2024-07-12	Revision of the document and clarification on: - "Agreed-Upon Change to Website – ACME" method (see 3.2.2.4.19).
4.9	2024-09-13	Revision of the document and clarification on: - All sections are structured in accordance with section 6 of RFC 3647; - Verification of entity's operational existence (see 3.2.2.1.3); - CAA Records (see 3.2.2.8); - Identification and Authentication for Routine Re-key (see 3.3.1.2 and 3.3.1.3); - Validation usage delay (see 4.2.1.2); - CA does not issue certificate containing a new gTLD (see 4.2.2).
5.0	2024-09-24	Revision of the document and clarification on: - The withdrawal of the Email to domain contact method (see 3.2.2.4.2); - The addition of the Email to DNS TXT contact method (see 3.2.2.4.14); - The information on Multi-Perspective Issuance Corroboration (See 3.2.2.9).
5.1	2025-03-19	Combining CP and CPS in a single document. Transfer of this CP/CPS in several CP/CPS by usage.

www.certigna.com