Certigna

CP/CPS CERTIFICATE POLICY / CERTIFICATION PRACTICE STATEMENT

CERTIGNA TLS WEB SERVER AUTHENTICATION

Last update:	2026-06-11	
Version:	2.2	
OID:	1.2.250.1.177.1.0.1	CERTIGNA
	1.2.250.1.177.2.0.1	CERTIGNA ROOT CA
	1.2.250.1.177.6.0.1.1	CERTIGNA SERVER AUTHENTICATION ROOT CA
	1.2.250.1.177.14.0.1.1	CERTIGNA SERVER AUTHENTICATION EU ROOT CA
Classification:	Public	

SUMMARY

1 INTRODUCTION 5

1.1 Overview 5

1.2 Document Name and Identification 6

1.3 PKI Participants 9

1.4 Certificate Usage 13

1.5 Policy Administration 14

1.6 Definitions and Acronyms 15

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 22

2.1 Repositories 22

2.2 Publication of Certification Information 22

2.3 Time or Frequency of Publication 25

2.4 Access Controls on Repositories 26

3 IDENTIFICATION AND AUTHENTICATION 27

3.1 Naming 27

3.2 Initial identity validation 28

3.3 Identification and Authentication for Re-key Requests 48

3.4 Identification and authentication for revocation request 49

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 50

4.1 Certificate Application 50

4.2 Certificate Application Processing 51

4.3 Certificate Issuance 53

4.4 Certificate Acceptance 55

4.5 Key Pair and Certificate Usage 56

4.6 Certificate Renewal 56

4.7 Certificate Re-key 57

4.8 Certificate modification 58

4.9 Certificate Revocation and Suspension 59

4.10 Certificate Status Service 68

4.11 End of Subscription 68

4.12 Key Escrow and Recovery 69

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 70
5.1 Physical Controls 71
5.2 Procedural Controls 73
5.3 Personnel Controls 74
5.4 Audit Logging Procedures 76
5.5 Records Archival 80
5.6 Key Changeover 82
5.7 Compromise and Disaster Recovery 83
5.8 CA or RA Termination 86

6 TECHNICAL SECURITY CONTROLS 88
6.1 Key Pair Generation and Installation 88
6.2 Private Key Protection and Cryptographic Module Engineering Controls 92
6.3 Other Aspects of Key Pair Management 95
6.4 Activation Data 96
6.5 Computer Security Controls 97
6.6 Life Cycle Technical Controls 97
6.7 Network Security Controls 98
6.8 Time-stamping 98

7 CERTIFICATE AND CRL PROFILES 99
7.1 Certificate profile 99
7.2 Profile of CRL 134
7.3 OCSP Profile 138

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT 142
8.1 Frequency or Circumstances of Assessment 142
8.2 Identity/Qualifications of Assessor 142
8.3 Assessor's Relationship to Assessed Entity 143
8.4 Topics Covered by Assessment 143
8.5 Actions Taken as a Result of Deficiency 143
8.6 Communication of Results 144
8.7 Self-Audits 144

9 OTHER BUSINESS AND LEGAL MATTERS 146

9.1 Fees 146
9.2 Financial Responsibility 146
9.3 Confidentiality of Business Information 147
9.4 Privacy of Personal Information 148
9.5 Intellectual Property Rights 149
9.6 Representations and Warranties 149
9.7 Disclaimers of Warranties 155
9.8 Limitations of Liability 155
9.9 Indemnities 156
9.10 Term and Termination 157
9.11 Individual Notices and Communications with Participants 157
9.12 Amendments 157
9.13 Dispute Resolution Provisions 158
9.14 Governing Law 159
9.15 Compliance with Applicable Law 159
9.16 Miscellaneous Provisions 159
9.17 Other Provisions 160

10 APPENDIX 1: SECURITY REQUIREMENTS FOR THE CA'S CRYPTOGRAPHIC MODULE 161
10.1 Security Objectives Requirements 161
10.2 Qualification Requirements 161

11 APPENDIX 2: SECURITY REQUIREMENTS FOR THE DEVISE USED BY THE CM 162
11.1 Security objectives requirements 162
11.2 Qualification Requirements 162

1 INTRODUCTION

1.1 Overview

CERTIGNA, formerly DHIMYOTIS, is a TESSI group company which specializes in providing digital trust services.

CERTIGNA has set up several Certification Authority (CA) to provide electronic certificates to legal and natural persons. This document is the Certificate Policy/Certification Practice Statement (CP/CPS) outlines the practices that CERTIGNA applies and undertakes to comply in the delivery of its electronic certification services. The reader's attention is drawn to the fact that the understanding of this CP/CPS guess he is familiar with the concepts related to the technology of Public Key Infrastructure (PKI).

CERTIGNA is audited by LSTI, a French certification body. The status of CERTIGNA's product qualifications and certifications can be consulted on the following websites:
- RGS Qualifications and ETSI certifications: Link to the LSTI website
- eIDAS Qualifications: Link to the European TSL

This CP/CPS aims to comply:
- with the latest version of the « Baseline Requirements documents (SSL/TLS Server Certificates) » and the « EV Guidelines for TLS Server certificate » from the CA/Browser Forum (http://www.cabforum.org),
- with the latest version of the of CCADB and Browser policies:
  - CCADB Policy: Link to policy
  - Mozilla Root Store Policy: Link to policy
  - Microsoft Trusted Root Program: Link to policy
  - Chrome Root Program Policy: Link to policy
  - Apple Root Certificate Program: Link to policy
- with the following standards and security levels.

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

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

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

In the event of any inconsistency between this CP/CPS and those Requirements, those Requirements take precedence over this CP/CPS.

This CP/CPS is available in PDF and Markdown formats. The PDF version of the CP/CPS is the reference version.

TLS certificates covered by this CP/CPS will no longer be officially recognized by all web browsers from September 15, 2026.

1.2 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
- 1.2.250.1.177.6.0.1.1 CERTIGNA SERVER AUTHENTICATION ROOT CA
- 1.2.250.1.177.14.0.1.1 CERTIGNA SERVER AUTHENTICATION EU ROOT CA

Intermediate and final CA certificates issued under each root CA also have an OID that clearly identifies the practices of this applicable CP/CPS.

1.2.1 Revisions

This CP/CPS brings together all the CPs and CPSs of the various root and intermediate CAs used to issue web server authentication certificates. To facilitate access to information, it was decided to group all these documents together in a single CP/CPS. The table below shows the history of the previous versions of the CP and CPS grouped together in this document, which can be consulted on the following page: https://www.certigna.com/autorites-de-certification/

Ver.	Date	Document change

1.0	2024-04-05	Creation of this CPS dedicated to Server Authentication CAs
		- Integration of our new SERVER AUTHENTICATION CAs
		- Integration of historical CAs:
		  o CERTIGNA and associated CA and end-entity certificates,
		  o CERTIGNA ROOT CA and associated CA and end-entity certificates.

1.1	2024-06-25	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).
1.2	2024-07-12	Revision of the document and clarification on: - "Agreed-Upon Change to Website – ACME" method (see 3.2.2.4.19).
1.3	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), - Validation usage delay (see 4.2.1.2), - CA does not issue certificate containing a new gTLD (see 4.2.2).
1.4	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).
1.5	2025-03-19	Combining CP and CPS in a single document. Transfer of TLS CAs from "Certigna Root CA" CP/CPS to this document. Revision of the document and clarification on: - The addition of new certificate profiles, - The router and firewall activities logging SC69 (See 5.4.1.1), - The compromised and weak keys SC73 (see 6.1.1.3), - The implementation of a linting process SC75 (See 4.3, 6.6.1, 8.7), - The multi-perspective issuance corroboration SC67 (See 3.2.2.9, 5.4.1), - The content of "OrganizationName" field SC78 (See 3.2.2.2), - The requirements for OCSP SC76 (See 4.9.10), - The retention period for application files (see 5.5.2.1).
1.6	2025-04-22	Revision of the document and clarification on: - RGS web authentication certificate profiles under ACME (see 7.1.12.9, 7.1.12.10), - Revocation status beyond end of validity (see 5.8.3), - The retention period for application files and logs (see 5.5.2, 9.4.1).
1.7	2025-05-20	Revision of the document and clarification on: - Withdrawal of CA revoked in may 2025.
1.8	2025-09-08	Revision of the document and clarification on: - Validity period of certificates and data reuse (see 4.2.1 and 6.3.2), - The use of DNSSEC (see 3.2.2.4, 3.2.2.8.1), - Mass certificate revocation (see 5.7.1.2).

1.9	2025-09-18	Revision of the document and clarification on: - Creation of a Markdown version of the CP/CPS in English, - Typographical corrections.
2.0	2025-12-12	Revision of the document and clarification on: - Compliance with CCADB and Browser policies (see 1.1), - Cross-signing of Certigna Root CA by Certigna (see 7).
2.1	2026-03-11	Revision of the document and clarification on: - The practices for accessing publication servers (see 2.4), - The use of DNSSEC (see 3.2.2.4), - The use of domain control methods (see 3.2.2.4.4 and 3.2.2.4.14), - The maximum interval between two system configuration checks (see 6.5.1), - The AIA field of cross-signed intermediate CAs (see 7.12.6 and 7.12.7), - The revocation of RSASSA-PKCS1-v1_5 with SHA-1 CA certificates (see 7.1.3.2.1).
2.2	2026-06-11	Revision of the document and clarification on: - Browsers no longer recognize our TLS certificates (see 1.1), - Addition of a list of RFC references (see 1.6.3), - Addition of sections related to new control methods (see 3.2.2.4.21, 3.2.2.4.22), - The addition of certificate not issued with a reverse IP zone suffix (see 4.2.2), - Reasons for Revoking a Legal Person Certificate (see 4.9.1.1), - CRL Issuance Frequency (see 4.9.7), - On-line Revocation Checking Requirements (see 4.9.9), - Facility, management, and operational controls (see 5), - Types of Events Recorded (see 5.4.1), - Withdrawal of unmarketed PSD2 certificates and associated references

1.3 PKI Participants

1.3.1 Certification authorities

The CA is responsible for the provision of certificate management services throughout their life cycle (generation, distribution, renewal, revocation, ...) and relies on a technical infrastructure: a PKI. The CA is responsible for the implementation of the CP/CPS to the PKI set in place. For certificates signed in its name, the CA has the following functions:

- Registration and renewal functions;
- Certificate generation function;
- Secret generation function;
- Publication function of the general conditions of the CP/CPS, CA certificates and certificate application forms;
- Revocation management function;
- Information function on the status of certificates via the Certificate Revocation List (CRL) updated at regular intervals and in a query mode / real-time response (OCSP).

The CA provides these functions directly or outsourcing them, some or all. In all cases, the CA retains responsibility. CA is committed to respecting the obligations described in this CP/CPS. It is also committed that the components of the PKI, internal or external to the CA, which they incumbent also respect them.

Finally, the parties of the CA concerned with certificate generation and revocation management are independent from other organizations regarding their decisions on the establishment, supply, maintenance and suspension of services; managers, support personnel and personnel with trusted roles are free from any pressure from commercial, financial or otherwise, could adversely affect the confidence in the services provided by the CA. The parties of the CA concerned with certificate generation and revocation management have a documented structure, which safeguards impartiality of operations.

1.3.2 Registration authorities

Registration authority provides the following functions, delegated by the CA under this CP/CPS:

- The acquisition and verification of future information of Certificate Manager (CM) and his/her entity and the constitution of the corresponding registration files;
- The acquisition and verification of information, if applicable, of the future certification agent (*) and his/her business entity and the constitution of the corresponding registration files;
- The establishment and transmission of the certificate request to the CA;
- The archiving of the certificate request files;
- Conservation and protection of confidentiality and integrity of personal authentication data of the Certificate Manager or of the Certification Agent;
- Verification of certificate revocation requests.

The RA performs these functions directly or with the contribution of Delegate Registration Authorities. In all cases, the RA remains responsible and the archiving of the registration files (electronic and / or paper) is the responsibility of the RA.

Before the CA authorizes a Delegated Third Party to perform a delegated function, the CA contractually requires the Delegated Third Party to:

- Meet the qualification requirements of Section 5.3, when applicable to the delegated function;
- Retain documentation in accordance with Section 5.5.2 of this CP/CPS;
- Abide by the other provisions of these Requirements that are applicable to the delegated function; and
- Comply with the CA's CP/CPS or the Delegated Third Party's practice statement that the CA has verified complies with these requirements.

Unless stated otherwise, in this document, "RA" covers the Registration Authority and Delegated Registration Authorities.

(*): The RA offers the possibility to the client entity to use a designated Certification Agent who is under its responsibility to carry out all or part of the information verification. In this case, the RA ensures that applications are complete and carried out by an authorized Certification Agent.

The CA does not designate an Enterprise RA to verify certificate requests from the Enterprise RA's own organization.

1.3.3 Subscribers

A Subscriber is a natural person attached or not to the entity designated in the requested certificate, who orders one or more certificates for himself or in the name of a Certificate Manager. A Subscriber is responsible for the obligations incumbent on the Subscribers, as well as those incumbent on the Certificate Manager, if applicable.

1.3.4 Certificate Manager

We will refer to the "Certificate Manager" (CM) when the issued certificate is intended for an application service or a server, such as a seal service or a web server. The CM is the person in charge of managing the certificate but is not explicitly designated in this legal person certificate. The CM must meet the conditions and obligations that are set in the CP/CPS and in the Terms and Conditions of Sale and Use (TCSU).

1.3.4.1 Certificate Manager for a CA

For the root CA and the intermediate CAs, the CM can only be the CERTIGNA Certification Authority.

1.3.4.2 Certificate Manager for a web server

CM can only be a natural person. It is responsible for the use of the certificate (and associated private key) in which the application service or the web server concerned is identified and the entity for which he/she uses the certificate and with which it maintains a contractual / reporting relationship / regulatory. The certificate is attached to the web server and not to the CM. In case of change of CM, the entity shall report it to the CA and appoint a successor. The CA revokes certificates for which there is no more CM explicitly identified.

1.3.5 Relying Parties

Certificate users must take all the precautions described in this CP/CPS as well as in the TCSU.

1.3.5.1 CA Certificate

Root CAs
Entity or physical person who uses a CA certificate and trusts it to verify the origin and the validity of a certificate issued by this CA.
Intermediate CAs
Entity or physical person who uses an intermediate CA certificate and trusts it to verify the origin and the validity of a certificate issued by this CA.

1.3.5.2 Legal Person Certificate

An electronic web authentication certificate user can be:

- A person accessing to a server and using the server certificate and an authentication verification module to authenticate the server it is accessing, which is identified in the server certificate to establish a session key shared between his/her system and the server;
- An application service accessing to a server and using the server certificate and an authentication verification module to authenticate the server it is accessing, which is identified in the server certificate to establish a session key shared between the servers.

1.3.6 Other Participants

1.3.6.1 Delegated Registration Authority

CA also relies on Delegated Registration Authorities (DRA) to outsource a part of RA's functions. A DRA operator has the power to:

- process a certificate generation or renewal;
- process a certificate revocation;
- record, if appropriate, the Certification Agents belonging to the entities which request certificates.

A DRA operator performs for the authority, in the context of issuance of the certificate, the verification of future CM identity under the same conditions and with the same level of safety as those required for the RA operator. For this it is directly related to RA.

The commitments of the DRA operator against CA are specified in a written agreement with the responsible entity of the operator and in the commitment letter to be signed by the latter. Both documents include state that the operator must perform impartial and scrupulous verification of the identity and of the possible future CM attributes and application services. He/she must also respect the parts of this CP/CPS incumbent on him.

1.3.6.2 Certification Agent

CA offers the opportunity for the client's entity to designate one or more Certification Agents. The Certification agent has, by law or by delegation, the power to:

- request a certificate generation or renewal certificate on behalf of the entity;
- request a certificate revocation on behalf of the entity.

The certification agent can be a legal representative of the entity or any person that the latter has formally designated. He or she provides for the CA, in the context of the issuance of certificates, the identity verification of future Certificate Managers under the same conditions and with the same level of safety as those required for the RA operator. For this it is directly in contact with the Registration Authority.

The commitments of the Certification Agent in respect of the CA are specified in a written agreement with the entity responsible of the Certification Agent and in the commitment letter to be signed by the Certification Agent. Both documents specify that the Certification Agent must perform impartial and scrupulous verification of the identity and of the possible future CM attributes and application services. He/she must also respect the parts of this CP/CPS incumbent on him.

The entity shall promptly report to CA, the Certification Agent's departure from office and possibly appoint a successor. The Certification Agent shall not have access to the private key activation data associated with the certificate issued to CM.

1.3.6.3 Customer service

To ensure a responsive service that meets requirements, Certigna can use a provider specializing in "Customer services" to assist its prospects and customers in their requests relating to certificates. To this end, the operators of this entity are recruited as operator of DRA to allow them to access the application files and to assist subscribers in their procedures.

A contract of DRA is established with the entity in charge of this service. The provider thus undertakes to respect the parts of this CP/CPS incumbent on him/her, and in particular the commitments of Chapters 3 and 4.

1.3.6.4 Hosts of the technical infrastructure

Certigna may use a provider for the physical hosting of its technical infrastructure. A contract is established with the provider to guarantee the security of the services in accordance with the commitments of chapter 5.1 of this CP/CPS.

1.3.6.5 Providers of cryptographic device

The cryptographic device, delivered, if necessary, by Certigna to the CM, to store and use the private key and the certificate, can be acquired from a supplier with whom a contract is established aiming to guarantee the conformity of the cryptographic device with a or several qualifications and / or certifications cited in chapter 11 of the Certification Policy.

Despite these provisions, it is important to remember that if one of these qualifications or certifications is no longer maintained or suspended for reasons such as the identification of a vulnerability or the cessation of production of the product, Certigna will inform the CM and revoke their certificate, without any condition of reimbursement.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

QNCP-w / QEVP-w
The electronic certificates are used for applications where security needs are very strong given the high risks that threaten them.
OVCP
The electronic certificates are used for applications where security needs are strong given the high risks that threaten them.
RGS *
The electronic certificates are used for applications where security needs are moderate given the risks that threaten them.

1.4.1.1 CA Certificate

Root CA
The root CA key pair is used for signing intermediate CA certificates and Authorities Revocation Lists (ARLs).
Intermediate CAs
The intermediate CA key pair is used for signing final certificates and Certificate Revocation Lists (CRLs).

1.4.1.2 Legal Person Certificate

Server authentication from other servers or person, as part of establishing secure sessions, such as SSL / TLS or IPsec to establish a symmetric session key to encrypt the exchanges in this session. The establishment of the session key can be done by an RSA or type Diffie-Hellman asymmetric cryptographic mechanism (obtaining the symmetric key using an algorithm combining the client private key and public key of the server, and inversely.

1.4.2 Prohibited Certificate Uses

Uses other than those mentioned in the previous paragraph are prohibited. The CA agrees to comply with these restrictions and to enforce compliance by Certificate Managers and certificate users. To this end, it publishes to the CM, Certification Agent and potential users the TCSU that can be found on the site https://www.certigna.com before any request or use of a certificate.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The CA has a Security Committee responsible for the development, monitoring and modification of this CP/CPS. It shall act on any necessary changes to be made to this CP/CPS at regular intervals.

The formal validation of this CP/CPS and the TCSU is ensured at a minimum by one person in a trusted role of controller and one person in a trusted role of security officer.

1.5.2 Contact Person

1.5.2.1 FAQs et customer support

Answers to frequently asked questions can be found in our FAQ section at https://www.certigna.com/faq/.

If you have any other questions, you can contact our Customer Service department as follows:
- Contact e-mail: contact@certigna.fr ;
- Telephone: 0 806 115 115 (Free service) available Monday to Friday from 09:00 to 18:00;
- Chat on the https://www.certigna.com website, available Monday to Friday from 09:00 to 18:00.

1.5.2.2 Requesting a revocation

As mentioned in chapter 3.4.2, the certificate revocation request by the CM, a legal representative of the entity, a DRA operator or, where applicable, a CA, can be made in one of the following ways:
- From the customer area of the CERTIGNA website https://www.certigna.com by selecting the certificate to be revoked.
- By post: by completing and signing the certificate revocation form available on the CERTIGNA website https://www.certigna.com. The applicant authenticates himself by attaching a photocopy of his identity document to the mail sent.

Information on the processing of your personal data is available in the Policy on the use of personal data, which can be accessed at the following address: https://www.certigna.com/politique-dutilisation-des-donnees-personnelles/.

1.5.2.3 Reporting a malicious or dangerous certificate

For reporting a malicious or dangerous certificate (suspected Private Key compromise, certificate misuse, or other types of fraud, compromise, inappropriate conduct, etc.) or any other matter related to certificates, use the contact form available at https://www.certigna.com/contactez-nous/ by selecting "Certificate considered malicious or dangerous".

1.5.2.4 Making a complaint

To bring a complaint to CERTIGNA's attention, please use the contact form available at the following address https://www.certigna.com/contactez-nous/ and select the "Réclamation" reason.

You can also make a complaint to our customer service department using the following contact details:
- Contact e-mail : contact@certigna.fr ;
- Telephone: 0 806 115 115 (Free service) available Monday to Friday from 09:00 to 18:00.
- Chat on the https://www.certigna.com website, available Monday to Friday from 09:00 to 18:00.
- Mail addressed to

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

Information on the processing of your personal data is available in the Policy on the use of personal data, which can be accessed at the following address: https://www.certigna.com/politique-dutilisation-des-donnees-personnelles/.

1.5.3 Person Determining CPS Suitability for the Policy

The Security Committee ensures the compliance of this CP/CPS. IT can optionally be assisted by external experts to ensure compliance.

1.5.4 CPS approval procedures

Initially, the CPS translates into technical, organizational, and procedural terms the requirements of the CP based on the company's “Information security policy”. The Security Committee shall ensure that the means used and described in this CP/CPS meet these requirements as the approval process in place. A compliance check of the CP/CPS is made through the internal and external audits for the CA qualification. Any update request of the CP/CPS also follows this process. Any new approved version of the CP/CPS is published without delay.

1.6 Definitions and Acronyms

1.6.1 Definitions

Useful terms to the understanding of the CP/CPS are the followings:

Affiliate - A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Administrative authorities - This term refers to government departments, local authorities, public administrative institutions, the bodies administering social protection systems and other bodies responsible for the management of an administrative public service.

Agent – Individual acting on behalf of an administrative authority.

Application Developer - A manager of a service of the public sphere electronically accessible.

Audit Report - A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the applicable requirements.

Authorities Revocation List - List including the serial numbers of the certificates of intermediate authorities which have been revoked, and signed by the root CA.

Business Entity: Any entity that is not a Private Organization, Government Entity, or Non-Commercial Entity as defined herein. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.

Certification Authority Authorization (CAA) - From RFC 8659, the CAA DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue.

Certification Authority - In a CSP, a Certification Authority is responsible, on behalf and under the responsibility of this CSP, applying at least one certification policy and is identified as such, as an issuer («issuer" field of the certificate).

Certificate Manager - Person in charge and responsible of the electronic certificate used by an application service.

Certification Policy - A set of rules, identified by a name (OID), defining the requirements that a CA comply in the implementation and delivery of its services and indicating the applicability of a certificate to a specific community and / or a class of applications with common security requirements. A CP can also, if necessary, identify the obligations and requirements on other stakeholders including CM and certificate users.

Certification Practice Statement - A CPS identifies practices (organization, operational procedures, technical and human resources) that the CA applies under the provision of its certification services to users and in accordance with the policies or certification that it has committed.

Certificate revocation list - List including serial numbers of certificates that have been revoked, and signed by the issuing CA.

Certification service provider - Any person or entity who is responsible for the management of electronic certificates throughout their life cycle, towards the CM and users of these certificates.

Certificate user - Entity or natural person who uses a certificate which it relies on to verify an electronic

signature or an authentication value from a certificate holder or encrypt data to a certificate holder.

Component - Platform operated by an entity and comprised of at least one computer station, an application and, where applicable, cryptographic means. Component play a specific role in the operational implementation of at least one function of PKI. The entity may be the CSP itself or an external entity related to CSP contractual, regulatory or hierarchical.

Cross Certificate - A certificate that is used to establish a trust relationship between two Root CAs.

CSPRNG - A random number generator intended for use in a cryptographic system.

Electronic Certificate - Electronic file certifying the link between a public key and the identity of its owner (natural or legal person or system). This certificate takes the form of an electronic signature made by a CSP. It is issued by a CA. The certificate is valid for a given period specified therein.

Electronic Seal - Digital Seal done by an application server with data to be used either as part of an authentication service data origin, as part of a service non-repudiation.

Entity - Means an administrative authority or a company in the broadest sense, namely also legal persons of private law type associations. It can be a Private Organization, Government Entity, Business Entity, or Non-Commercial Entity.

FQDN - Fully qualified domain name indicating the absolute position of a node in the DNS tree and specifying the top-level domains to the root.

Information System - Any set of means to develop, process, store or transmit information subject to electronic exchange between users and administrative authorities and between administrative authorities.

Jurisdiction of Incorporation - In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

Jurisdiction of Registration - In the case of a Business Entity, the state, province, or locality where the organization has registered its business presence by means of filings by a Principal Individual involved in the business.

Legal existence - A Private Organization, Government Entity, Business Entity or Non-Commercial Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.

Legal representative (principal individual) - An individual of a Private Organization, Government Entity, or Business Entity who is either an owner, partner, managing member, director, or officer, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance, and use of certificates.

Linting - A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined by the CA\Browser Forum Baselines Requirements.

Multi-Perspective Issuance Corroboration - A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.

Network Perspective - Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.

Online Certificate Status Protocol (OCSP) - An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate.

Primary Network Perspective - Network Perspective used by the CA to make the determination of:

- the CA's authority to issue a Certificate for the requested domain(s) and
- the Applicant's authority and/or domain authorization or control of the requested domain(s).

Private Key - The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Private organization - A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation. In France, incorporation is done with Business and Society Register.

Protection device secret elements - Refers to a storage device of secret elements given to CM (e.g. private key, PIN, ...). It can take the form of a smart card, USB key with cryptographic capability or report to software format (ex. PKCS # 12 file).

Public Key Infrastructure - Components, functions and procedures dedicated to the management of cryptographic keys and certificates used for trusted services. PKI can be composed of a CA, a certification operator, a centralized registration authority and / or local certification agents, an archiving entity, a publishing entity, ...

Qualification of electronic certification service provider - The RGS Decree and eIDAS Regulation describe the CSP qualification procedure. A CSP being a specific Trust Service Provider, the qualification of a CSP is an act by which a certification body certifies the compliance of all, or part of the electronic certification service provided by a CSP (family of certificates) to certain requirements of a CP for a given level of security and for the service covered by the certificates.

Qualification of a security product - Act by which ANSSI attests to the ability of a product to ensure with a given level of robustness, security features purpose of qualification. The qualification certificate states in the ability of the product to participate in the realization at some level of security of one or more functions covered in the RGS. The qualification procedure for security products is described in the decree RGS. The RGS specifies three qualification process: basic level qualification, standard level qualification and level strengthened qualification.

Qualified Government Information Source (QGIS) - A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided that it is maintained by a Government Entity, the reporting of data is required by law, and false or misleading reporting is punishable with criminal or civil penalties.

Qualified Government Tax Information Source (QTIS) - An Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals.

Qualified Independent Information Source (QIIS) - A regularly-updated and publicly available database that is generally recognized as a reliable source for certain information.

RSA - Public key algorithm (Rivest, Shamir and Adleman).

Security product - a software or hardware that implements security features necessary for securing information or system.

Seal verification application - This is the application implemented by the user to check the seal of the data received from the server's public key contained in the certificate.

Timestamping Authority - Authority responsible for the management of a timestamp service.

User - Individuals acting for its own account or on behalf of a corporation and making electronic communications with administrative authorities.

User applications - Application services operating certificates issued for the Certification Authority seal service needs which the certificate is associated.

Note - An agent of an administrative authority which conducts electronic exchange with another administrative authority is, for the latter, a user.
Note - The term "entity" is used to designate a company or an administration. The name "enterprise" covers enterprises in the broadest sense, namely all legal persons governed by private law: companies, associations as well as craftsmen and self-employed workers.

1.6.2 Acronyms

Useful abbreviations for the understanding of this CP/CPS are the followings:

AA	Administrative Authority
ACME	Automatic Certificate Management Environment

ANSSI	French National agency for Information system security
ARL	Authority Revocation List
BCP	Business Continuity Plan
CA	Certification Authority
CAA	Certification Authority Authorization
CAG	Certification Agent
CM	Certificate Manager
CNIL	National Commission for Computing and Liberties
CP	Certification Policy
CPS	Certification Practice Statement
CRL	Certificate revocation list
CSP	Certification Service Provider
CSR	Certificate Signing Request
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
DRA	Delegate Registration Authority
EBA	European Banking Authority
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
ICD	International Code Designator
INPI	National Institute of Industrial Property
ISMS	Information Security Management System
ISS	Information systems security
NCA	National Competent Authority
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PP	Protection Profile
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure
PSP	Payment Service Provider
RA	Registration Authority
RSA	Rivest Shamir Adleman
SCT	Signed Certificate Timestamp
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TCSU	Terms and Conditions of Sale and Use
TLS	Transport Layer Security
TSP	Trust Service Provider
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

1.6.3 References

RGS Appendix A3, National Agency for Information System Security (ANSSI); General Security Framework; Appendix A3: Standard certification policy for "electronic application service certificates".

ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

RFC 3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.

RFC 4035, Request for Comments: 4035, Protocol Modifications for the DNS Security Extensions.

RFC 4509, Request for Comments: 4509, Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs).

RFC 5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments.

RFC 5155, Request for Comments: 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence.

RFC 5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL).

RFC 5702, Request for Comments: 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC.

RFC 6840, Request for Comments: 6840, Clarifications and Implementation Notes for DNS Security (DNSSEC).

RFC 6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol- OCSP.

RFC 6962, Request for Comments: 6962, Certificate Transparency.

RFC 7231, Request For Comments: 7231, Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content.

RFC 7538, Request For Comments: 7538, The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect).

RFC 8555, Request for Comments: 8555, Automatic Certificate Management Environment (ACME).

RFC 8659, Request for Comments: 8659, DNS Certification Authority Authorization (CAA) Resource Record.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

The CA develops, implements, enforces, and at least once every 366 days update this CP/CPS that describes in detail how the CA implements the latest version of applicable Requirements.

2.1 Repositories

2.1.1 Entity in charge of providing information

The CA provides to users and applications using certificates it issues, information about the revocation status of valid certificates issued by the CA.

2.1.2 Information to be Published

The CA issues to the CM, Subjects and certificate users:

- The CP/CPS;
- The Terms and Conditions of Sale and Use (TCSU) of CA certification services;
- The various forms required for certificate management (certificate request, revocation request);
- The Root CA certificate and valid intermediate CA certificates;
- The Certificate Revocation List (ARL / CRL);

Note: Due to the complexity of reading a CP for Certificate Managers or users not experts in the field, the CA publishes outside the CP, the CPS and TCSU that the future CM or Subjects is obliged to read and to accept in all certificate request (initial and subsequent requests, in case of renewal) to the RA.

2.2 Publication of Certification Information

The CP/CPS is structured in accordance with RFC 3647. The CP/CPS and TCSU are annually updated.

2.2.1 Publication of CP, Terms and conditions, and forms

The CP/CPS, the TCSU, and the various forms required for certificate management are published in electronic format at http://cps.certigna.com.

2.2.2 Publication of CPS

The CA issues, to the CM and certificate users, the CPS to make possible the assessment of compliance with this CP/CPS. Sensitive details on its practices are however not made public.

2.2.3 Publication of CA Certificate

The CM and certificate users can access the CA certificates that are issued at the following URL https://www.certigna.com/autorites-de-certification/ or directly via the following URLs.

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

All publication services are hosted by the CA on several information systems to ensure a high availability. To detect and correct as soon as possible any incident occurring during the operation of one of these sites, the following measures have been deployed:

- Introduction of on-call during non-business hours.
- Subscription to a security monitoring service (24 hours a day).
- Installation and operation of a monitoring software to monitor all the components of the technical platform (servers, equipment, processes) and to send real-time alerts in case of detection of an incident.
- Development and implementation of scripts to automate and simplify load balancing from one site to another.

2.2.4 Publication of Test Certificates

For web authentication certificates, test certificates are published to allow user applications such as browsers to test their interpretation of the status of certificates.

CERTIGNA SERVER AUTHENTICATION ROOT CA	
Valid certificate	https://valid.serverauthenticationovcpca.certigna.com
Expired certificate	https://expired.serverauthenticationovcpca.certigna.com
Revoked certificate	https://revoked.serverauthenticationovcpca.certigna.com
CERTIGNA SERVER AUTHENTICATION EU ROOT CA	
Valid certificate	https://valid.serverauthenticationovcpeuca.certigna.com
Expired certificate	https://expired.serverauthenticationovcpeuca.certigna.com
Revoked certificate	https://revoked.serverauthenticationovcpeuca.certigna.com
CERTIGNA	
Valid certificate	https://valid.servicesca-racine.dhimyotis.com
Expired certificate	https://expired.servicesca-racine.dhimyotis.com
Revoked certificate	https://revoked.servicesca-racine.dhimyotis.com
CERTIGNA ROOT CA	
Valid certificate	https://valid.servicesca.dhimyotis.com
Expired certificate	https://expired.servicesca.dhimyotis.com
Revoked certificate	https://revoked.servicesca.dhimyotis.com

2.2.5 Publication of LAR

The Authority certificate revocation list is published electronically at the URLs described in the table above. These URLs are also indicated in the certificates.

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

2.2.6 Publication of CRL

The certificate revocation list is published electronically at the URLs described in the table above. These URLs are also indicated in the certificates issued by the CA.

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

2.3 Time or Frequency of Publication

2.3.1 Publication of documentation

The CP/CPS, the TCSU and the various forms required for certificate management are annually updated, if necessary, to ensure consistency at any time between the published information and the CA's actual commitments, means and procedures. These documents are available on a 24x7 basis. The publication function based on this information (excluding certificate status information) is available on workdays.

2.3.2 Publication of CA certificates

CA certificates are published prior to any publication of certificates issued by the CA and corresponding CRLs. Availability of systems publishing CA certificates is guaranteed 24/7 on a 24x7 basis.

2.3.3 Publication of ARL

The ARL is updated at least once every year, and at each new revocation.

2.3.4 Publication of CRL

The CRL is updated at least every 24 hours, and at each new revocation.

2.4 Access Controls on Repositories

Access to information published to users is free. Access to change the publishing systems (add, delete, change the information published) is strictly limited to authorized internal functions of the PKI, through a strong access control, based on a two-factor authentication.

The CP/CPS, and the TCSU are published in a read-only manner.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

In each certificate compliant with X.509 Standard, the issuing CA (corresponding to the "issuer" field) and the legal or natural person ("subject" field) are identified by a "Distinguished Name" conform with the requirements of the X.501 Standard.

3.1.2 Need for Names to Be Meaningful

The certificate DN identifies the legal or natural person and is built from the identity of the service, the server or the Subject specified in his/her identity document provided during the registration with the RA or the Certification Agent.

The DN format is defined at chapter "7.2 Profile of certificates and CRL" of this CP/CPS.

3.1.3 Anonymity or Pseudonymity of Subscribers

The CA does not issue certificates with an anonymous identity.

3.1.4 Rules for Interpreting Various Name Forms

3.1.5 Uniqueness of Names

Note: The attribute serialNumber present in the DN field and the certificate serialNumber field are distinct data.

3.1.5.1 CA Certificate

CA ensure that names positioned in the CN field of Intermediate CA certificates are unique in the CA perimeter.

3.1.5.2 Legal Person Certificate

The combination of the country, the entity and the FQDN uniquely identifies the certificate holder. Throughout the lifetime of the CA, the name of the server attached to an entity cannot be assigned to another entity.

EN 319 411-1 OVCP
The "serialNumber" attribute, unique value assigned to each certificate issued by the CA and present in the DN, also ensures the uniqueness of the DN. This field is made up from a unique random number generated by the CA and begin with a letter which indicates certificate's usage(s) and its storage mode: - "C" for « Client authentication », - "S" for « Server authentication ».
EN 319 411-2 QNCP-w EN 319 411-2 QEVCP-w
The "serialNumber" attribute is constituted with the entity's registration number.

3.1.6 Recognition, Authentication, and Role of Trademarks

The CA is responsible for the uniqueness of the names of legal person used in its certificates and the resolution of disputes over the demand for use of a name. This commitment of responsibility rests on the assured level of control when processing license applications. The CA may possibly check the membership of the trademark with the INPI.

3.2 Initial identity validation

Registering a CM can be done either directly from the RA (RA or DRA) or via a Certification Agent of the entity. In the latter case, the Certification Agent must first be registered with the RA.

During the certificate request, the email address of the CM is verified through sending multiple emails that allow the CM to access to his/her CERTIGNA or DRA customer account and certain activation data enabling him/her to recover and to use its certificate.

The RA verifies that the entity has an operational existence by checking the QIIS or the QTIS in order to make sure that the entity appears there.

The certificate request can be communicated to the RA or the DRA in paper format signed by hand by the CM and the co-signers. The request can also be communicated to the RA or the DRA in electronic format under the following conditions:

EN 319 411-2 QNCP-w EN 319 411-2 QEVCP-w
In electronic format if signed by each signatory using a qualified electronic signature certificate within the meaning of the eIDAS Regulation. The certificate must be valid when registering by the RA.
EN 319 411-1 OVCP RGS *
In electronic format, if possible, signed using an electronic signature process that meets at least the requirements of the RGS level *.

3.2.1 Method to Prove Possession of Private Key

CA ensures the detention of the private key by the CM before certifying the public key. For this, the RA, the CM generates the key pair in a device compliant with the requirements of the chapter 11 and provides to the CA the proof of possession of the private key by signing his certificate request (Certificate signing request with the PKCS # 10 format). The RA verifies beforehand the validity of the signature during the processing of the certificate requests received. This treatment is automated and therefore requires no human intervention. Any signature error, due in particular to the non-possession of the private key associated with the public key to be certified, is systematically detected and causes the rejection of the request.

3.2.2 Authentication of Organization Identity

The CA inspects any document relied upon under this Section for alteration or falsification.

3.2.2.1 Identity

The CA collects and retains evidence supporting the following identity attributes for the Entity:

- Formal name of the Legal Entity;
- A registered Assumed Name for the Legal Entity (if included in the Subject);
- An organizational unit of the Legal Entity (if included in the Subject);
- An address of the Legal Entity (if included in the Subject);
- Jurisdiction of Incorporation or Registration of the Legal Entity; and
- Unique identifier and type of identifier for the Legal Entity. The unique identifier is included in the subject:organizationIdentifier field of the certificate.

3.2.2.1.1 Verification of entity's legal and operational existence and identity

Verification that the entity has the exclusive legal use of the name specified in the "Organization" field of the certificate is performed by reconciliation with information retrieved from official database (QIIS, QGIS, QTIS) confirming the existence of the entity. These databases contain reliable information provided by a trusted source that registered the entity. The information that is checked during the authentication of the entity's identity includes the SIREN or SIRET number, the VAT return number, the D-U-N-S number (Dun & Bradstreet). The controls applied are as follows:

For private organizations, checks are carried out in the QIIS or the QGIS (ex: directory of companies of France, registries of commercial courts, Dun & Bradstreet) to check:

- Legal existence: the RA checks that the entity's legal existence is established by the political subdivision in which the entity operates and is not designated on the records of the Incorporating or Registration Agency by labels such as "inactive", "invalid," "not current," or the equivalent,
- The name of the entity: the RA checks that the formal name as registered with the incorporating or registration agency of the entity's jurisdiction corresponds to that specified in the certificate request,

- The registration number: a registration number assigned by the incorporating or registration agency must be provided by the entity. In case of non-attribution of registration number by this organization the date of registration must be provided.
- The legal representative: the RA must obtain the name and address of a legal representative designated by the incorporating or registration agency of its jurisdiction.

For public entities, checks are carried out in the QIIS or the QGIS to verify:

- Legal existence: the RA checks that the entity is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates,
- The name of the entity: the RA checks that the entity's formal legal name as recognized by the Registration Agency in the entity's Jurisdiction of Registration matches the entity's name in the certificate request,
- The registration number: Attempt to obtain the specific unique Registration Number assigned to the entity by the registration agency in its Jurisdiction of registration. Where the registration agency does not assign a registration number, the CA integrates in the DN of the certificate that the entity is a public entity.

For business entities, checks are carried out in the QIIS or the QGIS to check:

- Legal existence: the RA checks that the applicant is engaged in business under the name submitted in the request.
- The name of the entity: the RA checks that the formal name as registered with the incorporating or registration agency of the entity's jurisdiction corresponds to that specified in the certificate request,
- The registration number: a registration number assigned by the incorporating or registration agency must be provided by the entity. In case of non-attribution of registration number by this organization the date of registration must be provided.
- The legal representative: the RA verifies the identity of the identified Principal Individual.

For non-commercial entities, checks are carried out in the QIIS or the QGIS to check:

- Legal existence: the RA checks that the entity is a legally recognized International Organization Entity.
- The name of the entity: the RA checks that the entity's formal legal name as recognized by the Registration Agency in the entity's Jurisdiction of Registration matches the entity's name in the certificate request,
- The registration number: the RA must obtain the Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available, the CA integrates in the DN of the certificate that the entity is an international organization entity.

In the case of a LEI data reference, the CA or RA SHALL verify the associated data record with the "Global Legal Entity Identifier Foundation" available at the following address: https://search.gleif.org/#/search/.

3.2.2.1.2 Verification of entity's operational existence

The RA checks that the physical address provided by the Applicant is an address where the Applicant or a Parent/Subsidiary Company conducts business operations (not, for example, a mail drop or P.O. box, or 'care of' (C/O) address), and is the address of the Applicant's Place of Business:

- For an entity whose place of business is in the same country as the entity's Jurisdiction of Incorporation or Registration, a verification of the presence of the address provided in the QGIS, the QIIS or the QTIS is carried out by the RA.
- For an entity whose place of business is not in the country of Incorporation or Registration, the RA rely on a verified professional letter that indicates the address of the Applicant's Place of Business and that business operations are conducted there.

3.2.2.1.3 Verification of entity's operational existence

The RA checks that the entity's operational existence verifying that it's listed in either a current QIIS or QTIS and that such filing continues to be valid.

3.2.2.1.4 Verification of entity's communication means

When requesting a certificate, the applicant's email address is checked by sending an activation link. The CA does not delegate the verification of mailbox authorization or control.

SERVICES CA	*Web authentication*
EN 319 411-2 QEVCP-w	
Check is made that the phone number provided in the application is consistent with the telephone number available through the public telephone directories and the entity's official website, if applicable. A call is made by the RA to verify the entity's telephone number and the ability to reach the caller via that channel and to have his/her confirmation about the legitimacy of the certificate request.	

3.2.2.2 DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, the CA verifies the Applicant's right to use the DBA/tradename using at least one of the following:

- Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition,
- A Reliable Data Source,
- Communication with a government agency responsible for the management of such DBAs or tradenames,
- An Attestation Letter accompanied by documentary support; or
- A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

The "organizationName" field can contain the organization's name and/or DBA/tradename. The CA can include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations

used are locally accepted abbreviations, e.g. if the official record shows "Company Name Incorporated", the CA can use "Company Name Inc." or "Company Name". If both are included, the DBA/tradename appears first, followed by the organization's name in parentheses.

3.2.2.3 Verification of Country

The CA verifies the country associated with the Subject using one of the following:

- the IP Address range assignment by country for either the web site's IP address, as indicated by the DNS record for the web site or the Applicant's IP address,
- the ccTLD of the requested Domain Name,
- information provided by the Domain Name Registrar; or
- a method identified in Section 3.2.2.1.

The CA implements a process to screen proxy servers to prevent reliance upon IP addresses assigned in countries other than where the Applicant is located.

3.2.2.4 Validation of Domain Authorization or Control

For each FQDN listed in the certificate, the RA checks that, at the time the certificate is issued, either the entity is the owner of the domain name, or it has obtained authorization to use the FQDN using the procedure described in chapter 4.2.1.

In addition to the validation of the authorization on the domain name, one of the checks below is implemented for each FQDN to ensure that it is controlled by the CM and to confirm the legitimacy of the certificate request. This verification is carried out before the issuance of each certificate, even when it is renewal. CAs maintains a record of which domain validation method was used to validate every domain.

Effective March 15th, 2026: DNSSEC validation back to the IANA DNSSEC root trust anchor is performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective:

- performs DNSSEC validation using the algorithm defined in RFC 4035 Section 5; and
- supports NSEC3 as defined in RFC 5155; and
- support SHA-2 as defined in RFC 4509 and RFC 5702; and
- properly handles the security concerns enumerated in RFC 6840 Section 4.

Effective March 15th, 2026:

For e-mail Domain Validation methods described in sections 3.2.2.4.4 and 3.2.2.4.14, DNSSEC validation back to the IANA DNSSEC root trust anchor is performed on all DNS CNAME, CAA, TXT queries attempting to obtain the Authorization Domain Name associated with the validation of domain authorization or control by the Primary Network Perspective and the CA do not use local policy to disable DNSSEC validation.

For all other Domain Validation methods, DNSSEC validation back to the IANA DNSSEC root trust anchor is performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective and the CA do not use local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of:

- self-audits performed to fulfill the commitments in Section 8.7,
- the logging commitments of Section 5.4.1.

DNSSEC validation back to the IANA DNSSEC root trust anchor May be performed on all DNS queries associated with the validation of domain authorization or control by Remote Network Perspectives used for Multi-Perspective Issuance Corroboration.

The CA maintains a record of which domain validation method, including relevant BR version number, they used to validate every domain.

3.2.2.4.1 Validating the Applicant as a Domain Contact

No stipulation.

3.2.2.4.2 Email to Domain Contact

No stipulation. This method has been withdrawn by the CA.

3.2.2.4.3 Phone Contact with Domain Contact

No stipulation.

3.2.2.4.4 Email to a Constructed Address

An email is sent by CERTIGNA to one of the addresses below created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the atsign ("@"), followed by the Domain Name. This email provides a link with a request token and allows access to a page where the applicant will confirm that he controls this domain name and that the certificate request is legitimate.

The request token is unique for each FQDN and remains valid no more than 30 days from its creation. The CA may resend the email in its entirety, including re-use of the request token, provided that the communication's entire contents and recipient(s) remain unchanged. If the constructed email is similar for multiple requested FQDNs (e.g. case of subdomains), then only one mail is sent to the domain contact containing associated links to confirm the control of each FQDN.

Effective March 15, 2028: the CA must not rely on this method and prior validations using this method and validation data gathered according to this method cannot be used to issue server certificates.

3.2.2.4.5 Domain Authorization Document

No stipulation.

3.2.2.4.6 Agreed-Upon Change to Website

No stipulation.

This method has been retired and replaced by the method "3.2.2.4.18 Agreed-Upon Change to Website v2".

3.2.2.4.7 DNS Change

A DNS CNAME record is displayed to the Subscriber when customizing his certificate request. This record must be set to the website DNS configuration and consists of the domain name that is prefixed with a label with an underscore character ("_") and of a request token. The request value is unique for each FQDN and remains valid no more than 30 days from its creation. A request value is available for each FQDN beyond the 30 days invalidating the value provided previously.

If multiple FQDNs are concerned by the same request, several records will be created. The Subscriber must add all the records to the website DNS configuration to allow the control of each FQDN. Effective March 15, 2025, the CA implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. Other Network Perspectives observe the same challenge information (Request Token) as the Primary Network Perspective.

3.2.2.4.8 IP Address

No stipulation.

3.2.2.4.9 Test Certificate

No stipulation.

3.2.2.4.10 TLS Using a Random Number

No stipulation.

3.2.2.4.11 Any Other Method

No stipulation.

3.2.2.4.12 Validating Applicant as a Domain Contact

No stipulation.

3.2.2.4.13 Email to DNS CAA Contact

No stipulation.

3.2.2.4.14 Email to DNS TXT Contact

An email is sent by CERTIGNA to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN. This email provides a link with a request token and allows access to a page where the applicant will confirm that he controls this domain name and that the certificate request is legitimate.

The request token is unique for each FQDN and remains valid no more than 30 days from its creation. The CA may resend the email in its entirety, including re-use of the request token, provided that the communication's entire contents and recipient(s) remain unchanged. If the email is similar for multiple requested FQDNs (e.g. case of subdomains), then only one mail is sent to the DNS TXT Record Email Contact containing associated links to confirm the control of each FQDN.

Effective March 15, 2028: the CA must not rely on this method and prior validations using this method and validation data gathered according to this method cannot be used to issue server certificates.

3.2.2.4.15 Phone Contact with Domain Contact

No stipulation.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

No stipulation.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

No stipulation.

3.2.2.4.18 Agreed-Upon Change to Website v2

A request token is displayed to the Subscriber when customizing his certificate request and must be set by the Subscriber in a text file. The request token in the file does not appear in the request used for the check. the CA must receive a successful HTTP response from the request.

The file containing the request token:

- must be located on the Authorization Domain Name, and
- must be located under the "/.well-known/pki-validation" directory of the website, and
- must be retrieved via either the "http" or "https" scheme, and
- must be accessed over an Authorized Port.

Wen the CA follows redirects, the following apply:

- Redirects is initiated at the HTTP protocol layer. a. Redirects must be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects must be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2. b.
- Redirects point to resource URLs with either the "http" or "https" scheme.
- Redirects point to resource URLs accessed via Authorized Ports.

The request token is unique for each FQDN and remains valid no more than 30 days from its creation. A new request token is available for each FQDN beyond the 30 days invalidating the value provided previously. If multiple FQDNs are concerned by the same request, several files will be created, each file containing a value for an FQDN. The Subscriber must place all files in the directory to allow the control of each FQDN.

Effective March 15, 2025, the CA implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. Other Network Perspectives observe the same challenge information (Request Token) as the Primary Network Perspective.

This method is not allowed for "wildcard" certificates.

3.2.2.4.19 Agreed-Upon Change to Website – ACME

Confirming the subscriber's control over the FQDN by using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555.

The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received). The token (as defined in RFC 8555, Section 8.3) remains valid until 30 days from its creation.

The file containing the request token must:

- must be located on the Authorization Domain Name, and
- must be located under the "/.well-known/acme-challenge/" directory of the website, and
- must be retrieved via either the "http" scheme, and
- must be accessed over an Authorized Port.

Wen the CA follows redirects, the following apply:

- Redirects MUST be initiated at the HTTP protocol layer. a. Redirects must be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects must be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2. b.
- Redirects must be to resource URLs with either the "http" or "https" scheme.
- Redirects must be to resource URLs accessed via Authorized Ports.

The request token is unique for each FQDN and remains valid no more than 30 days from its creation. A new request token is available for each FQDN beyond the 30 days invalidating the value provided previously. If multiple FQDNs are concerned by the same request, several files will be created, each file

containing a value for an FQDN. The Subscriber must place all files in the directory to allow the control of each FQDN.

Effective March 15, 2025, the CA implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. Other Network Perspectives observe the same challenge information (Request Token) as the Primary Network Perspective.

This method is not allowed for "wildcard" certificates.

3.2.2.4.20 TLS Using ALPN

No stipulation.

3.2.2.4.21 DNS Labeled with Account ID - ACME

No stipulation.

3.2.2.4.22 DNS TXT Record with Persistent Value

No stipulation.

3.2.2.5 Authentication for an IP Address

No stipulation.

3.2.2.6 Wildcard Domain Validation

CERTIGNA WILD CA	*Web Authentication*
CERTIGNA SERVER AUTHENTICATION OVCP CA	*Web Authentication*
CERTIGNA SERVER AUTHENTICATION AUTO OVCP CA	*Web Authentication*
CERTIGNA SERVER AUTHENTICATION QCP CA	*Web Authentication*
CERTIGNA SERVER AUTHENTICATION AUTO QCP CA	*Web Authentication*
Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, the CA establishes and follows a documented procedure that determines if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. "*.com", "*.co.uk"). If a wildcard would fall within the label immediately to the left of a registry-controlled1 or public suffix, CAs refuses issuance unless the applicant proves his/her rightful control of the entire Domain Namespace. (e.g. CAs MUST NOT issue "*.co.uk" or "*.local", but may issue "*.example.com" to Example Co.).	

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the CA evaluates the source for its reliability, accuracy, and resistance to alteration or falsification.

The CA consider the following during its evaluation:

- The age of the information provided,
- The frequency of updates to the information source,
- The data provider and purpose of the data collection,
- The public accessibility of the data availability, and
- The relative difficulty in falsifying or altering the data.

3.2.2.7.1 Denied Lists and Other Legal Blacklists

CERTIGNA SERVICES CA	*Web Authentication*
EN 319 411-2 QEVCP-w	
The RA verifies whether one of the signers (Certificate Manager, Legal Representative) or the entity: - Is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation; or - Has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business. The RA rejects systematically the request if one of the signers or the entity is present in these lists.	

3.2.2.7.2 Parent/Subsidiary/Affiliate Relationship

CERTIGNA SERVICES CA	*Web Authentication*
EN 319 411-2 QEVCP-w	
The RA verifies the entity's relationship to the Parent, Subsidiary, or Affiliate when used in the request. The relationship between the entity and the Parent, Subsidiary, or Affiliate is identified in a QIIS or QGIS.	

3.2.2.7.3 Final Cross-Correlation and Due Diligence

SERVICES CA	*Web authentication*
EN 319 411-2 QEVCP-w	
A cross-correlation is performed by the RA for Qualified/EV (QEVCP-w) certificate applications. The results of these verification process and procedures are performed by an initial RA operator, are then controlled by a RA officer who analyses the integrality of the application by searching for discrepancies or other details requiring further examination. If necessary, the RA officer requests additional information or clarification from stakeholders, consults with QIIS, and / or other sources of information to resolve the anomalies encountered. If necessary, the operator and the Officer shall consult each other to decide, in the final analysis, on the validity of the application. The CA refrains from issuing a Qualified/EV (QEVCP-w) certificate until the information collected for the application file is complete, so that the certificate does not transmit incorrect information that the CA would know, or reasonable diligence would uncover. If the supporting documents or supplementary information are not received within one month, the RA shall reject the application	

and notify the entity.

The documents constituting the application must be provided exclusively in French or English. If the subscriber is unable to provide the documentation in either of these languages, the authority may, if necessary, translate the relevant documents and bear the incurred cost to the subscriber.

3.2.2.8 CAA Records

As part of the Certificate issuance process, the CA retrieves and process CAA records in accordance with RFC 8659 for each “dNSName” in the “subjectAltName” extension.

Effective March 15, 2025, a remote Network Perspective’s CAA check response is interpreted as permission to issue, regardless of whether the responses from both Perspectives are byte-for-byte identical. Additionally, the CA can consider the response from a remote Network Perspective as corroborating if one or both of the Perspectives experience an acceptable CAA record lookup failure, as defined in this section.

The CA can check CAA records at any other time.

When processing CAA records, the CA treats the issue, issuewild, and iodef property tags as specified in RFC 8659. These controls allow to check that the CA is part of the authorities authorized to issue a certificate for these domains.

The following cases do not allow the CA to authorize the issuance of the certificate:
- The CAA DNS field is present, it contains an "issue", "issuewild" or « iodef property » tag and does not list Certigna as an authorized Certificate Authority;
- The CAA DNS field is present, it is designated as "critical" and the tag used is not supported by the CA (it is not an "issue" or "issuewild" tag);
- The zone is validly DNSSEC-signed and our DNS query times out.

If any of these cases are encountered, the certificate request is automatically blocked, and the applicant is notified by email of the need to update the associated DNS records.

To add CERTIGNA to DNS CAA records, several syntaxes are available depending on the server used:
- example.com. IN CAA 0 issue "certigna.fr"
- example.com. IN CAA 0 issue "certigna.com"

The CA issues a certificate after processing a CAA record, it can do so within the TTL of the CAA record, or 8 hours, whichever is greater.

3.2.2.8.1 DNSSEC Validation of CAA Records

Effective March 15th, 2026: DNSSEC validation back to the IANA DNSSEC root trust anchor is performed on all DNS queries associated with CAA record lookups performed by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with CAA record lookups performed by the Primary Network Perspective:
- performs DNSSEC validation using the algorithm defined in RFC 4035 Section 5; and
- supports NSEC3 as defined in RFC 5155; and

- supports SHA-2 as defined in RFC 4509 and RFC 5702; and
- properly handles the security concerns enumerated in RFC 6840 Section 4.

Effective March 15th, 2026: CAs do not use local policy to disable DNSSEC validation on any DNS query associated CAA record lookups.

Effective March 15th, 2026: DNSSEC-validation errors observed by the Primary Network Perspective (e.g., SERVFAIL) are not treated as permission to issue.

DNSSEC validation back to the IANA DNSSEC root trust anchor may be performed on all DNS queries associated with CAA record lookups performed by Remote Network Perspectives as part of Multi-Perspective Issuance Corroboration.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in Section 8.7.

3.2.2.9 Multi-Perspective Issuance Corroboration

Multi-Perspective Issuance Corroboration attempts to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before Certificate issuance. This process can improve protection against equally-specific prefix Border Gateway Protocol (BGP) attacks or hijacks.

The CA can use either the same set, or different sets of Network Perspectives when performing Multi-Perspective Issuance Corroboration for the required Domain Authorization or Control and CAA Record checks.

The set of responses from the relied upon Network Perspectives provide the CA with the necessary information to allow it to affirmatively assess:
- a. the presence of the expected Request Token as required by the relied upon validation method specified in Sections 3.2.2.4 and
- b. the CA's authority to issue to the requested domain(s), as specified in Section 3.2.2.8.

Section 3.2.2.4 describes the validation methods that require the use of Multi-Perspective Issuance Corroboration and how a Network Perspective can corroborate the outcomes determined by the Primary Network Perspective.

Results or information obtained from one Network Perspective cannot be reused or cached when performing validation through subsequent Network Perspectives (e.g., different Network Perspectives cannot rely on a shared DNS cache to prevent an adversary with control of traffic from one Network Perspective from poisoning the DNS cache used by other Network Perspectives).

The network infrastructure providing Internet connectivity to a Network Perspective are administered by the same organization providing the computational services required to operate the Network Perspective. All communications between a remote Network Perspective and the CA take place over an authenticated and encrypted channel relying on modern protocols (e.g., over HTTPS).

A Network Perspective may use a recursive DNS resolver that is not co-located with the Network Perspective. However, the DNS resolver used by the Network Perspective must fall within the same

Regional Internet Registry service region as the Network Perspective relying upon it. Furthermore, for any pair of DNS resolvers used on a Multi-Perspective Issuance Corroboration attempt, the straight-line distance between the two DNS resolvers reside in are at least 500 km.

The location of a DNS resolver is determined by the point where unencapsulated outbound DNS queries are typically first handed off to the network infrastructure providing Internet connectivity to that DNS resolver. The CA can immediately retry Multi-Perspective Issuance Corroboration using the same validation method or an alternative method (e.g., CA can immediately retry validation using "Email to DNS TXT Contact" if "Agreed-Upon Change to Website - ACME" does not corroborate the outcome of Multi-Perspective Issuance Corroboration).

When retrying Multi-Perspective Issuance Corroboration, the CA cannot rely on corroborations from previous attempts. There is no stipulation regarding the maximum number of validation attempts that may be performed in any period of time.

The "Quorum Requirements" Table describes quorum requirements related to Multi-Perspective Issuance Corroboration. If the CA does not rely on the same set of Network Perspectives for both Domain Authorization or Control and CAA Record checks, the quorum requirements is met for both sets of Network Perspectives (i.e.,the Domain Authorization or Control set and the CAA record check set). Network Perspectives are considered distinct when the straight-line distance between them is at least 500 km. Network Perspectives are considered "remote" when they are distinct from the Primary Network Perspective and the other Network Perspectives represented in a quorum.

The CA can reuse corroborating evidence for CAA record quorum compliance for a maximum of 398 days. After issuing a Certificate to a domain, remote Network Perspectives can omit retrieving and processing CAA records for the same domain or its subdomains in subsequent Certificate requests from the same Applicant for up to a maximum of 398 days.

Quorum Requirements	
# of Distinct Remote Network Perspectives used	**# of Allowed non-Corroborations**
2-5	1
6+	2

Remote Network Perspectives performing Multi-Perspective Issuance Corroboration:

- Network Hardening - Rely upon networks (e.g., Internet Service Providers or Cloud Provider Networks) implementing measures to mitigate BGP routing incidents in the global Internet routing system for providing internet connectivity to the Network Perspective.

The CA will implement Multi-Perspective Issuance Corroboration using at least:

- **two (2)** remote Network Perspectives. The CA can proceed with certificate issuance if the number of remote Network Perspectives that do not corroborate the determinations made by the Primary Network Perspective ("non-corroborations") is greater than allowed in the Quorum Requirements table. **Effective March 15, 2025**
- **two (2)** remote Network Perspectives. The CA will not proceed with certificate issuance if the number of non-corroborations is greater than allowed in the Quorum Requirements table. **Effective September 15, 2025**

- **three (3)** remote Network Perspectives. **Effective March 15, 2026**
- **four (4)** remote Network Perspectives. **Effective June 15, 2026**
- **five (5)** remote Network Perspectives. **Effective December 15, 2026**

The CA does not proceed with certificate issuance if the number of non-corroborations is greater than allowed in the Quorum Requirements table and if the remote Network Perspectives that do corroborate the determinations made by the Primary Network Perspective do not fall within the service regions of at least two (2) distinct Regional Internet Registries.

3.2.3 Validation of an individual's identity

Verification of the identity targets:
- A Certificate Manager for a legal person;
- The legal representative of the organization attached to the certificate;
- The Certification Agent associated with the organization, if applicable.

The CA collects and retains evidence supporting the following identity attributes for the CM:
- Given name(s) and surname(s), which are current names,
- Further information as needed to uniquely identify the CM.

To authenticate an individual's identity, verification of a photocopy of an individual's identification is required. It could be an official identity document valid (National Identity Card, passport or residence permit) or a professional card issued by an administrative authority (if that authority maintaining a register of identities ensuring the link between the agent and the professional card) with an ID photo or a reference to the administrative file of the agent. The CA inspects the copy for any indication of alteration or falsification. The existence of the alleged identity is known to an authoritative source and the CA must be able to assume that the person is who he claims to be.

RA and DRA operators are made aware of the frauds that may occur on the issue of documents or copies of official documents (falsified documents). Particular attention is given to the validity checks of the pieces supplied (date of validity of identity documents, date of requests, etc.). These aspects are developed during the initial training planned for the RA operators and detailed in the training program defined in the document "Staff monitoring". Periodic checks take into account sampling checks of processed files to ensure compliance with procedures. These controls are conducted by people in the roles of Controllers or Security Officers.

3.2.3.1 CA Certificate

The registration of a new CA certificate request is achieved through the RA by the CA responsible. This request is formalized through a script during the key ceremony used for certificate generation.

3.2.3.2 Legal Person Certificate

Registration of a service or server to which a certificate should be issued is performed via the registration of the corresponding Certificate Manager. A Certificate Manager may have to change

valid corresponding server certificate. In this case, any new Certificate Manager shall also be subject to a registration procedure.

The Certificate Manager is either the legal representative of the entity or a natural person formally designated by the legal representative. The registration of a Certificate Manager, and the corresponding server can be done either directly from the RA, a DRA or via a Certification Agent of the entity. In this last case, the Certification Agent must have been registered by the RA.

The registration of the future Certificate Manager requires the "legal person" identity verification (the entity attached to the future Certificate Manager), and the "natural person" identity verification (the future Certificate Manager), his/her authorization to be a CM for the concerned service or server and the concerned entity.

The Certificate Manager is informed that personal identity information can be used as authentication data during a possible revocation request.

3.2.3.2.1 Certificate Manager Registration

The certificate request files shall be completed with the forms available on CERTIGNA website or DRA website. The files sent to RA shall include the following elements:

Certificate request form	
Subject	Designation of a legal representative of the entity and his/her information
	Designation of the future CM and his/her information
	Designation of the identity of the entity attached to the service or server
	Designation of applicable TCSU
Date	Signed less than 3 months ago
Signature	Signed by a legal representative to mandate the future CM Signed by the future CM to accept this role and the TCSU

Official identification document of the Certificate Manager	
Subject	A photocopy of a valid CM identification element, recognized by the Member State in which the request for a certificate is filed
Date	Piece valid at the time of registration

Official identification document of the legal representative or the Certification Agent	
Subject	A photocopy of a valid identification element of the legal representative or the Certification Agent, recognized by the Member State in which the request for a certificate is filed
Date	Piece valid at the time of registration

Document attesting to the quality of legal representative	
Subject	**For a company**, a document attesting to the quality of legal representative nationally recognized. *e.g. a copy of the articles of the company, valid, bearing the signature of its representatives.* **For an administrative authority**, one piece, support of delegation or sub-delegation of responsible authority of the administrative structure nationally recognized.
Date	Piece valid at the time of registration

Document bearing the SIREN number of the company	
Subject	**For a company**, any document, valid at the time of registration, bearing the SIREN number of the company (*KBIS extract or Certificate of Identification at the National Directory of Companies and of their Establishments*) or, failing that, another valid document certifying the unique identification of the company to be included in the certificate.
Date	Piece valid at the time of registration

EN 319 411-2 QNCP-w
The authentication of the CM by the RA is carried out via one of the following means: - Face-to-face authentication with the CM with presentation of valid ID at the face-to-face (National Identity Card, Passport or Residence Card). - Remote authentication using a means of electronic identification qualified at substantial or high level within the meaning of the eIDAS Regulation. - Authentication using a nationally recognized identification method that provides equivalent assurance in terms of reliability to face to face authentication. The equivalent warranty is confirmed by a conformity assessment body. Authentication of the CM using a qualified electronic signature certificate as defined in the eIDAS Rules.
EN 319 411-2 QEVCP-w

Authentication of the Certificate Manager by the RA (RA or DRA operator) is performed with a face-to-face during which the following elements are controlled:
- A valid official document of the CM with an ID photo (national identity card, passport or residence permit).
- At least two secondary documentary evidences that include the name of the CM, one of which is from a financial institution:
  o A major credit card indicating an expiration date and it has not expired;
  o A debit card indicating an expiration date and it has not expired;
  o A bank statement from a regulated financial institution that is less than six months old;
  o Recent original utility bills (telecom bill for a fixed line or an EDF / GDF bill) indicating the name and the fixed address;
  o A copy of a statement for payment of a lease, provided that the statement is dated within the past six months;
  o A local authority tax bill for the current year (property tax, residential tax);
  o A certified copy of a birth certificate.

EN 319 411-1 OVCP
Authentication of the Certificate Manager by the RA (RA or DRA operator) is performed by sending the files by postal mail or in a dematerialized form (scanned files which are sent by email).
RGS *
Authentication of the Certificate Manager by the RA (RA or DRA operator) is performed by sending the files by postal mail or in a dematerialized form (scanned files which are sent by email).

3.2.3.3 Registration of a Certification Agent

The Certification Agent must register with the RA to substitute for RA in the processing of registration of certificate requests. The registration of a Certification Agent requires the verification of the "legal person" identity of the entity for which the Certification Agent is attached, the verification of the "natural person" identity of the future Certification Agent, and the relation between the future Certification Agent and this entity. The certificate request files shall be completed with the forms available on CERTIGNA website or DRA website. The files sent to RA shall include the following elements:

Certification Agent registration form	
Subject	Designation of a legal representative of the entity and his/her information
	Designation of the future Certification Agent and his/her information
	Designation of applicable Terms and conditions
Date	Signed less than 3 months ago
Signature	Signed by a legal representative to mandate the Certification Agent Signed by the future Certification Agent to accept this role and the TCSU

Letter of commitment from the Certification Agent	
Subject	Designation of the future Certification Agent and its information
	Designation of the role and responsibilities of Certification Agent with: - Conduct impartial and scrupulous identity checks of the future Subjects as defined in the CP, - Notify the RA on leaving the entity.
Date	Signed less than 3 months ago
Signature	Signed by the future Certification Agent to accept these responsibilities

Official identification document of the Certification Agent	
Subject	A photocopy of a valid identification element of the Certification Agent, recognized by the Member State in which the request for a certificate is filed
Date	Piece valid at the time of registration

Document attesting to the quality of legal representative	
Subject	**[Company]** A document attesting to the quality of legal representative known nationally. *eg a copy of the articles of the company, valid, bearing the signature of its representatives.* **[Administrative authority]** One piece, support of delegation or sub-delegation of responsible authority of the administrative structure known nationally.
Date	Piece valid at the time of registration

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

The authentication of the Certification Agent by the RA is carried out via one of the following means:

- Face-to-face authentication with the Certification Agent with presentation of valid ID at the face-to-face (National Identity Card, Passport or Residence Card).

- Remote authentication using a means of electronic identification qualified at substantial or high level within the meaning of the eIDAS Regulation. - Authentication using a nationally recognized identification method that provides equivalent assurance in terms of reliability to face to face authentication. The equivalent warranty is confirmed by a conformity assessment body. Authentication of the Certification Agent using a qualified electronic signature certificate as defined in the eIDAS Rules.
EN 319 411-1 OVCP RGS *
The authentication of the Certification Agent by the RA is carried out by sending the paper file by postal mail accompanied by a photocopy of the identity documents of each of the signatories of the documents in the file (legal representative, Certification Agent). This authentication can also be done in dematerialized form on condition that the various supporting documents of the file are signed using an electronic signature process in accordance with the requirements of the RGS level * and that the signature is verified and valid at the time of recording. If the Certification Agent is not equipped with a certificate of RGS level * or higher, the files cannot be sent in dematerialized form. In this case, each file will only be validated after receipt of the original documents by postal mail.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of Authority

This step is performed simultaneously with the validation of the identity of the legal representative, the CM or the Subject (directly by the RA or the Certification Agent).

3.2.6 Criteria for Interoperation

The CA disclose all Cross Certificates that identify the CA as the Subject, provided the CA has arranged for or accepted the establishment of the trust relationship (i.e., the Cross Certificate at issue).

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

The CA does not issue a new certificate for previously issued key pair. Renewal involves through the generation of a new key pair and a new certificate request.

3.3.1.1 CA Certificate

Identifying and authenticating a current CA certificate renewal request is the same as the original request.

3.3.1.2 Legal Person Certificate

At the first renewal, the CA at a minimum ensures that the information in the initial registration request is still valid and that the certificate to be renewed exists and is still valid.

At the next renewal, the RA identifies the Certificate Manager and the application service or the server according to the same procedure as for the initial registration.

Documents provided to validate the identity of the Subject, the CM, the Legal Representative and the entity may be used in compliance with requirements of section 4.2.1.2.

For validation of Domain Names according to Section 3.2.2.4, any data, document, or completed validation used is obtained no more than the delay described at section 4.2.1.2.

EN 319 411-1 OVCP EN 319 411-2 QNCP-w EN 319 411-2 QEVCP-w
The applicant always has control of the domain via one of the methods used for the initial registration.

3.3.2 Identification and Authentication for Re-key After Revocation

Identification and authentication for re-key after revocation is the same as the original request.

3.4 Identification and authentication for revocation request

3.4.1 CA Certificate

A CA certificate revocation can only be decided by the entity responsible of the CA, or by legal authority through a justice decision.

The revocation of other component certificates is decided by the entity operating the component concerned, which must inform the CA without delay.

3.4.2 Legal or Natural Person Certificate

3.4.2.1 Current request

The certificate revocation request sent by the Certificate Manager, the Subject, the legal representative of the entity, a DRA operator, or if appropriate a Certification Agent can be done by one of the following means:

- Mail: request completed and signed from the form of revocation of a certificate available on the website of CERTIGNA https://www.certigna.com. The requester is authenticated by sending its Official identification document with the mail.
- From the customer area of the CERTIGNA website https://www.certigna.com selecting the certificate to be revoked.
- Through the ACME Service by sending a request to revoke the certificate.

The mailing address of the revocation service is available on the website of CERTIGNA https://www.certigna.com

The paper request must include the following:

- The FQDN of the server,
- The email address of the Certificate Manager,
- The reason for the revocation.

If the Certificate Manager is not the subscriber:

- The first and last name of the subscriber,
- The quality of the subscriber (legal representative, DRA operator, Certification Agent),
- The subscriber's phone number.

The paper form can also be transmitted electronically. The electronic application can be performed by an authorized person with a certificate of the same level or higher (a DRA operator or if appropriate a Certification Agent). The application will be electronically signed with this certificate of the same level or higher.

The revocation request processing by the RA is detailed in the "Operational Revocation Request Procedure". As with certificate applications, periodic audits may consider sample checks of revocation requests processed by the RA to ensure compliance with procedures.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

4.1.1.1 CA Certificate

The certificate request must come from a legal representative of the entity.

4.1.1.2 Legal or Natural Person Certificate

For certificates attached to an organization, the certificate request must come from a legal representative of the entity or from a Certification Agent duly mandated for this entity, with the prior consent of the future Certificate Manager or Subject.

The CA maintains an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. The CA uses this information to identify subsequent suspicious certificate requests.

4.1.2 Enrolment Process and Responsibilities

4.1.2.1 CA Certificate

The registration files are established directly by the Certification Authority during the Key ceremony.

4.1.2.2 Legal or Natural Person Certificate

The registration files are established directly by the future CM from the evidence provided by his entity if applicable, or by the entity and signed by the CM. The files are transmitted directly to the RA if the entity has not implemented the use of Certification Agent. The files are delivered to it otherwise. When recording of the future CM, it must provide an email address that allows the RA to contact for any questions regarding registration. The Certification Agent must also provide an email address when registering for allows the RA to contact him on any matter relating to the registration of the CM. The certificate application must contain the elements described in section 3.2.3.

The email address of the Certificate Manager, and where applicable the Certification Agent, is stored in the RA databases. These addresses are used to transmit service messages when processing certificate or revocation requests, or for additional requests made by RA operators processing these requests.

Documents provided to validate the identity of the Subject, the CM, the Legal Representative and the entity may be used during any of the periods defined in section 4.2.1.2 to issue a certificate, provided that they are still valid at the time of validation of the certificate request. For the validation of domain names in accordance with section 3.2.2.4, all data, documents, or validations used are reusable for issuing a new certificate during one of the periods defined in section 4.2.1.2.

A certificate requiring authentication of the Subject or CM by means of a physical face-to-face, an eID, or an electronic signature using an eIDAS-qualified certificate, can only be renewed after re-authentication of the Subject or CM via one of these processes. The process used for renewal (e.g. an eIDAS-qualified certificate signing renewal form) must itself have been issued on the basis of a physical face-to-face.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 CA Certificate

The request is validated by all witnesses which participate to the key ceremony comprising one RA administrator.

4.2.1.2 Legal or Natural Person Certificate

The RA does the following operations when processing a certificate request:

- Validation of the server,
- Validation of the identity of the entity,
- Validation of the identity of the signatory of the request (CM, legal representative, or Certification Agent),
- Validation of domain control for a server,
- Validation of the files and the consistency of evidence presented,
- Assurance that the future CM is informed of the applicable requirements to the use of the certificate.

Documents provided to validate the identity of the Subject, the CM, the Legal Representative and the entity may be used during any of the periods defined in the table below to issue a certificate, provided that they are still valid at the time of validation of the certificate request.

Certificate issued	Period during which valid identity documents can be reused
Before March 15, 2026	825 days
On or after March 15, 2026	398 days

For the validation of domain names in accordance with section 3.2.2.4, all data, documents, or validations used are reusable for issuing a new certificate during one of the periods in the table below.

Certificate issued		Period during which valid identity documents can be reused
After	**And before**	
	March 15, 2026	398 days
March 15, 2026	March 15, 2027	200 days
March 15, 2027	March 15, 2029	100 days
March 15, 2029		10 days

All the operations mentioned above are carried out by the RA, but in the case of a request made via a DRA or a Certification Agent, the latter retransmits the request to the RA after having carried out the following checks:

- Ensure that the future Certificate Manager has been informed of the TCSU, in addition to their distribution operated by the CA.
- Check the identity of the CM and the original documents attesting to his identity to identify and authenticate him/her.
- Check the completeness of the request file.

The RA then ensures that the request corresponds to the mandate of the DRA operator or the Certification Agent. The identity of the future Certificate Manager and the legal representative is approved if the supporting documents provided are valid at the date of receipt.

In addition to the methods for the validation of the domain control (see 3.2.6), the verification of the FQDN and the entity holding it is achieved using "WHOIS" websites (e.g. AFNIC) and/or the provision of supporting documentation to attest, as far as possible, to the ownership of the domain name. A legal representative of the entity which holds the domain according to these websites and/or supporting documents, must formally designate the entity to which the RC is attached or the RC and its entity in a domain authorization document signed by that representative (request form or specific form provided by the CA).

In compliance with the RFC 8659, controls are performed on CAA record (See chapter 3.2.2.8).

The CA develops, maintains, and implements documented procedures that identify and require additional verification activity for High-Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements. In particular, the RA has carried out controls with databases of domain names that are suspected to be used for phishing activities (e.g., APWG, Phishing initiative, etc.) and with CA's internal databases of revoked certificates for compromising reason or request of certificates which are suspected to be used for phishing activities. These practices are supported by the CA and not delegated to third parties (e.g., DRA).

4.2.2 Approval or Rejection of Certificate Applications

After processing the request, in case of rejection, the RA notifies the CM, if applicable the operator of DRA, or the Certification Agent.

The justification for any refusal is made by the RA specifying the cause:

- The request files are incomplete (missing document),
- One of the documents is invalid (signature date more than 3 months, the date of validity of a document is exceeded, etc.),
- The request does not match with the mandate of the DRA operator or the Certification Agent.

If accepted by the RA, after generation of the certificate by the CA, the RA sends a mail to the CM to complete the certificate acceptation and the acquisition of activation data.

The CA does not issue web SSL/TLS server certificates containing internal names, Reserved IP Addresses, Domain Names that end in an IP Reverse Zone Suffix or containing a new gTLD under consideration by ICANN.

An automatic process is implemented, when ordering a wildcard TLS/SSL certificate, to verify that the requested domain name is made up as "*.domain.tld". To consolidate this check, TLDs validated by ICANN are everyday automatically retrieved through the list on the https://publicsuffix.org website. In addition, the verification of the domain name owner performed by the RA will in all cases lead to a rejection of the application as it is impossible to identify the owner of a domain name of type "*.tld". Applications with an invalid TLD or non-domain (E.g. *.co.uk) will therefore be systematically rejected.

CERTIGNA SERVICES CA	*Web authentication*
EN 319 411-2 QEVCP-w	
Request acceptation by the RA needs an action by a RA operator and a Registration Officer before creating the certificates.	

4.2.3 Time to Process Certificate Applications

4.2.3.1 CA Certificate

As the request for a CA certificate is formally established during the key ceremony, the concerned certificate is generated within hours of the request.

4.2.3.2 Legal Person Certificate

As from the receipt of the full registration files and electronic request (CSR), the certificate is issued within 30 days.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

After validation by the RA, the CA initiates the certificate generation process for the CM. The conditions for generating keys and certificates and security measures to meet are described in Chapters 5 and 6 below, including the separation of trusted roles. (See section 5.2). Request validation on the RA

component and certificate generation on the CA component are detailed in the "Certificate request operating procedure".

4.3.1.1 Manual authorization of certificate issuance for Root CAs

Keys pairs of Root CA and intermediate CA are generated during the key ceremony. The operations for generating and signing certificates issued by the root CA are carried out under the same controlled circumstances as the generation of CA key pairs (see section 6.1.1), in the presence of people in authorized trusted roles by CA (i.e. the CA system operator, security officer, or PKI administrator) and as part of "key ceremonies". The CA administrator performs commands to generate and sign certificates by the root CA in the presence of trusted roles which ensure that practices comply with security requirements and the defined script.

4.3.1.2 Linting of to-be-signed Certificate content

Due to the complexity involved in implementing Certificate Profiles that conform to requirements, effective 2025-03-15, the CA systematically implements a Linting process to test the technical conformity of each to-be-signed artifact prior to signing it.

4.3.1.3 Linting of issued certificates

The CA uses a linting process to test each issued certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

4.3.2.1 CA Certificate

The delivery of the CA certificate is carried out during the key ceremony, to a CA administrator authorized by the CA in charge of its exploitation and dissemination.

4.3.2.2 Legal Person Certificate

Complete and accurate certificate is made available to the CM on the customer area or on the device provided by CA if applicable. The CM authenticates on the customer area to accept the certificate or complete a paper form.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

4.4.1.1 CA Certificate

The authority representant and the witnesses, which participate to the key ceremony, control the compliance of the certificate with the request. The acceptance is formalized through the record of the key ceremony.

4.4.1.2 Legal Person Certificate

The acceptance of the certificate is carried out by the CM, from their customer area and before downloading their certificate or retrieving the activation data from their support. The CM explicitly chooses whether to accept the certificate and the notification of acceptance or refusal is automatically transmitted to the CA. When using the ACME Service, the certificate is tacitly accepted by the CM.

In case of detection of inconsistency between the information in the contractual agreement and the content of the certificate, the CM must refuse the certificate, which will result in its revocation.

4.4.2 Publication of the Certificate by the CA

4.4.2.1 CA Certificate

Root CA and intermediate certificates are published by CA. See Section 2.

4.4.2.2 Legal Person Certificate

Prior to the issuance of the server certificate, a precertificate similar to the certificate is issued and recorded in the public logs linked to the "Certificate Transparency" system, in order to ensure recognition of server authentication certificates by Browsers. The list of public logs used and publishing the precertificate is provided in chapter 7.2 of this document.

No publication of the certificate is made by the CA after acceptance of the certificate by its CM.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The RA is informed of the generation of the certificate by the CA which is responsible for issuing the generated certificate.

4.5 Key Pair and Certificate Usage

4.5.1 Subject Private Key and Certificate Usage

The CA, the CM, must strictly respect the permitted uses of key pairs and certificates described at chapter 1.5.1. In the opposite case, they could be held liable.

The authorized use of the key pair and of the associated certificate is also specified in the certificate itself, via the extensions relating to the key usage, if applicable.

As part of the registration files, the Terms and condition are made known to the CM, or to the Certification Agent by the CA before entering in a contractual relationship. They are consulted prior to any online certificate request. They are available on the https://www.certigna.com website.

The TCSU accepted by the Subject during the certificate request shall remain valid for the entire life of the certificate. When using the ACME service to request an SSL/TLS web authentication certificate, the CM accepts the applicable TCSU on the first request via the https://www.certigna.com website. The CM is then automatically informed by e-mail of the application of the new TCSU, which he tacitly accepts by continuing to use the ACME service for all new certificate requests.

4.5.2 Relaying Party Public Key and Certificate Usage

Certificate users must strictly respect the permitted uses of certificates mentioned at section 1.5.1. In the opposite case, they could be held liable.

4.6 Certificate Renewal

The CA does not issue a new certificate for previously issued key pair. Renewal involves the generation of a new key pair and a new certificate request (see section 4.1). If the CM or the Subject generates his/her key pair, he is committed, accepting the TCSU, to generate a new key pair for each request.

4.6.1 Circumstance for Certificate Renewal

No stipulation.

4.6.2 Who May Request Renewal

No stipulation.

4.6.3 Processing Certificate Renewal Requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

The key pairs must be periodically renewed to minimize the possibilities of cryptographic attacks. Thus, the key pairs of CAs, servers, and the corresponding certificates, are renewed regularly (cf. validity period chapter 6.3.2). Moreover, a key pair and a certificate can be renewed early, following the revocation of the certificate.

4.7.2 Who may Request Certification of a New Public Key

The triggering of the provision of a new certificate is initiated by the CM. The entity, through its Certification Agent if necessary, can also be at the initiative of a new certificate request for a CM attached to it.

4.7.3 Processing certificate re-keying requests

See section 4.2.1.

4.7.4 Notification of new certificate issuance to subscriber

See section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See section 4.4.3.

4.8 Certificate modification

Changing Server certificates is not allowed. In case of need to change information in the certificate (mainly DN), a new certificate must be issued after revocation of the old.

4.8.1 Circumstance for Certificate Modification

No stipulation.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Legal Person Certificate

The CA revokes a Certificate within 24 hours and use the corresponding CRLReason if one or more of the following occurs:

- **Key compromise** (RFC 5280 CRLReason #1)
  - The CM, the legal representative of the entity to which it belongs, if any Certification Agent or DRA operator request the revocation of the certificate (especially in the case of destruction or alteration of the private key and / or its support) because they have reason to believe that the private key of the certificate has been compromised, e.g. an unauthorized person has had access to the private key of the certificate.
  - The CA obtains verifiable evidence that the private key corresponding to the public key in the certificate is suspected of being compromised or is compromised,
  - The CA is made aware a demonstrated or proven method that can easily compute the server Private Key based on the Public Key in the Certificate, including but not limited to those identified in Section 6.1.1.3,
  - The CA is made aware of a demonstrated or proven method that exposes the Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed. Methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).

- **Privilege withdrawn** (RFC 5280 CRLReason #9)
  - The legal representative of the entity to which the server belongs or the RC notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization,
  - The CA obtains evidence that the certificate was misused,
  - The CA is made aware of a material change in the information contained in the Certificate,
  - The CA is made aware that the CM has violated one or more of its material obligations under these TCSU,
  - The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name,
  - The CA determines or is made aware that any of the information appearing in the certificate is inaccurate or misleading,
  - The cryptographic device used to store the certificate and the private key of the server no longer complies or will no longer comply with the requirements of chapter 11 of the CP/CPS (Ex: a qualification or certification would no longer be maintained or would be suspended),

- **Cessation of operation** (RFC 5280 CRLReason #5)
  - The CA is made aware of any circumstance indicating that use of an email address, a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a

court or arbitrator has revoked a Domain Name Registrant's right to use the email address or the Domain Name),
  - The final shutdown of the server or the cessation of activity of the CM entity,
  - The CM no longer controls, or is no longer authorized to use, all of the domain names in the certificate,
  - The CM will no longer be using the certificate because they are discontinuing their website.

- **Affiliation changed** (RFC 5280 CRLReason #3)
  - The information of the server contained in its certificate, is not in accordance with the identity or purpose in the certificate (eg, change in the identity or function of the server), this before the normal expiry of certificate.

- **Superseded** (RFC 5280 CRLReason #4)
  - The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon, including cases where the CA failed to perform CAA checking correctly or where issuance was not permitted according to Section 3.2.2.8 (CAA Records),
  - The certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CP/CPS,
  - The CA is made aware that the certificate was not issued in accordance with this CP/CPS,
  - The CM, the entity, if any Certification Agent or DRA operator, has not fulfilled its obligations under this CP/CPS,
  - The CM has requested a new certificate to replace an existing certificate,

- **Other reason of revocation which results in no reasonCode extension being provided in the CRL:**
  - The CM, the legal representative of the entity to which it belongs, requests in writing, without specifying a CRLreason, that the CA revoke the Certificate,
  - The CA obtains evidence that the private key corresponding to the public key in the certificate is suspected of being lost or stolen (or possibly the activation data associated with the private key),
  - The CM, the legal representative of the entity to which it belongs, if any Certification Agent or DRA operator request the revocation of the certificate (especially in the case of destruction or alteration of the private key and / or its support),
  - The CA's right to issue certificates under CA/Browsers Forum Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository,
  - Revocation is required by this CP/CPS, for a reason that is not otherwise required to be specified by this section,
  - The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate,
  - The CA signing the certificates is revoked (which results in the revocation of all valid certificates signed by the corresponding private key),

- The technical content or format of the certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g., the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such certificates should be revoked and replaced by CA within a given period of time),
- An error (intentional or not) was detected in the certificate request and the associated registration files,
- For technical reasons (failure to send the certificate ...).

4.9.1.2 Reasons for Revoking a CA Certificate

One or more of the following occurs can conduct of revocation the subordinate certificate within 7 days:

- The CA requests revocation in writing,
- The CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization,
- The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6,
- The Issuing CA obtains evidence that the Certificate was misused,
- The Issuing CA is made aware that the Certificate was not issued in accordance with or that CA has not complied with this document or the applicable CP/CPS,
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading,
- The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate,
- The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository.

4.9.2 Who Can Request Revocation

4.9.2.1 CA Certificate

The revocation of a CA certificate can only be decided by the entity responsible of the CA, or by the judicial authorities via a court order.

The revocation of the other components of certificates is decided by the entity operating the concerned component, which must inform the CA immediately.

4.9.2.2 Legal Person Certificate

Individuals or entities may request revocation of a server certificate are:

- The CM,
- A legal representative of the entity to which is attached the server,

- If appropriate, a Certification Agent,
- The CA,
- The RA or DRA operators.

The Certificate Manager is informed, particularly through the TCSU accepted by him/her, persons or entities that may request a revocation of the certificate for which he/she is responsible.

In addition, applicants, application service providers, or third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

4.9.3 Procedure for Revocation Request

4.9.3.1 CA Certificate

In case the CA decides to revoke the intermediate CA certificate (following the compromise of the private key of the CA), the latter informed by email all CMs that their certificates are no longer valid because one of the certificates in the certificate chain is no longer valid. This information will also be relayed directly from the entities and where appropriate their Certification Agent. The contact identified on the site of ANSSI (https://www.ssi.gouv.fr) is immediately informed in case of revocation of a certificate of the certification chain.

The revocation mechanism is described in the "Operational revocation request procedure". The process is detailed in the "Cryptographic key management procedure" and in the "Component certificate management procedure".

4.9.3.2 Legal Person Certificate

The revocation request is made by the RA, a Certification Agent or the CA. The revocation management function is available 24h/24 7D/7 for revocations online. For a request made from the customer area, the user authenticates with his/her account and select the certificate to be revoked.

For a request by mail, the following information must be included in the certificate revocation request (form to download on the website):
- The identity of the CM,
- The email address of the CM,
- The reason of the revocation.

If the CM or the Subject is not the subscriber:
- The first and last name of the subscriber,
- The quality of the subscriber (legal representative, if appropriate DRA operator or Certification Agent),
- The subscriber's phone number.

If the application is sent by mail, it must be signed by the subscriber (the signature is verified by the RA with that of the certificate request files).

If the request is made online, the empowerment of the person to perform this request is checked (authentication with the user account). In this case the person making the request can be:

- The CM,
- If appropriate, a Certification Agent,
- The CA,
- The RA or DRA operators.

The steps are:

- The applicant for revocation sends his/her request to the RA by mail or online,
- The RA authenticates and validates the revocation request to the requirements described in Chapter 3.4,
- The certificate serial number is registered in the CRL,
- In all cases, the CM is notified of the revocation by email,
- The transaction is recorded in the event logs with, if necessary, sufficient information on the underlying causes that led to the revocation of the certificate.

The CA can revoke a certificate presumed to exist, if revocation of the certificate is required under this Certification Policy, even if the final certificate does not actually exist. The CA is providing CRL and OCSP services and responses in accordance with this CP/CPS for all certificates presumed to exist based on the presence of a precertificate, even if the certificate does not actually exist.

From 10/01/2022, the reason for revocation of a certificate will be published in the CRL when one of the following revocation reasons is used:

- Key compromise,
- Privilege withdrawn,
- Cessation of operation,
- Affiliation changed,
- Superseded.

The CM is informed of the publication of the reason for revocation when requesting it to obtain his/her agreement. If none of these revocation causes is selected, the "CRLReason" field is set to "Unspecified (0)" by default and no "ReasonCode" extension is positioned in the CRL.

For reporting a malicious or dangerous certificate (suspected Private Key compromise, certificate misuse, or other types of fraud, compromise, inappropriate conduct, etc.) or any other matter related to certificates, use the contact form available at https://www.certigna.com/contactez-nous/ by selecting “Certificate considered malicious or dangerous”.

4.9.4 Revocation Request Grace Period

As soon as the CM or an authorized person has knowledge that a possible cause for revocation is effective, it must make its revocation request without delay.

4.9.5 Time within which CA Must Process the Revocation Request

4.9.5.1 CA Certificate

The revocation of a certificate of a PKI component is performed upon detection of an event described in the possible causes of revocation for this type of certificate.

The revocation of the signing CA certificate (signing certificates / CRL / OCSP responses) is performed immediately, particularly in the case of compromise of the key.

The organization and the means implemented in the event of revocation of a certificate of a component of the PKI are described in the "Cryptographic key management procedure" and in the "Component certificate management procedure".

4.9.5.2 Legal or Natural Person Certificate

In all cases, the maximum period for processing revocation request is 24 hours. This delay means between the receipt of the authenticated revocation request and the provision of revocation information from users.

Within 24 hours after receiving a certificate problem report, the CA investigates the facts and circumstances related to a certificate problem report and provides a preliminary report on its findings to both the Certificate Manager and the entity who filed the certificate problem report.

After reviewing the facts and circumstances, the CA works with the Certificate Manager and any entity reporting the certificate problem report or other revocation-related notice to establish whether the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the certificate problem report or revocation-related notice to published revocation will not exceed the time frame set forth in Section 4.9.1. The date selected by the CA can consider the following criteria:

- The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
- The consequences of revocation (direct and collateral impacts to Certificate Managers and Relying Parties);
- The number of certificate problem reports received about a particular certificate or Certificate Manager;
- The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered);
- Relevant legislation.

The revocation management function is available 24h/24 7D/7 for revocations online.

RGS *
The maximum downtime of the revocation management function: - per interruption (failure or maintenance) is 2 hours (workdays). - per month is 16 hours (workdays).

4.9.6 Revocation Checking Requirement for Relying Parties

The user of a server certificate must check before its use, the status of certificates of all the relevant certificate chain. The method used (CRL or OCSP) is at the discretion of the user based on their availability and constraints in its implementation.

4.9.7 CRL Issuance Frequency

CRLs are available via a publicly-accessible HTTP URL.

Within twenty-four (24) hours of issuing its first Certificate, the CA generates and publishes a full and complete CRL.

An ARL is issued at least every year. In addition, a new ARL is systematically generated and published within twenty-four (24) hours after the revocation of a CA certificate.

A CRL from an intermediate CA is issued at least every 24 hours. In addition, a new CRL is published systematically and immediately after the revocation of a certificate.

The CA continues to issue CRLs until all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; or the corresponding Subordinate CA Private Key is destroyed.

4.9.8 Maximum Latency for CRLs

An ARL or a CRL is issued within a maximum of 30 minutes after its generation.

4.9.9 On-line Revocation/status Checking Availability

In addition to the CRL publication on the online websites, CA make available an OCSP responder conform to RFC6960 and/or RFC5019. The OCSP responder meets the requirements of integrity, availability and deadline for the publication described in this CP/CPS.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdatefield, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

A certificate serial is “assigned” if:

- A Certificate or Precertificate with that serial number has been issued by the Issuing CA; or
- a Precertificate with that serial number has been issued by a Precertificate Signing Certificate, associated with the Issuing CA.

A certificate serial is “unassigned” if it is not “assigned”.

For the status of a Subscriber Certificate or its corresponding Precertificate, an authoritative OCSP response is available (i.e. the responder must not respond with the "unknown" status) starting no more than 15 minutes after the Certificate or Precertificate is first published or otherwise made available.

The information provided by OCSP responder for server certificates are updated every four (4) days at most, and OCSP responses are valid for seven (7) days. The CA provides an updated OCSP response at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

The information provided by OCSP responder for subordinate CA certificates are updated at least every twelve months and within 24 hours after revoking a subordinate CA certificate.

OCSP responders operated by the CA supports the "HTTP GET" method, as described in RFC 6960 and/or RFC 5019. OCSP responses are signed by an OCSP Responder whose certificate is signed by the CA that issued the certificate whose revocation status is being checked. OCSP responses are signed by an OCSP Responder which complies with the OCSP Responder Certificate Profile in Section 7.3.The OCSP signing Certificate contains an extension of type "id-pkix-ocsp-nocheck", as defined by RFC6960.

4.9.10 On-line Revocation Checking Requirements

Revoked and expired certificates are maintained ins CRLs and OCSP responders.

In addition to the CRL publication on the online websites, CA make available an OCSP responder available at the following addresses.

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

4.9.11 Other Forms of Revocation Advertisements Available

As part of the CERTIGNA OCSP Responder service, up to 250,000 OCSP requests are allowed per certificate per day. If this threshold is exceeded, CERTIGNA reserves the right to impose on the Certificate Manager the implementation of the *OCSP Stapling* mechanism on the server secured by the certificate. If the *OCSP stapling* is refused, CERTIGNA may revoke the certificate to maintain and guarantee the availability of the OCSP responder for all its customers.

Note - The *OCSP Stapling* mechanism consists of configuring the client's secure server so that it acts as a proxy for the OCSP interrogation, to drastically reduce the number of requests transmitted to the CA OCSP responder.

4.9.12 Special Requirements Re Key Compromise

The Certificates Manager or the Certification Agent must request the certificate revocation promptly after becoming aware of the compromise of the private key.

For CA certificates, in addition to the requirements of Section 4.9.3 above, the revocation following a compromise of the private key is being clear information distributed at least on the website of the CA and possibly relayed by other means (other institutional websites, newspapers, etc.). The implemented measures are defined in the "Cryptographic key management procedure" and in the "Component certificate management procedure".

The following methods may be used to report to the contact information described in section 4.9.3.2, a key Compromise of a CERTIGNA Certificate:

- Submitting a CSR signed by the Private Key and verifiable with the Public Key;
- Submitting a test file/challenge response signed by the Private Key and verifiable with the Public Key;
- Providing references to vulnerability and/or security incident sources from which the Compromise is verifiable;
- Submitting the Compromised Private Key to CERTIGNA. This method is not recommended but will be considered proof of Key Compromise.

CERTIGNA may allow additional methods that do not appear in this section at its own discretion and will update the CP/CPS if a new method is accepted.

4.9.13 Circumstances for Suspension

The certificates issued by the CA cannot be suspended.

4.9.14 Who can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Service

4.10.1 Operational characteristics

The CA provides to certificate users the information needed to verify and validate, prior to their use, the status of their certificates and all the corresponding certificate chain (up to and including Root CA), i.e. to also check the signatures of the certificates in the chain, signatures guaranteeing the origin and integrity of the CRL/LAR and the state of the certificate of Root CA. The information based on the status of certificates makes available to certificates users a free consultation mechanism CRL/ARL. These CRL/ARL are in CRL V2 format published on the publication website http://www.certigna.com (available with the HTTP protocol). The CRL and the OSCP responder can provide a different response as to the status of a certificate for a maximum of 30 minutes after its revocation has been validated. As a reminder, when a revocation is validated, the OCSP responder is updated immediately, while the CRL is produced and then published within a maximum of 30 minutes. The publishing service activities are defined in the "Publishing Service Management Procedure". Revocation entries on a CRL or OCSP Response are not removed until after the Expiry Date of the revoked Certificate.

4.10.2 Service Availability

The information function on the status of certificates is available 24/7. The CA maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

RGS *
The maximum downtime of the information function on the status of certificates: - per interruption (failure or maintenance) is 4 hours (workdays). - per month is 32 hours (workdays).

If check online of the status of a certificate, the OCSP server response time to the received request is a maximum of 10 seconds. This is the time measured at the server (request received by the server and response from the latter). The replication of services on several information systems ensures automatic continuity of services in the event of a disaster. The CA also relies on its staff on-call during non-working hours to supervise the availability alerts for these functions.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

In case of termination of the contractual or the statutory relationship between the CA and the entity attached to the server before the end of validity of the certificate, the certificate is revoked.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

The escrow of private keys is prohibited.

4.12.2 Session Key Encapsulation and Recovery Policy and Practice

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

REMINDER – CA conducted a risk analysis to determine the specific security objectives, to cover the business risks of the entire PKI, and technical and non-technical security measures to implement. Its CP/CPS was developed based on this analysis. This CP/CPS is established based on this risk analysis. The management of information security risks is described in the "IS Risk Management Procedure" and in the "IS Risk Management Form".

This CP/CPS also aims to comply with the current version of the « Network and Certificate System Security Requirements » from the CA/Browser Forum.

The CA develops, implements, and maintains a comprehensive Information Security Management System (ISMS) designed to:

- Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
- Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
- Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
- Comply with all other security requirements applicable to the CA by law.

The Certificate Management Process includes:

- physical security and environmental controls;
- system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
- network security and firewall management, including port restrictions and IP address filtering;
- user management, separate trusted-role assignments, education, awareness, and training; and
- logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

The ISMS includes an annual Risk Assessment that:

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the Risk Assessment, the CA develops, implements, and maintains an ISMS consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

The ISMS includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan also takes into account then-available technology and the cost of implementing the specific measures and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical Controls

5.1.1 Site Location and Construction

The information systems used for CA functions are hosted in several production centers with the same security features. The location of the sites does not present major risks.

The risks are identified in the document "Risk Management IS".

5.1.2 Physical Access

A strict control of physical access to the components of PKI is performed, with access logging and video surveillance: the defined security perimeter around the systems hosting the PKI components is limited to people within a trusted role on this PKI.

Outside working hours, the implementation of physical and logical intrusion detection means strengthening the security of the PKI. In addition, any person (external service provider, etc.) entering in this physically secure area cannot be left without the supervision of an authorized person. Physical access to production centers is restricted through physical access control measures. The measures implemented are described in the "Safety Policy".

5.1.3 Power and Air Conditioning

Measures concerning the supply of electricity and air conditioning are taken to meet the commitments of the CA described in this CP on ensuring the level of availability of its functions, including revocations management features and information functions on the status of certificates. The production centers are equipped with inverters and generators. The measures implemented are described in the "Safety Policy".

5.1.4 Water Exposures

Measures for protection against water damage are taken to address the CA commitments described in this CP/CPS on ensuring the level of availability of its functions, including revocations management functions and information functions on the status of certificates. Means for the detection of water leaks are positioned in the production centers. The measures implemented are described in the "Safety Policy".

5.1.5 Fire Prevention and Protection

Measures for prevention and protection against fire are taken to address the CA commitments described in this CP/CPS on ensuring the level of availability of its functions, including revocations management functions and information functions on the status of certificates.

The computer rooms of the production centers are equipped with inert gas extinguishing systems. The measures implemented are described in the "Safety Policy".

5.1.6 Media Storage

The information and their supporting assets involved in the activities of the IGC are identified, inventoried and their security needs defined in terms of availability, integrity and confidentiality.

The assets are listed in the "Asset Inventory" document, and the security requirements in the "IS Risk Management Form".

Specific measures are implemented to avoid compromise or theft of information. The assets corresponding to this information are managed according to procedures conforming to these security needs. They are handled in a secure manner to protect the assets from damage, theft and unauthorized access. Management procedures protect media against obsolescence and deterioration during the period during which the CA agrees to keep the information contained therein.

The measures implemented allow to cover the risks identified through the form “IS risk management”.

The "Security Policy", the "Asset Management Procedure" and the "Materiel Management Procedure" describe the measures implemented.

5.1.7 Waste Disposal

The measures taken for the disposal of media are compliant with the level of confidentiality of the corresponding information.

The "Security Policy", the "Asset Management Procedure" and the "Materiel Management Procedure" describe the measures implemented.

5.1.8 Off-site Backup

Outsourced backups are implemented and organized in such a way as to ensure that the IGC functions are available as soon as possible after an incident, and in accordance with the commitments of this PC, in particular regarding the availability and protection of the confidentiality and integrity of saved information.

The "Backup Procedure", the "Asset Management Procedure" and the "Materiel Management Procedure" describe the measures implemented.

5.2 Procedural Controls

5.2.1 Trusted Roles

Each PKI component distinguishes at least the seven following functional trust roles:

- **Security officer**: The security officer is responsible of implementing the component's security policy. He manages the controls on the physical access to the component's system hardware. He is authorised to review the archives and is responsible of analysing the event logs to detect any incident, anomaly, attempted compromise, etc.
- **Application manager**: Within the component to which he is attached, the application manager is responsible of implementing the certification policy and the declaration of the PKI's certification practices on the level of the application for which he is responsible. His responsibility includes all the functions provided by this application and the corresponding performances.
- **System administrator**: He is responsible of the start-up, configuration and technical maintenance of the component's IT hardware. He provides the technical administration of the component's systems and networks.
- **Operator**: Within a PKI component, based on his duties, an operator runs applications for the functions implemented by the component.
- **Controller**: Designated by a competent authority, this person's role is to regularly perform verifications on the compliance of the implementation of the functions provided by the component relative to the certification policies, to the PKI's declarations of certification practices, and to the component's security policies.
- **Registration Officer**: Responsible for approving end entity Certificate generation and revocation.
- **Secret share holder**: It has the responsibility to ensure the confidentiality, integrity and availability of the secrets assigned to him.

The different roles are defined in the description of functions specific to any entity operating a component of the PKI on the principles of separation of duties and least privilege. These roles determine the sensitivity of the functions, depending on responsibilities and access levels, background checks and employee training and awareness.

The documents "Roles, Responsibilities and Authorities", "Personnel Management Procedure" and "Staff Monitoring" describe the measures implemented.

Measures are in place to prevent equipment, information, media and software relating to CA services are removed from the site without permission.

The "Security Policy", the "Asset Management Procedure" and the "Materiel Management Procedure" describe the measures implemented.

5.2.2 Number of Individuals Required per Task

For reasons of availability, each task must be performed by at least two people. For some sensitive tasks like operations on HSM (e.g. key ceremony), many people are required for security reasons and "dual control."
The documents "Roles, Responsibilities and Authorities", "Personnel Management Procedure" and "Staff Monitoring" describe the measures implemented.

5.2.3 Identification and Authentication for Each Roles

Each role assignment to a member of the PKI staff is attributed and accepted formally. This role is clearly mentioned and described in his/her job description. CA checks the identity and permissions of any member of its staff before assigning privileges to its functions. Assigning a role to a member of staff following the PKI particularly strict procedure with signing of the minutes for the allocation of all elements necessary for the performance of this role in the PKI (keys, access codes, cryptographic keys, etc.).

The documents "Roles, Responsibilities and Authorities", "Personnel Management Procedure" and "Staff Monitoring" describe the measures implemented.

5.2.4 Role Requiring Separation of Duties

About trusted roles, the following rollups are prohibited within the PKI:

- Security officer and system administrator / operator,
- Controller and any other role,
- System operator and administrator.

The document "Roles, Responsibilities and Authorities", the "Personnel Management Procedure" and the "Staff Monitoring" document describe the measures implemented.

5.3 Personnel Controls

5.3.1 Qualifications, Experiences, and Clearance Requirements

All staff must work within the PKI components must sign the internal security charter. This charter contains a confidentiality clause which applies both in respect of third parties and users. It lists the roles of each employee within the PKI. She is co-signed by the employee and the security officer.

Matching skills of personnel involved in the PKI is checked in compliance with its duties on the components. The management personnel, the security officer, system administrators, have the expertise necessary for the performance of their respective roles and are familiar with the security procedures applied to the operation of the PKI. AC informs any employee involved in the PKI trusted roles of its responsibilities for PKI services and procedures related to system security and monitoring staff.

Professional skills are determined during recruitment and each year by Security Officers.

The documents "Roles, Responsibilities and Authorities", "Personnel Management Procedure" and "Staff Monitoring" describe the measures implemented.

5.3.2 Background Check Procedures

The CA ensures that all employees involved on the PKI suffered no contradiction in justice conviction with their functions. The employees provide a copy of the bulletin Number 3 before their Assignment of his/her criminal record. This check is renewed periodically (at least every 3 years). In addition, the CA ensures that the employees do not suffer from conflict of interests detrimental to the impartiality of their tasks. The CA can decide in case of refusal of the personnel to communicate this copy or in case of presence of a court judgment incompatible with the attributions of the personnel, to withdraw these attributions to them.

The documents "Roles, Responsibilities and Authorities", "Personnel Management Procedure" and "Staff Monitoring" describe the measures implemented.

5.3.3 Training Requirements

Initial training to software, hardware and internal operating and safety procedures is provided to employees, in line with the role that the CA assigns. An awareness on the implications of the operations whose they are responsible is also achieved.

The CA keeps records of the training provided and ensures that the personnel enrolled as the Registration Officer maintain a level of competence that allows them to carry out their missions. The CA ensures that the Registration Officers have the necessary skills before allowing them to carry out their missions and that each Registration Officer passes the evaluations provided by the CA on the verification of information related to the requirements of the CA / Browser Forum.

The document "Roles, Responsibilities and Authorities", the "Personnel Management Procedure" and the "Staff Monitoring" document describe the measures implemented.

5.3.4 Retraining Frequency and Requirements

The staff concerned receives adequate information and training prior to any changes in systems, procedures in the organization.

The document "Roles, Responsibilities and Authorities", the "Personnel Management Procedure" and the "Staff Monitoring" document describe the measures implemented.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Any member of the CA staff acting in contradiction with established policies and procedures and internal processes and procedures of the PKI, or negligently or maliciously, will see his/her privileges revoked and will be subject to administrative sanctions or judicial proceedings.

5.3.7 Independent Contractor Requirements

The staff of external providers involved in local and / or components of the PKI must also meet the requirements of this Section 5.3. This is translated into appropriate clauses in contracts with those providers. If so, whether the level of intervention requires, it may be asked to the provider to sign the IT charter and / or provide background check elements.

External staff are monitored through the "Third Party Management Procedure". An assessment of the IS risks related to the third parties is carried out and the security needs/requirements are mapped in order to be followed through the document "Third party monitoring" and the associated contractual agreements.

5.3.8 Documentation Supplied to Personnel

Each employee has the adequate documentation of operational procedures and specific tools that implements and general policies and practices of the component within which he/she works. The CA gives him/her the impacting security policies. Operators have the operator manuals corresponding to the components on which they are involved.

The document "Roles, Responsibilities and Authorities", the "Personnel Management Procedure" and the "Staff Monitoring" document describe the measures implemented for awareness and training, and the "Document Management Procedure" defined the management of these documents.

5.4 Audit Logging Procedures

Relevant events involved in the management and operation of the PKI are recorded in manuscript or electronically form (by seizure or by automatic generation) and, for purposes of audit.

5.4.1 Types of Events Recorded

The operating systems of the PKI servers will log the following events automatically on start-up and in electronic form (non-exhaustive list):

- Create / modify / delete user accounts (access rights) and corresponding authentication data,
- Start and stop IT systems and applications,
- Events related to logging: actions taken following a failure of the logging function,
- Connecting / disconnecting users with trusted roles, and corresponding unsuccessful attempts.

Other events are also collected. It is those concerning safety and not automatically generated by computer systems:

- Physical access,
- Logical access to PKI systems,
- PKI and security system actions performed,
- Actions of maintenance and configuration changes in systems,
- Installation, update and removal of software on a Certificate System,
- System crash, hardware failures, and other anomalies,
- Firewall and router activities,
- Cryptographic device (used for CA keys) lifecyle management events,
- Changes in personnel,
- Operation of disposal and reset of media containing confidential information (keys, activation data, personal information on Subscribers, and CMs).

Specific events to different functions of the PKI are also logged:

- Events related to signing keys and CA certificates or activation data (generation, backup and recovery, revocation, destruction, disposal of media, …),
- Introduction of a new Certificates Profiles and retirement of existing Certificate Profiles,
- Receiving a certificate request (initial and renewal),
- Events related to controls operated for certificate request validation, including:
  - the information being validated (e.g., the applied-for FQDN or the organization name);
  - the Authorization Domain Name used (if applicable and different from the applied-for FQDN); and
  - the validation method used (e.g., the CAB Forum Baseline Requirements section number or the registered label of an ACME validation method);
- Validation / reject a certificate request,
- Certificate generation of servers,
- Certificate transmission to CM and, if appropriate, acceptances / explicit releases by CMs,
- Publish and update information related to the CA (CP / CPS, CA certificates, Terms and Conditions, etc.),
- Receipt of requests for revocation,
- Validation / reject a request for revocation,
- CRL generation and publication,
- Signing of OCSP Responses (as described in Section 4.9 and Section 4.10),
- Disposal of media containing personal information on Subscribers, and CMs,

- Multi-Perspective Issuance Corroboration attempts from each Network Perspective, minimally recording the following information:
  - An identifier that uniquely identifies the Network Perspective used;
  - The attempted domain name and/or IP address; and
  - The result of the attempt (e.g., "domain validation pass/fail", "CAA permission/prohibition").
- Multi-Perspective Issuance Corroboration quorum results for each attempted domain name represented in a Certificate request (i.e., "3/4" which should be interpreted as "Three (3) out of four (4) attempted Network Perspectives corroborated the determinations made by the Primary Network Perspective).

The logging process allows real-time recording of the operations carried out.

Each record of an event in a journal contains at least the following fields:
- The type of event,
- The date and time of the event (the exact time of the significant CA events on the environment, key management and certificate management is recorded),
- The name of the executant or the reference of the system that triggered the event,
- The result of the event (success or failure).

Depending on the type of event, there are also the following fields:
- The recipient of the operation,
- the name of the applicant of the operation or the reference of the system which request
- The names of those present (for operations requiring several persons),
- The cause of the event,
- All the information characterizing the event (eg. Serial number of the certificate issued or revoked).

The logging process allows real-time recording of transactions. In case of manual input, writing is made exceptions the same business day as the event. The events and specific data to be logged are documented by the CA.

In case of manual entry, the writing is done, except exception, the same working day as the event.

The events and specific data to be logged are documented by the CA.
The measures implemented are described in the « Logging Procedure » and the « Archive Procedure ».

The CA makes these records available to its Qualified Auditor as proof of the CA's compliance with applicable requirements.

5.4.1.1 Router and firewall activities logs

Logging of router and firewall activities at a minimum include:
- Successful and unsuccessful login attempts to routers and firewalls; and
- Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and

- Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
- Logging of all system events and errors, including hardware failures, software crashes, and system restarts

5.4.2 Frequency of Processing Log

Cf. chapter 5.4.8

5.4.3 Retention Period for Audit Log

The retention period for event logs on site is 1 month. Archiving of event logs is made no later than 1 month after their generation.

5.4.4 Protection of Audit Log

Only members dedicated CA can process these files. The systems generate event logs (except for physical access control systems) are synchronized to a reliable source of UTC time (cf. 6.8. Timestamp / dating system).

Write access to the logs is protected through the logical and physical access controls described in the "Logging Procedure", the "Logical Access Control Policy" and the "Safety Policy".

The systems generate event logs (except for physical access control systems) are synchronized to a reliable source of UTC time (cf. 6.8. Timestamp / dating system).

The "Clocks Synchronization Procedure" describes the measures implemented.

5.4.5 Audit Log Backup Procedures

Security measures are implemented by any entity operating a PKI component to ensure the integrity and availability of event logs for the component considered, in accordance with the requirements of this CP/CPS. A backup is performed at high frequency to ensure the availability of such information.

5.4.6 Audit collection System (Internal or external)

Event logs are centralized in a hub. The consolidation obtained is accessible by CERTIGNA staff. The protection of the confidentiality and integrity of event logs is ensured by logical access control and the use of file sealing tools.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

An annual risk assessment is performed to:

- Identify foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes.
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
- Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

The event logs are monitored once per workday to identify abnormalities related to failed attempts (access or instruction).

Event logs are analysed in their entirety to the frequency of at least once every workday and upon detection of an abnormality. A summary analysis is produced for the occasion. A reconciliation between the various logs of functions that interact with each other is made at the rate of at least 1 time per week to verify the correlation between dependent events and to reveal any abnormality. The auditor is assisted by a person with skills related to the different environments used. The measures implemented are described in the « Logging Procedure ».

5.5 Records Archival

5.5.1 Types of Records Archived

CA is archiving:

- Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems,
- Documentation related to their verification, issuance, and revocation of certificate requests and Certificates,
- The software (executable) constituent of the PKI,
- IT equipment configuration files,
- Event Logs of various components of the PKI,
- The CP/CPS,
- The digital Certificate requests,
- The records of Certification Agent registration,
- The records of DRA operator registration,
- The certificate request files with credentials,
- The certificates issued,
- The requests for revocation,
- The CRL issued,
- The OCSP responses.

5.5.2 Retention Period for Archive

5.5.2.1 Certificates Application Files

All accepted certificate registration files are archived seven years minimum from the expiration of the certificate and as long as necessary for supply needs of the proof of certification in legal proceedings in accordance with applicable law, in particular Article 6-II of the implementing decree n ° 2001-272 of 30 March 2001. In this context, it is archived for at least seven years, as maximum from the expiration of the certificate. During this period of enforceability of documents, the certificate request files can be submitted by the CA in any solicitation by the competent authorities. The files, completed by the words recorded by the RA or Certification Agents, is traceable to find at an instant "t" the real identity of CM of the certificate issued by the CA in the certificate.

5.5.2.2 Certificates, CRL / ARL and OCSP responses issued by the CA

Certificates of servers and of CA and the CRL / ARL produced (respectively by the CA and Certigna Root CA), are archived for at least seven years after their generation. OCSP responses produced are archived for at least two years after their expiration.

OCSP responses are automatically destroyed after this delay.

5.5.2.3 Event logs

Event logs specified in Chapter 5.4 are archived for seven years after the expiration of the associated certificates. The archives are kept in multiple copies through the process of replication between production centers, which ensures the protection and availability of information. Electronic records are deleted (Periodic Process) after their retention period has passed.

The paper application files are physically destroyed. A clear archive procedure is performed on the different production centers once the retention time has been reached.

5.5.3 Protection of Archive

During the time of their conservation, the archives are protected in integrity. They can be played back and used by the dedicated members of the CA. Write access to these files is protected (rights management). Access to read the logs (stored on NetApp servers) is only possible from a machine identified and authorized in the internal networks.

5.5.4 Archive Backup Procedures

The mirroring process (automatic or manual in case of recovery) guarantees the existence of a backup of the entire archive.

To compensate for the impossibility of replication between the production sites, daily backups are carried out in order to guarantee the existence of a copy of the recorded data.

5.5.5 Requirements for Time-stamping of Records

The data are dated according to Chapter 6.8.

5.5.6 Archive Collection System (Internal or external)

Archiving is achieved with archiving servers which ensure the availability, integrity and confidentiality of archives.

The "Backup Procedure" and the "Archive Procedure" describe the measures implemented.

5.5.7 Procedures to Obtain and Verify Archive Information

Archives can be recovered only by the dedicated members of the CA authorized to process these files within a maximum of two workdays. Data about contractors can be retrieved on their request.

5.6 Key Changeover

5.6.1 CA Key

The CA cannot generate a certificate for which the end date is later than the expiration date of the certificate corresponding to the CA. For this, the validity period of the CA certificate must be higher than the certificate that it signs. Knowing the date of expiry of the certificate, renewal must be requested within a delay at least equal to the lifespan of the certificates signed by the corresponding private key.

When a new CA key pair is generated, only the new private key is used to sign certificates. The previous certificate can still be used to validate certificates issued under this key until that all certificates signed with the corresponding private key have expired.

The CERTIGNA PKI communicate on its website in case of generation of a new certificate for the CA or CERTIGNA Root CA, inviting users to download the new certificate chain.

The "Cryptographic Key Management Procedure" and the "Key monitoring" document describe the measures implemented.

5.6.2 Keys of the Other Components

The associated key pairs and certificates of the PKI components are renewed in the three months before their expiry or after revocation of the certificate valid.

5.7 Compromise and Disaster Recovery

The CA establishes procedures to maintain activities, wherever possible, and described in these procedures, the steps provided in case of corruption or loss of computing resources, software and data. These procedures are formalized as part of the implementation of Business Continuity Plans. In particular for the major risks identified, these plans address the immediate treatment in the case of strong constraints of service availability required by the CP/CPS. The operation of a supervisory monitor ensures that incidents are detected and taken into account in real time at both production sites.

5.7.1 Incident and Compromise Handling Procedures

5.7.1.1 Incident Response and Disaster Recovery Plans

In the event of a major incident, such as loss, suspicion of compromise, compromise, theft of the private key of the CA, the triggering event is the finding of this incident in the component concerned, which must inform the CA immediately.

The case of major incidents is imperative treated when detected, and the publication of the certificate revocation information, if any, will be made in the most urgent, if not immediately, by all appropriate and available means (press, website, receipt, etc.).

Similarly, if one of the algorithms, or associated parameters, used by the CA or its promoters / servers becomes insufficient for its intended use remaining, then the CA:

- Inform all CMs and third certificate users with whom the CA has agreements or other forms of established relationships. In addition, this information must be made available to other users of certificates,
- Revoke any certificate concerned.

The "Incident Management Procedure" and the "Business Continuity Plans" describe the measures implemented.

Business continuity plan is reviewed, updated, and tested annually through one or more simulated disaster scenarios. The business continuity plan includes:

- The conditions for activating the plan,
- Emergency procedures,
- Fallback procedures,
- Resumption procedures,
- A maintenance schedule for the plan,
- Awareness and education requirements,
- The responsibilities of the individuals,
- Recovery time objective (RTO),
- Regular testing of contingency plans.
- The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes,

- A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location,
- What constitutes an acceptable system outage and recovery time,
- How frequently backup copies of essential business information and software are taken,
- The distance of recovery facilities to the CA's main site; and
- Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

5.7.1.2 Mass Revocation Plans

The CA maintains a comprehensive and actionable plan for mass revocation events.

The CA performs annual testing of the mass revocation plan and incorporates lessons learned into this plan in order to continually improve the preparedness for mass revocation events over time.

The CA's mass revocation plan includes clearly defined, actionable, and comprehensive procedures designed to ensure rapid, consistent, and reliable response to large-scale certificate revocation scenarios. The CA is not required to publicly disclose its mass revocation plan or procedures but makes it available to its auditors upon request.

The CA annually tests, reviews, and updates its plan and such procedures.

The CA's mass revocation plan may be integrated into the CA's incident response, business continuity, disaster recovery, or other similar plans or procedures, provided that provisions governing mass revocation events remain clearly identifiable and satisfy these requirements.

Mass revocation provisions include:

1. Activation criteria: specific, objective, and measurable thresholds at which the mass revocation plan is triggered based on the CA's risk profile, issuance volumes, and operational capabilities;
2. Customer contact information: how subscriber and customer contact details are stored, maintained, and kept up to date;
3. Automation points: processes that are automated or could be automated, and those processes that require manual intervention;
4. Targets and timelines: for incident triage, revocation initiation, certificate replacement, and post-event review;
5. Subscriber notification methods: mechanisms for notifying impacted Subscribers;
6. Role assignments: roles and responsibilities of personnel responsible for initiating, coordinating, and executing the plan;
7. Training and education: training, awareness, and readiness activities for personnel responsible for, or supporting, the plan;
8. Plan testing: annual operational testing to assess readiness and demonstrate implementation feasibility, using one or more of tabletop exercises, simulations, parallel testing, or controlled test environments that do not involve the revocation of active Subscriber Certificates; and
9. Post-test analysis and update schedule: how lessons learned from testing or live incidents are incorporated into the plan, and how often it is reviewed and updated.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

Each component of the PKI is integrated into the business continuity plan (BCP) of the company to meet the availability requirements of the various functions of the PKI under the CA commitments and results of the analysis risk of PKI, especially regarding the functions related to the publication and / or related to the revocation. This plan is tested at least once every two years. The "Incident Management Procedure" and the "Business Continuity Plans" describe the measures implemented.

5.7.3 Recovery Procedures After Key Compromise

The case of compromise of a key infrastructure or control of a component is treated in the business continuity plan of the component as a disaster (see Section 5.7.2).

In the case of compromise of a CA key, the corresponding certificate will be immediately revoked (see section 4.9).

Similarly, all valid Server certificates issued by this CA will be revoked. In addition, the CA meets at least the following commitments:

- It shall inform the following entities of the compromise: all CMs, Certification Agent and other entities with which the CA has agreements or other forms of established relationships, including third-party users and others CA. In addition, this information is made available to other third-party users,
- It shall inform especially that certificates and revocation status information issued using this CA key may no longer be valid.

Note: In the case of Certigna Root CA, the signing certificate is not revoked, it is the intermediate CA certificates that are revoked in case of compromise of the private key of the Certigna Root CA.

The "Cryptographic Key Management Procedure", the "Incident Management Procedure" and the "Business Continuity Plans" describe the measures implemented.

5.7.4 Business Continuity Capabilities after a Disaster

The various components of the PKI have the necessary means to ensure the continuity of their activities in accordance with the requirements of the CA Certification Policy. CA uses the redundancy of its information systems into several sites and its business continuity plans to ensure the services continuity.

The measures are described in the "Business Continuity Plans".

5.8 CA or RA Termination

One or more components of the PKI may have to stop working or to transfer it to another entity. The transfer of activity is defined as:

- The End of the activity of a PKI component having no effect on the validity of certificates issued prior to the transfer in question;
- The resumption of this activity organized by the CA in collaboration with the new entity.

The cessation of activity is defined as the end of the activity of a PKI component influencing the validity of certificates issued prior to the relevant termination.

5.8.1 Transfer of Activity or Cessation of Activity Affecting a Component of the PKI

One or more components of the PKI may have to stop working or to transfer it to another entity. To ensure a constant level of confidence during and after such events, the CA takes the following actions:

- It ensures the continuity of the archive service, especially certificates and registration records;
- It ensures the continuity of the revocation service, in accordance with the availability requirements for its functions under this CP/CPS;
- It informs CMs if the proposed changes may affect the commitments and that, at least in the period of 1 month;
- It informs application managers listed in Chapter 1.4.1 the principles of the action plan for dealing with the cessation of business or to organize the transfer of activities;
- It carries information to the administrative authorities. In particular, contact of the ANSSI is warned (https://www.ssi.gouv.fr). The CA will inform him including any obstacles or additional delay encountered during the process of transfer or retirement.

The "Incident Management Procedure" and "Business Continuity Plans" describe the measures implemented in detail.

5.8.2 Cessation of Activity Affecting the CA

In the event of termination of total activity, before the CA stops its services, it does the following:

- It informs all the CMs, the other components of the PKI and third parties by email of the cessation of activity. This information will also be relayed directly to the entities and if appropriate their Certification Agent;
- It revokes all certificates it has signed and which are still valid;
- It revokes its certificate;
- It destroys the private key stored in the cryptographic module and the context of the module. Holders of secret (private key and context) are summoned and destroy their secrets. It also prohibits transmitting the key to third parties.

If the CA is bankrupt, it is the commercial court which decides on the follow-up to the company's operations. Nevertheless, if any, CA is committed to supporting the commercial court under the following conditions: before bankruptcy, there is a prior period, generated most of time by several alert procedures or by a legal redress; during this period, CA is committed to preparing for the commercial court, if appropriate, a proposal to transfer digital certificates to another authority with the same level of certification.

The contact identified on the website of the ANSSI (https://www.ssi.gouv.fr) is immediately informed in case of cessation of trading of the CA. The "Incident Management Procedure", the "Business Continuity Plans", and the "Transfer and Cessation Procedure" describe the measures implemented.

5.8.3 Accessibility of revocation status beyond the end of validity

The CA undertakes to always ensure the availability of the revocation status and beyond the certificate validity period, by complying with the following practices:

- After expiration of an eIDAS-qualified certificate:
  - The published CRL will include the "ExpiredCertsOnCRL" extension, as provided for in the ITU-T X.509 recommendation; and will contain the serial numbers of all revoked certificates, including certificates that expired after revocation.
  - If an OCSP responder is implemented on this CA, OCSP responses will include the "archive cutoff" extension, as provided for in RFC 6960, with a date identical to the CA certificate's validity start date, and the certificate's revocation status will be kept available after its expiration.
- If the key of the CA issuing an eIDAS qualified certificate is about to expire:
  - Unexpired certificates issued by this CA will be revoked if their end date of validity period is greater than that of CA.
  - A final CRL will be published with an end of validity date of December 31st 9999, 23h59m59s ("99991231235959Z").
  - If an OCSP responder is implemented on this CA, a last OCSP response will be pre-generated for each certificate issued, with an end of validity date of December 31st 9999, 23h59m59s ("99991231235959Z").

    These measures will be implemented even if CERTIGNA ceases to provide the eIDAS qualified trust service, without transferring it to another eIDAS qualified trust service provider.

- If CERTIGNA ceases to provide the eIDAS qualified trust service, without transferring it to another eIDAS-qualified trust service provider, CERTIGNA is not obliged to maintain the publication of CRLs or to maintain the OCSP service, but the CRLs and/or OCSP responses produced will be made available to CERTIGNA's customers under conditions that guarantee their integrity. These measures will be made public if the situation should arise.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

This chapter describes the key pair generation context of the CA.

The generation of CA signing key is performed in a secure environment (see Chapter 5). The CA signing keys are generated and implemented in a cryptographic module complies with the requirements of Chapter 10.

The generation of CA signing key is performed under perfectly controlled circumstances by people in trusted roles (see Section 5.2.1), as part of "key ceremony".

The ceremony took place following a predefined script:

- It takes place under the control of at least two persons with a trusted role within the PKI and in the presence of several witnesses whom at least two are externed of the CA and are impartial;
- Witnesses testify in an objective and factual manner, the order of the key ceremony in relation to previously defined script.

For CA Key Pairs that are either used as a CA Key Pair for a Root Certificate or used as a CA Key Pair for a Subordinate CA Certificate, where the Subordinate CA is not the operator of the Root CA or an Affiliate of the Root CA, the CA:

- prepare and follow a Key Generation Script,
- have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process, and
- have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

The generation of CA signing key is accompanied by the generation of secret share. PKI's secrets are data to manage and manipulate, subsequently to the key ceremony, the private signing keys of the CA to later initiate new cryptographic modules with the signing key of the CA. These secrets are parts of the private key of the CA decomposed per a Shamir's threshold scheme.

After their generation, the secrets are issued to their holders designated in advance and skills to this trusted role by CA. One carrier can hold only one secret of the same CA. Secrets are placed in sealed envelopes, placed in vaults. Key ceremony scripts and the distribution of secret shares are monitored and documented. The "Cryptographic Key Management Procedure" and the "HSM Management Procedure" describe the measures implemented.

6.1.1.2 RA Key Pair Generation

No stipulation.

Note: The RA uses as much as possible the final certificates issued by the Cas covered by this CP/CPS to authenticate its personnel and secure its services.

6.1.1.3 Legal Person Key Pair Generation

The CM is committed by contract, accepting the TCSU, to:

- generate the private key in a device which meets the requirements of Section 11.
- comply with requirements for the device he uses to generate and store the private key, if it is not provided by the CA.

The CA will take any necessary measures to obtain technical information about the device of the CM and reserves the right to reject the certificate request if it is found that this device does not meet these requirements.

The CA rejects a certificate request if:

- The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
- There is clear evidence that the specific method used to generate the Private Key was flawed;
- The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
- The CA has previously been notified that the Applicant's Private Key has suffered a Key Compromise using the CA's procedure for revocation request as described in Section 4.9.3 and Section 4.9.12;
- The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, at least the following precautions are implemented:
  - In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), the CA rejects all keys found at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of Section 6.1.5, with the exception of RSA key sizes greater than 8192 bits, the CA rejects Debian weak keys.
  - In the case of ROCA vulnerability, the CA rejects keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.
  - In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), the CA rejects weak keys which can be factored within 100 rounds using Fermat's factorization method.

If the Certificate will contain an extKeyUsage extension containing either the values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280], the CA do not generate a Key Pair on behalf of a Subscriber, and do not accept a certificate request using a Key Pair previously generated by the CA.

Parties other than the CM do not archive the Private Key without authorization by the CM. If the CA or any of its designated RAs become aware that a legal person Private Key has been communicated to an unauthorized person or an organization not affiliated with the Legal Person, then the CA revokes all certificates that include the Public Key corresponding to the communicated Private Key.

6.1.2 Private Key Delivery to Subscriber

The CM generates the server's private key.

Parties other than the Subscriber shall not archive the Subscriber Private Key without authorization by the Subscriber.

If the CA or any of its designated RAs become aware that a CM Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subject of the Certificate, then the CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.1.3 Public Key Delivery to Certificate Issuer

The key pair is not generated by the CA, the certificate request (PKCS # 10 format) containing the key of the server, is sent to the CA by the CM. This request is signed with the private key, which enables the RA to verify its integrity and ensure that the CM has the private key associated with the public key transmitted in this request. Once these checks are complete, the RA signs the request and sends it to the CA.

6.1.4 CA public Key Delivery to Relying Parties

The issuance of public key of the CA, which allows all those who need to validate a certificate issued by the CA under the CP/CPS, is made by means ensuring integrity and authentication of the public key.

The public key of an intermediate CA is broadcast in a certificate signed by the Root CA. The public key of the Root CA is distributed in a self-signed certificate. These public CA keys and their control values are disseminated and retrieved by the information systems of all certificates acceptors through the Certigna website at https://www.certigna.com. See Section 2.2.1.2.

6.1.5 Key Sizes

6.1.5.1 Root CA Certificate

- Digest algorithm: SHA-256,
- RSA modulus size (bits): 4096

6.1.5.2 Subordinate CA Certificate

- Digest algorithm: SHA-256, or SHA-384 for new CAs
- RSA modulus size (bits): 4096

6.1.5.3 Legal Person Certificate

- Digest algorithm: Equal or superior to SHA-256 (SHA-256, SHA-384 or SHA512)
- RSA modulus size (bits): 2048, 3072 or 4096 (see Certificate profiles in section 7)

6.1.6 Public Key Parameters Generation and Quality Checking

The parameters and signature algorithms implemented in cryptographic boxes, physical media and software are documented by CA. The CA confirms that the value of the public exponent is an odd number is superior to 3 and is in the range between $2^{16}+1$ and $2^{256}-1$.

6.1.6.1 CA Key

The key pair generation equipment uses parameters respecting the safety standards corresponding to the key pair.

6.1.6.2 Legal Person Key

The key pair generation equipment used by the CM uses parameters respecting the safety standards corresponding to the key pair.

6.1.7 Key Usage Purposes (as per X.509 v3 Key usage field)

6.1.7.1 CA Key

The use of the private key of the root CA and associated certificate is exclusively limited to signing the root CA certificate, intermediate CA certificates and ARLs. The use of the private key of the CA and associated certificate is exclusively limited to signing legal and natural person certificates, CRLs, and OCSP responder certificate.

6.1.7.2 Legal Person Key

The use of the server private key and the associated certificate is exclusively limited to the usages defined at chapter 1.5.1. Otherwise, their responsibility could be engaged.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Modules Standards and Controls

6.2.1.1 Cryptographic Modules

The cryptographic module used by the Root CA and CA for the generation and the implementation of their signing keys are compliant with the requirements of the Section 10. These devices are resources exclusively available for CA's servers through a dedicated VLAN. The "HSM Management Procedure" describes the measures implemented. The CA implements physical and logical safeguards to prevent unauthorized certificate issuance.

6.2.1.2 Device to protect Legal Person private key

The device used by the CA, the CM to protect the private key is compliant with the requirements of the Section 11. In the case where the CA provides the device to the CM, directly or indirectly, CA ensure that:

- The device preparation is controlled securely;
- The device is stored and provided securely;
- The deactivation and reactivation of the device is controlled securely.

6.2.2 Private Key (n out of m) Multi-Person Control

Control of CA signature private key is provided by trusted personnel and with a tool implementing sharing secrets (systems where n operators of m must authenticate, with n at least equal to 2). The "HSM Management Procedure" and the "Cryptographic Key Management Procedure" describe the measures implemented.

6.2.3 Private Key Escrow

6.2.3.1 CA Key

The CA private keys are never escrowed.

6.2.3.2 Legal Person Key

The escrow of private keys is prohibited.

6.2.4 Private Key Backup

6.2.4.1 CA Key

The private key of the CA is saved:

- Inside one or several cryptographic modules compliant with the requirements of the Section 10.
- Outside the cryptographic module enciphered by the module and dispatched to several persons in trusted roles.

6.2.4.2 Legal Person Key

Private keys of the servers are not held by Certigna.

6.2.5 Private key archival

6.2.5.1 CA Key

The private key of the CA is never archived.

6.2.5.2 Legal Person Key

Private keys servers are not held or archived by Certigna.

6.2.6 Private Key Transfer into or from a Cryptographic Module

6.2.6.1 CA Key

The CA private keys are generated in the cryptographic module. As described in Section 6.2.4, the CA private keys are exportable / importable from the cryptographic module in encrypted form. If the CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the CA revokes all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.6.2 Legal Person Key

The server private keys are generated under the responsibility of the CM.

6.2.7 Private Key Storage on Cryptographic Module

6.2.7.1 CA Key

The root CA private key is generated in a cryptographic module described in chapter 6.2.1 and is exported in accordance with the requirements of chapter 6.2.4 in order to be continuously taken offline. The key is reconstituted in the cryptographic module to allow the annual generation of ARLs or

the creation of a new intermediate authority, then deleted from the module once the operation is complete. The "HSM Management Procedure" and the "Cryptographic Key Management Procedure" describe the measures implemented.

6.2.7.2 Legal Person Key

The server private keys shall be generated and stored by the CM in a device compliant with the requirements from the Section 11.

6.2.8 Method of Activating Private Key

6.2.8.1 CA Key

Activation of CA private key in the cryptographic module is controlled via activation data (see Section 6.4) and involves two people with a trusted role within PKI. The "HSM Management Procedure" and the "Cryptographic Key Management Procedure" describe the measures implemented.

6.2.8.2 Legal Person Key

Activation of key pairs is controlled by activation data (cf. chapter 6.4) under the CM responsibility.

6.2.9 Method of Deactivating Private Key

6.2.9.1 CA Key

The cryptographic module resists physical attacks by erasing the CA private keys. The module can detect the following physical attacks: Opening the device, removing or forcing.

6.2.9.2 Legal Person Key

The method of disabling the private key depends on the cryptographic module used by the CM.

6.2.10 Method of Destroying Private Key

6.2.10.1 CA Key

End of life of a CA private key, normal or anticipate (revocation), the key and the secrets of shares to reconstruct are systematically destroyed. A record of key and secret destruction is established at the end of this procedure. The measures implemented are described in the "Procedure for managing cryptographic keys".

6.2.10.2 Legal Person Key

The CM is the sole owner of the private key and is the only one who can destroy it (deletion of the key or physical destruction of the device).

6.2.11 Cryptographic Module Rating

6.2.11.1 CA Key

The assessment level of the CA cryptographic module is specified in Section 10.

6.2.11.2 Legal or Natural Person Key

The assessment level of the device used, if applicable, by the CM, is specified in Section 10.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public keys of the CA and of the legal persons are stored within the archival of relevant certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1 CA Key Pair and Certificate

Root CAs	Validity period of the certificate
Certigna	20 years maximum
Subordinate CAs	10 years maximum
Certigna Root CA	20 years maximum
Subordinate CAs	18 years maximum
Certigna Server Authentication Root CA	15 years maximum
Subordinate CAs	15 years maximum
Certigna Server Authentication EU Root CA	15 years maximum
Subordinate CAs	15 years maximum

The end of validity of a CA certificate is later than the end of life of end-entity certificates it issues.

6.3.2.2 Legal Person Key Pair and Certificate

The validity period of issued server certificates is determined based on their date of issue and defined in the table below.

Certificate issued		Validity period of the certificate
after	**and before**	
September 1, 2020	March 15, 2026	Maximum 398 days
March 15, 2026	March 15, 2027	Maximum 200 days
March 15, 2027	March 15, 2029	Maximum 100 days
March 15, 2029		Maximum 47 days

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.1 Generation and Installation of Activation Data Corresponding to the Private Key of the CA

Generation and installation of activation data of the cryptographic module of the CA are performed during the initialization and customization phase of the module (see chapter 6.1.1).

The "HSM Management Procedure" and the "Cryptographic Key Management Procedure" describe the measures implemented.

6.4.1.2 Generation and installation of activation data corresponding to the private key of the server

The key pair is generated and installed by the CM.

6.4.2 Activation Data Protection

6.4.2.1 Protection of Activation Data Corresponding to the CA Private Key

Activation data are directly provided to secret holders during the key ceremonies. Their storage conditions ensure their availability, integrity and confidentiality. The secrets are stored in devices with limited access, in secure envelopes to detect any unauthorized opening and traced. The "HSM Management Procedure" and the "Materiel Management Procedure" describe the measures implemented.

6.4.2.2 Protection of Activation Data Corresponding to Private Key of Legal Person

The key pair is generated and installed by the CM.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

A minimum level of safety assurance on the computer systems of persons in trusted role is ensured by:

- Strong and multi-factor identification and authentication of user for system access (E.g., physical access control to enter in the room + logic control by id / password or certificate to access the system);
- Management of user sessions (logoff after idle time, file access controlled by role and user name);
- User rights management (to implement the access control policy defined by the CA, to implement the principles of least privilege, multiple controls and separation of roles);
- Protection against computer viruses and other forms of compromise or unauthorized software and software updates using the firewall;
- Manage user accounts, including changes and the rapid removal of access rights;
- Network protection against intrusion of an unauthorized person using the firewall;
- Secure inter-sites communication (tunnel IPSec VPN) ;
- Audit Functions (non-repudiation and nature of the actions performed).

Monitoring devices and audit procedures of the system settings, including routing elements, are in place. The "Safety Policy", the "Logical Access Control Policy", the "Security Charter", the "Firewall Management Procedure" describe the measures implemented.

System configurations are analysed daily by the entity's tools, which reset any configuration for which an anomaly is identified. The configuration models deployed on the systems by these tools are reviewed at least once a year.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

According to the risk analysis conducted, during the design of any new development project, an analysis of security is achieved and approved by the CA Security Committee. The configuration of CA

systems and any changes and upgrades are documented. The development is done in a controlled and secured environment requiring a high level of authorization.

To enable its prospects or future customers to test some of their dematerialized trading applications, CA has set up a test CA issuing certificates identical in all respects to the production certificates (only the certificate issuer is different). This test CA has its own private key. The public key certificate is self-signed. These certificates are used for testing purposes only.

The CERTIGNA solutions are tested in a development/test environment before being used in the production environment. Production and development environments are separated.

The description of the evolution context of the PKI is defined in the "Procedure for updating the technical platform". Developments of the modules related to the exploitation of the components of the PKI are carried out in accordance with the rules and instructions enacted in the "Development Guide".

When the CA uses Linting software developed by third parties (i.e. pkimetal linter), the CA monitors for updated versions of that software and plans for updates no later than three (3) months from the release of the update. The CA can perform Linting on the corpus of its unexpired, un-revoked Subscriber Certificates whenever it updates the Linting software.

6.6.2 Security Management Controls

Any significant change to a system of a component of the PKI is documented and reported to the CA for validation.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

This CP/CPS also aims to comply with the current version of the « Network and Certificate System Security Requirements » from the CA/Browser Forum. Interconnection to public networks is protected by security gateways configured to accept only the necessary protocols to the desired operation by CA. The CA guarantees that the components of the local network are kept in a physically secure environment and their configurations are periodically audited for compliance with the requirements specified by the CA. The "Firewall Management Procedure", the "Monitoring Management Procedure" and the "Logical Access Control Policy" describe the measures implemented.

6.8 Time-stamping

To ensure synchronization between different dating of events, the various components of the PKI synchronize their clocks with respect to a reliable source of UTC time. The "Clocks Synchronization Procedure" describes the measures implemented.

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate profile

The CA meets the technical requirements set forth in:

- Section 6.1.5 - Key Sizes, and
- Section 6.1.6 - Public Key Parameters Generation and Quality Checking.

The CA generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG. The certificates and CRLs generated by the CA comply with ITU-T Recommendation X.509 v3 standard, RFC 5280 and applicable requirements from EN 319 412 ETSI specifications.

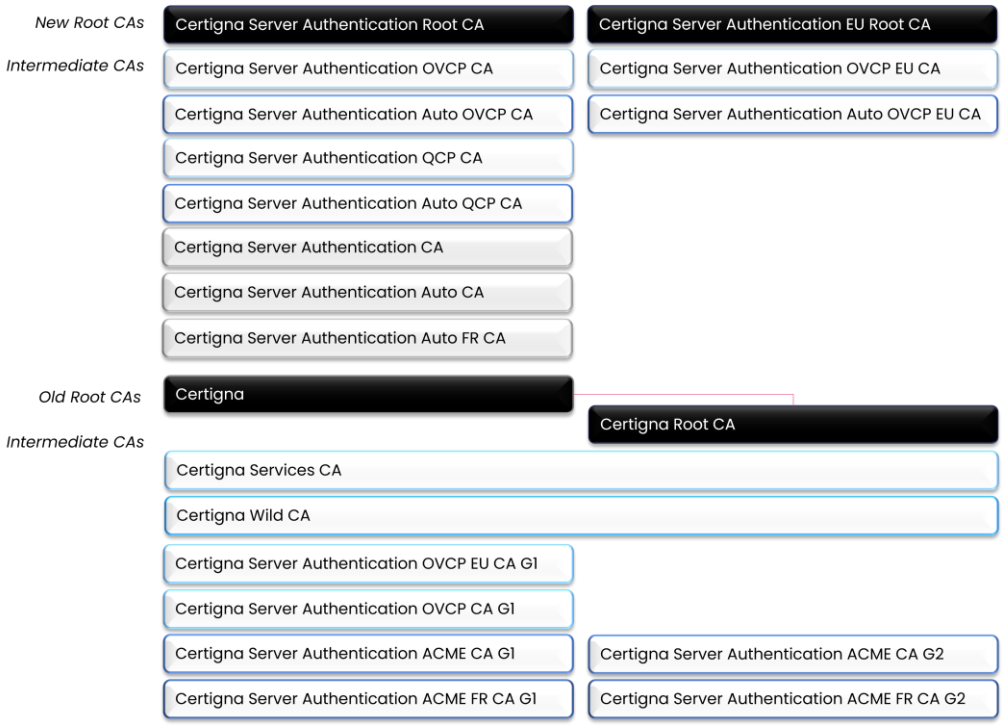
CERTIGNA has the following root CAs:

- The historical "Certigna";
- The current "Certigna Root CA" (also signed by Certigna: Cross signing),
- The new dedicated to TLS “Certigna Server Authentication Root CA”,
- The new dedicated to the European TLS “Certigna Server Authentication EU Root CA”.

Effective July 1, 2023, the CA shall not sign SHA-1 hashes over:

- certificates with an EKU extension containing the id-kp-ocspSigning key purpose;
- intermediate certificates;
- OCSP responses;
- or CRLs.

The trusted hierarchy is composed with following certificates and authorities:



7.1.1 Version number(s)

Certificates are of type X.509 v3.

7.1.2 Certificates extensions

See requirements for all profiles in section 7.10.

7.1.2.1 Processing certificates extensions by applications

Extensions defined for X509 V3 certificates are used to associate additional information with a public key, relating to the subject or the CA.

7.1.2.2 Criticality

The criticality character must be treated as follows depending on whether the extension is critical or not:

- If the extension is uncritical, then:
  - If the application does not recognise the OID, the extension is abandoned but the certificate is accepted;
  - If the application recognizes the OID, then:
    - If the extension is compliant with what the application wants to do, the extension is processed.
    - If the extension is not compliant with what the application wants to do, the extension is abandoned but the certificate is accepted.
  - If the extension is critical, then:
    - If the application does not recognise the OID, the certificate is rejected.
    - If the application recognizes the OID, then:
      - If the extension is compliant with what the application wants to do, the extension is processed.
      - If the extension is not compliant with what the application wants to do, the certificate is rejected.

7.1.2.3 Extension description

Authority Key Identifier: This extension identifies the public key used to verify the signature on a certificate. It differentiates the different keys used by the CA when it has multiple signing keys. The authorityKeyIdentifier field is necessarily informed. It contains a unique identifier (keyIdentifier). This CA key identifier has the same value as the subject-field KeyIdentifier of the CA certificate. The authorityCertIssuer authorityCertSerialNumber fields are blank.

Subject Key Identifier: This extension identifies the public key of the subject associated with the certificate. It allows to distinguish the different keys used by the subject. Its value is the value in the field keyIdentifier.

KeyUsage: This extension defines the intended use of the key contained in the certificate. CA Indicates the intended use of the key and manages the criticality as defined in section 7.2.

Extended Key Usage: This extension defines the advanced use of the key.

CertificatePolicies: This extension defines the certification policy following which the certificate was created. This field is processed during the validation of the certification chain. The CA includes the policyInformation field by filling the policyIdentifier field with the OID of the CP/CPS.

CRL Distribution Points: This extension identifies the location where the user can find the CRL indicating that the certificate has been revoked. The CA includes as many distributionPoint fields than it offers access mode to CRL. Each of these fields includes the uniformRessourceIdentifier of the CRL.

Authority Information Access: This extension identifies (with Method = OCSP) the location of OCSP server(s) providing information on the status of certificates, and the CA with providing a link to its certificate.

Basic Constraints: This extension indicates whether the certificate is an end entity certificate or an authority certificate.

Certificate Transparency: This extension allows to control the registration of the certificate in the logs used for the "Certificate Transparency".

7.1.3 Algorithm object identifiers

7.1.3.1 SubjectPublicKeyInfo

7.1.3.1.1 RSA

The CA indicates an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameter is present and is an explicit NULL. The CA do not use a different algorithm, such as the id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10) algorithm identifier, to indicate an RSA key. When encoded, the AlgorithmIdentifier for RSA keys is byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500

7.1.3.2 Signature AlgorithmIdentifier

7.1.3.2.1 RSA

For TLS, S/MIME and Code Signing certificates, the CA uses one of the following signature algorithms and encodings:

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

Prior to 2026-09-15, the CA will revoke any unexpired Subordinate CA Certificate that contains RSASSA-PKCS1-v1_5 with SHA-1 within the Certificate.

7.1.4 Name forms

Attribute values are encoded according to RFC 5280.

7.1.4.1 Name encoding

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate is byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA Certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate is byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

7.1.4.2 Subject information - subscriber certificates

See requirements for all profiles in section 7.10.

7.1.5 Name Constraints

No stipulation. See requirements for all profiles in section 7.10.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers

The following Certificate Policy identifiers are reserved to assert that a Certificate complies with CA\Browsers Requirements.

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

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

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

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

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

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the critical Certificates Policies Extension

No stipulation.

7.1.10 Profile of Root CA Certificates

7.1.10.1 Basic fields

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

7.1.10.2 Extensions

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

7.1.11 Profile of Intermediate CA certificates

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

		SERVER AUTHENTICATION EU ROOT CA	
Authority		SERVER AUTHENTICATION OVCP EU CA	SERVER AUTHENTICATION AUTO OVCP EU CA
Fields		**Description**	
Version		V3	
Serial Number		Unique serial number	
Signature		CA signing algorithm identifier / SHA-384 RSA 4096	
Subject Public Key Info		RSA 4096	
Validity		15 years	
Issuer DN	CN = O = C =	Certigna Server Authentication EU Root CA Certigna FR	
Subject DN	CN =	Certigna Server Authentication OVCP EU CA	Certigna Server Authentication Auto OVCP EU CA
	OI =	NTRFR-48146308100036	
	O =	Certigna	
	C =	FR	
SKI	No	CA public key identifier	
AKI	No	Root CA Public key identifier	
Certificate Policies	No	OID=2.23.140.1.2.2 (OV) OID=1.2.250.1.177.14.0.1.1 CPS = http://cps.certigna.com/	
Authority Informat. Access	No	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationEURootCA.cer	
CRL Distribution Points	No	URL=http://crl.certigna.com/CertignaServerAuthenticationEURootCA.crl	
Basic Constraints	Yes	cA = TRUE PathLengthConstraint = 0	
Key Usage	Yes	Certificate signature CRL signature	
Extended Key Usage	No	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	

Authority		CERTIGNA				
		SERVER AUTHENTICATION OVCP EU CA G1	SERVER AUTHENTICATION OVCP CA G1	SERVICES CA	WILD CA	CERTIGNA ROOT CA
Fields		**Description**				
Version		V3				
Serial Number		Unique serial number				
Signature		CA signing algorithm identifier / SHA-384 RSA 4096		SHA-256 RSA 4096		
Subject Public Key Info		RSA 4096				
Validity		< 3 years (2027-06-28)		18 ans		< 3 years (2027-06-28)
Issuer DN	CN =	Certigna				
	O =	Dhimyotis				
	C =	FR				
Subject DN	CN =	Certigna Server Authentication OVCP EU CA G1	Certigna Server Authentication OVCP CA G1	Certigna Services CA	Certigna Wild CA	Certigna Root CA
	OU =					0002 48146308100036
	OI =	NTRFR-48146308100036				
	O =	Certigna		Dhimyotis		
	C =	FR				
SKI	No	CA public key identifier				
AKI	No	Root CA Public key identifier				
Certificate Policies	No	OID=2.23.140.1.2.2 (OV) OID=1.2.250.1.177.1.0.1.2 CPS = http://cps.certigna.com/				OID=2.23.140.1.2.2 (OV)
Authority Informat. Access	No	caIssuers= http://cert.certigna.com/Certigna.cer				
CRL Distribution Points	No	URL=http://crl.certigna.com/Certigna.crl				
Basic Constraints	Yes	cA = TRUE	PathLengthConstraint = 0			cA = TRUE
Key Usage	Yes	Certificate signature	CRL signature			
Extended Key Usage	No	Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)			Server Authentication

Authority		CERTIGNA ROOT CA	
		SERVICES CA	WILD CA
Fields		**Description**	
Version		V3	
Serial Number		Unique serial number	
Signature		SHA-256 RSA 4096	
Subject Public Key Info		RSA 4096	
Validity		18 ans	
Issuer DN	CN = OU = O = C =	Certigna Root CA 0002 48146308100036 DHIMYOTIS FR	
Subject DN	CN =	Certigna Services CA	Certigna Wild CA
	OI =	NTRFR-48146308100036	
	O =	Dhimyotis	
	C =	FR	
SKI	No	CA public key identifier	
AKI	No	Root CA Public key identifier	
Certificate Policies	No	OID=1.2.250.1.177.2.0.1.1 CPS=https://www.certigna.fr/autorites/	
Authority Informat. Access	No	http://autorite.certigna.fr/certignarootca.der http://autorite.dhimyotis.com/certignarootca.der	
CRL Distribution Points	No	URL=http://crl.certigna.fr/certignarootca.crl URL=http://crl.dhimyotis.com/certignarootca.crl	
Basic Constraints	Yes	cA = TRUE	PathLengthConstraint = 0
Key Usage	Yes	Certificate signature	CRL signature
Extended Key Usage	No	Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)

Authorities		CERTIGNA		CERTIGNA ROOT CA	
		SERVEUR AUTHENTICATION ACME CA G1	SERVEUR AUTHENTICATION ACME FR CA G1	SERVEUR AUTHENTICATION ACME CA G2	SERVEUR AUTHENTICATION ACME FR CA G2
Fields		**Description**			
Version		V3			
Serial Number		Unique serial number			
Signature		CA signing algorithm identifier / SHA-384 RSA 4096			
Subject Public Key Info		RSA 4096			
Validity		15 years			
Issuer DN	CN = OU = O = C =	Certigna Dhimyotis FR		Certigna Root CA 0002 48146308100036 Dhimyotis FR	
Subject DN	CN =	Certigna Server Authentication ACME CA G1	Certigna Server Authentication ACME FR CA G1	Certigna Server Authentication ACME CA G2	Certigna Server Authentication ACME FR CA G2
	OI =	NTRFR-48146308100036			
	O =	CERTIGNA			
	C =	FR			
SKI	No	CA public key identifier			
AKI	No	Root CA Public key identifier			
Certificate Policies	No	OID= 2.23.140.1.2.1 (DV) OID= 2.23.140.1.2.2 (OV) OID= 2.23.140.1.1 (EV) OID= 1.2.250.1.177.1.0.1.2 id-qt-cps = http://cps.certigna.com		OID= 2.23.140.1.2.1 (DV) OID= 2.23.140.1.2.2 (OV) OID= 2.23.140.1.1 (EV) OID= 1.2.250.1.177.2.0.1.1 id-qt-cps = http://cps.certigna.com	
Authority Informat. Access	No	URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/Certigna.cer		URL=http://ocsp.certigna.com caIssuers= http://autorite.dhimyotis.com/certignarootca.der	
CRL Distribution Points	No	URL=http://crl.certigna.com/Certigna.crl		URL=http://crl.certigna.com/CertignaRootCA.crl	
Basic Constraints	Yes	cA = TRUE	PathLengthConstraint = 0		
Key Usage	Yes	Certificate signature	CRL signature		
Extended Key Usage	No	Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)		

7.1.12 Profile of server certificates

7.1.12.1 Profile of Certificates issued by Certigna Server Authentication OVCP CA & AUTO OVCP CA

7.1.12.1.1 Basic Fields

Authority		CERTIGNA SERVER AUTHENTICATION ROOT CA	
		CERTIGNA SERVER AUTHENTICATION OVCP CA	CERTIGNA SERVER AUTHENTICATION AUTO OVCP CA
Usage		Server authentication	
OID 1.2.250.1.177.6		.4.1.1.1	.5.1.1.1
ETSI 319 411		OVCP	OVCP
Champs		**Description**	
Version		V3	
Serial Number		Unique serial number output from a CSPRNG. Between 128 and 160 bits	
Signature		CA signing algorithm identifier / SHA-256 minimum	
Subject Public Key Info		RSA 2048 minimum before 2025-12-31 / RSA 3072 minimum from 2025-12-31	
Validity		398 days maximum	
Issuer DN	CN =	Certigna Server Authentication OVCP CA	Certigna Server Authentication Auto OVCP CA
	OI =	NTRFR-48146308100036	NTRFR-48146308100036
	O =	Certigna	Certigna
	C =	FR	FR
Subject DN	Serial Number	Series of characters consisting of a random value	
	Common Name	One FQDN of the « Subject Alternative Name » Extension	
	Organization Identifier		
	Organizat. Unit Name		
	Organization Name	Name of the entity linked to the server	
	Street Address		
	Locality Name	Locality Name (2.5.4.7)	
	Postal Code		
	State or Province Name		
	Country Name	Country of entity's domiciliation	
	Business Category		
	Jurisd. Locality Name		
	Jurisd. State/Prov. Name		
	Jurisd. Country Name		

7.1.12.1.2 Extensions

Authority		CERTIGNA SERVER AUTHENTICATION ROOT CA	
		CERTIGNA SERVER AUTHENTICATION OVCP CA	CERTIGNA SERVER AUTHENTICATION AUTO OVCP CA
Usage		Server authentication	
OID 1.2.250.1.177.6		.4.1.1.1	.5.1.1.1
ETSI 319 411		OVCP	OVCP
RGS v2			
Extension	**Crit.**	**Description**	
Authority Key Ident.	No	CA public key identifier	
Subject Key Ident.	No	Public key identifier of the server	
Subject Alt. Name	No	FQDN of domains to protect. « _ » character is not present in any dNSName entry	
Key Usage	**Yes**	Digital signature / Key Encipherment	
Extended Key Usage	No	id-kp-serverAuth / id-kp-clientAuth	
Certificate Policies	No	.4.1.1.1	.5.1.1.1
		2.23.140.1.2.2 (OVCP)	
		0.4.0.2042.1.7 (OVCP)	
		CPS= http://cps.certigna.com	
CRL Distribut. Points	No	URL=http://crl.certigna.com/CertignaServerAuthenticationOVCPCA.crl	http://crl.certigna.com/CertignaServerAuthenticationAutoOVCPCA.crl
Authority Info. Access	No	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationOVCPCA.cer	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationAutoOVCPCA.cer
Basic Constraints	**Yes**	cA = FALSE	
Cabf Organization. Identifier 2.23.140.3.1	No		
Certif. Transparency	No	List of SCTs. *Only for certificates containing one or more FQDNs.*	
QC Statement	No		

7.1.12.2 Profile of Certificates issued by Certigna Server Authentication QCP CA & AUTO QCP CA

7.1.12.2.1 Basic Fields

Authority		CERTIGNA SERVER AUTHENTICATION ROOT CA	
		CERTIGNA SERVER AUTHENTICATION QCP CA	CERTIGNA SERVER AUTHENTICATION AUTO QCP CA
Usage		Server authentication	
OID 1.2.250.1.177.6		.6.1.1.1	.7.1.1.1
ETSI 319 411		QNCP-w	QNCP-w
RGS v2			
Champs		**Description**	
Version		V3	
Serial Number		Unique serial number output from a CSPRNG. Between 128 and 160 bits	
Signature		CA signing algorithm identifier / SHA-256 minimum	
Subject Public Key Info		RSA 2048 minimum before 2025-12-31 / RSA 3072 minimum from 2025-12-31	
Validity		398 days maximum	
Issuer DN	CN = OI = O = C =	Certigna Server Authentication QCP CA NTRFR-48146308100036 Certigna FR	Certigna Server Authentication Auto QCP CA NTRFR-48146308100036 Certigna FR
Subject DN	Serial Number	Series of characters consisting of a random value	
	Common Name	One FQDN of the « Subject Alternative Name » Extension	
	Organization Identifier	Registration number of the entity linked to the certificate	
	Organizat. Unit Name		
	Organization Name	Name of the entity linked to the server	
	Street Address		
	Locality Name	Locality Name (2.5.4.7)	
	Postal Code		
	State or Province Name		
	Country Name	Country of entity's domiciliation	
	Business Category		
	Jurisd. Locality Name		
	Jurisd. State/Prov. Name		
	Jurisd. Country Name		

7.1.12.2.2 Extensions

Authority		CERTIGNA SERVER AUTHENTICATION ROOT CA	
		CERTIGNA SERVER AUTHENTICATION QCP CA	CERTIGNA SERVER AUTHENTICATION AUTO QCP CA
Usage		Server authentication	
OID 1.2.250.1.177.6		.6.1.1.1	.7.1.1.1
ETSI 319 411		QNCP-w	QNCP-w
RGS v2			
Extension	**Crit.**	**Description**	
Authority Key Ident.	No	CA public key identifier	
Subject Key Ident.	No	Public key identifier of the server	
Subject Alt. Name	No	FQDN of domains to protect. « _ » character is not present in any dNSName entry	
Key Usage	**Yes**	Digital signature / Key Encipherment	
Extended Key Usage	No	id-kp-serverAuth / id-kp-clientAuth	
Certificate Policies	No	.6.1.1.1	.7.1.1.1
		2.23.140.1.2.2 (OVCP)	
		0.4.0.194112.1.5 (QNCP-w)	
		CPS= http://cps.certigna.com	
CRL Distribut. Points	No	URL=http://crl.certigna.com/CertignaServerAuthenticationQCPCA.crl	http://crl.certigna.com/CertignaServerAuthenticationAutoQCPCA.crl
Authority Info. Access	No	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationQCPCA.cer	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationAutoQCPCA.cer
Basic Constraints	**Yes**	cA = FALSE	
Cabf Organization. Identifier 2.23.140.3.1	No		
Certif. Transparency	No	List of SCTs. *Only for certificates containing one or more FQDNs.*	
QC Statement	No	QcCompliance	
		QcEuPDS	
		QcType 3 (web)	

7.1.12.3 Profile of Certificates issued by Certigna Server Authentication CA

7.1.12.3.1 Basic Fields

CERTIGNA SERVER AUTHENTICATION CA							
Usage		Server authentication					
OID 1.2.250.1.177.6		.1.1.1.1	.1.1.1.2	.1.1.1.3	.1.1.2.1	.1.1.2.2	.1.1.2.3
ETSI 319 411		OVCP	OVCP	OVCP	QNCP-w	QNCP-w	QNCP-w
RGS v2		RGS *	RGS *	RGS *			
Fields		Description					
Version		V3					
Serial Number		Unique serial number output from a CSPRNG. Between 128 and 160 bits					
Signature		CA signing algorithm identifier / SHA-256 minimum					
Subject Public Key Info		RSA 2048	RSA 3072	RSA 4096	RSA 2048	RSA 3072	RSA 4096
Validity		398 days maximum					
Issuer DN	CN =	Certigna Server Authentication CA					
	OI =	NTRFR-48146308100036					
	O =	Certigna					
	C =	FR					
Subject DN	Serial Number	Series of characters consisting of a random value					
	Common Name	One FQDN of the « Subject Alternative Name » Extension					
	Organization Identifier				Registration number of the entity linked to the certificate		
	Organizat. Unit Name						
	Organization Name	Name of the entity linked to the server					
	Street Address						
	Locality Name	Locality Name (2.5.4.7)					
	Postal Code						
	State or Province Name						
	Country Name	Country of entity's domiciliation					
	Business Category						
	Jurisd. Locality Name						
	Jurisd. State/Prov. Name						
	Jurisd. Country Name						

7.1.12.3.2 Extensions

CERTIGNA SERVER AUTHENTICATION CA							
Usage		Server authentication					
OID 1.2.250.1.177.6		.1.1.1.1	.1.1.1.2	.1.1.1.3	.1.1.2.1	.1.1.2.2	.1.1.2.3
ETSI 319 411		OVCP	OVCP	OVCP	QNCP-w	QNCP-w	QNCP-w
RGS v2		RGS *	RGS *	RGS *			
Extension	**Crit.**	**Description**					
Authority Key Ident.	No	CA public key identifier					
Subject Key Ident.	No	Public key identifier of the server					
Subject Alt. Name	No	FQDN of domains to protect. « _ » character is not present in any dNSName entry					
Key Usage	**Yes**	Digital sign. / Key Enciph.					
Extended Key Usage	No	id-kp-serverAuth / id-kp-clientAuth			id-kp-serverAuth / id-kp-clientAuth		
Certificate Policies	No	.1.1.1.1	.1.1.1.2	.1.1.1.3	.1.1.2.1	.1.1.2.2	.1.1.2.3
	No	2.23.140.1.2.2 (OVCP)					
	No	0.4.0.2042.1.7 (OVCP)			0.4.0.194112.1.5 (QNCP-w)		
	No	CPS= http://cps.certigna.com					
CRL Distribut. Points	No	URL=http://crl.certigna.com/CertignaServerAuthenticationCA.crl					
Authority Info. Access	No	URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/CertignaServerAuthenticationCA.cer					
Basic Constraints	**Yes**	cA = FALSE					
Cabf Organization. Identifier 2.23.140.3.1	No				Info. Entité [2]		
Certif. Transparency	No	List of SCTs. *Only for certificates containing one or more FQDNs.*					
QC Statement	No				QcCompliance		
					QcEuPDS		
					QcType 3 (web)		

7.1.12.4 Profile of Certificates issued by Certigna Server Authentication Auto CA & Auto FR CA

7.1.12.4.1 Basic Fields

CERTIGNA SERVER AUTHENTICATION		AUTO CA				AUTO FR CA	
Usage		Server authentication					
OID 1.2.250.1.177.6		.2.1.2.1	.2.1.2.2	.2.1.3.1	.2.1.3.2	.3.1.1.1	.3.1.1.2
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	OVCP	OVCP
RGS v2						RGS *	RGS *
Fields		Description					
Version		V3					
Serial Number		Unique serial number output from a CSPRNG. Between 128 and 160 bits					
Signature		CA signing algorithm identifier / SHA-256 minimum					
Subject Public Key Info		RSA 3072	RSA 4096	RSA 3072	RSA 4096	RSA 3072	RSA 4096
Validity		398 days maximum					
Issuer DN	CN =	Certigna Server Authentication Auto CA				Certigna Server Authentication Auto FR CA	
	OI =	NTRFR-48146308100036				NTRFR-48146308100036	
	O =	Certigna				Certigna	
	C =	FR				FR	
Subject DN	Serial Number	Series of characters consisting of a random value					
	Common Name	One FQDN of the « Subject Alternative Name » Extension					
	Organization Identifier						
	Organizat. Unit Name						
	Organization Name	Name of the entity linked to the server					
	Street Address						
	Locality Name	Locality Name (2.5.4.7)					
	Postal Code						
	State or Province Name						
	Country Name	Country of entity's domiciliation					
	Business Category						
	Jurisd. Locality Name						
	Jurisd. State/Prov. Name						
	Jurisd. Country Name						

7.1.12.4.2 Extensions

CERTIGNA SERVER AUTHENTICATION		AUTO CA				AUTO FR CA	
Usage		Server authentication					
OID 1.2.250.1.177.6		.2.1.2.1	.2.1.2.2	.2.1.3.1	.2.1.3.2	.3.1.1.1	.3.1.1.2
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	OVCP	OVCP
RGS v2						RGS *	RGS *
Extension	**Crit.**	**Description**					
Authority Key Ident.	No	CA public key identifier					
Subject Key Ident.	No	Public key identifier of the server					
Subject Alt. Name	No	FQDN of domains to protect. « _ » character is not present in any dNSName entry					
Key Usage	**Yes**	Digital sign. / Key Enciph.					
Extended Key Usage	No	id-kp-serverAuth / id-kp-clientAuth				id-kp-serverAuth	
Certificate Policies	No No No	.2.1.2.1	.2.1.2.2	.2.1.3.1	.2.1.3.2	.3.1.1.1	.3.1.1.2
		2.23.140.1.2.2 (OVCP)					
		0.4.0.2042.1.7 (OVCP)					
		CPS= http://cps.certigna.com					
CRL Distribut. Points	No	URL=http://crl.certigna.com/CertignaServerAuthenticationAutoCA.crl				URL=http://crl.certigna.com/CertignaServerAuthenticationAutoFRCA.crl	
Authority Info. Access	No	URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/CertignaServerAuthenticationAutoCA.cer				URL=http://ocsp.certigna.com http://cert.certigna.com/CertignaServerAuthenticationAutoFRCA.cer	
Basic Constraints	**Yes**	cA = FALSE					
Cabf Organization. Identifier 2.23.140.3.1	No						
Certif. Transparency	No	List of SCTs. *Only for certificates containing one or more FQDNs.*					
QC Statement	No						

7.1.12.5 Profile of Certificates issued by Certigna Server Authentication OVCP EU CA & AUTO OVCP EU CA

7.1.12.5.1 Basic Fields

Authority		CERTIGNA SERVER AUTHENTICATION EU ROOT CA	
		CERTIGNA SERVER AUTHENTICATION OVCP EU CA	CERTIGNA SERVER AUTHENTICATION AUTO OVCP EU CA
Usage		Server authentication	
OID		1.2.250.1.177.14.1.1.1.1	1.2.250.1.177.14.2.1.1.1
ETSI 319 411		OVCP	OVCP
RGS v2		*	*
Champs		**Description**	
Version		V3	
Serial Number		Unique serial number output from a CSPRNG. Between 128 and 160 bits	
Signature		CA signing algorithm identifier / SHA-256 minimum	
Subject Public Key Info		RSA 2048 minimum before 2025-12-31 / RSA 3072 minimum from 2025-12-31	
Validity		398 days maximum	
Issuer DN	CN =	Certigna Server Authentication OVCP EU CA	Certigna Server Authentication Auto OVCP EU CA
	OI =	NTRFR-48146308100036	NTRFR-48146308100036
	O =	Certigna	Certigna
	C =	FR	FR
Subject DN	Serial Number	Series of characters consisting of a random value	
	Common Name	One FQDN of the « Subject Alternative Name » Extension	
	Organization Identifier		
	Organizat. Unit Name		
	Organization Name	Name of the entity linked to the server	
	Street Address		
	Locality Name	Locality Name (2.5.4.7)	
	Postal Code		
	State or Province Name		
	Country Name	Country of entity's domiciliation	
	Business Category		
	Jurisd. Locality Name		
	Jurisd. State/Prov. Name		
	Jurisd. Country Name		

7.1.12.5.2 Extensions

Authority		CERTIGNA SERVER AUTHENTICATION EU ROOT CA	
		CERTIGNA SERVER AUTHENTICATION OVCP EU CA	CERTIGNA SERVER AUTHENTICATION AUTO OVCP EU CA
Usage		Server authentication	
OID		1.2.250.1.177.14.1.1.1.1	1.2.250.1.177.14.2.1.1.1
ETSI 319 411		OVCP	OVCP
RGS v2		*	*
Extension	**Crit.**	**Description**	
Authority Key Ident.	No	CA public key identifier	
Subject Key Ident.	No	Public key identifier of the server	
Subject Alt. Name	No	FQDN of domains to protect. « _ » character is not present in any dNSName entry	
Key Usage	**Yes**	Digital sign. / Key Enciph.	
Extended Key Usage	No	id-kp-serverAuth	
Certificate Policies	No	1.2.250.1.177.14.1.1.1.1	1.2.250.1.177.14.2.1.1.1
		2.23.140.1.2.2 (OVCP)	
		0.4.0.2042.1.7 (OVCP)	
		CPS= http://cps.certigna.com	
CRL Distribut. Points	No	URL=http://crl.certigna.com/CertignaServerAuthentication OVCPEUCA.crl	http://crl.certigna.com/CertignaServerAuthenticationAuto OVCPEUCA.crl
Authority Info. Access	No	caIssuers= http://cert.certigna.com/CertignaServerAuthentication OVCPEUCA.cer	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationAuto OVCPEUCA.cer
Basic Constraints	**Yes**	cA = FALSE	
Cabf Organization. Identifier 2.23.140.3.1	No		
Certif. Transparency	No	List of SCTs. *Only for certificates containing one or more FQDNs.*	
QC Statement	No		

7.1.12.6 Profile of Certificates issued by Certigna Services CA

7.1.12.6.1 Basic Fields

CERTIGNA SERVICES CA										
Usage		Server authentication		Client authentication		Server authentication				
OID 1.2.250.1.177.2		.5.1.1.1	.5.1.1.2	.5.1.2.1	.5.1.2.2	.5.1.3.1	.5.1.4.1	.5.1.4.2	.5.1.5.1	5.1.5.2
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	QEVCP-w	QEVCP-w		QNCP-w	QNCP-w
RGS v2		RGS *	RGS *	RGS *	RGS *					
Fields		**Description**								
Version		V3								
Serial Number		Unique serial number output from a CSPRNG. Between 128 and 160 bits								
Signature		CA signing algorithm identifier / SHA-256 minimum								
Subject Public Key Info		RSA 2048	RSA >=3072	RSA 2048	RSA >=3072	RSA 2048	2048	3072	RSA 2048	RSA >=3072
Validity		398 days maximum								
Issuer DN	CN =	Certigna Services CA								
	OU =	0002 48146308100036								
	OI =	NTRFR-48146308100036								
	O =	Dhimyotis								
	C =	FR								
Subject DN	Serial Number	Series of characters consisting of a random value								
	Common Name	One FQDN of the « Subject Alternative Name » Extension								
	Organization Identifier					Registration number of the entity linked to the certificate				
	Organizat. Unit Name			ICD + identifier of entity						
	Organization Name	Name of the entity linked to the server								
	Street Address					N° and street (2.5.4.9)				
	Locality Name	Locality Name (2.5.4.7)								
	Postal Code					Postal code (2.5.4.17)				
	State or Province Name					State/province (2.5.4.8)				
	Country Name	Country of entity's domiciliation								
	Business Category					Business category (2.5.4.15)				
	Jurisd. Locality Name					City or town juridiction				
	Jurisd. State/Prov. Name					State or province juridiction				
	Jurisd. Country Name					Country juridiction				

7.1.12.6.2 Extensions

CERTIGNA SERVICES CA										
Usage		Server authentication		Client authentication		Server authentication				
OID 1.2.250.1.177.2		.5.1.1.1	.5.1.1.2	.5.1.2.1	.5.1.2.2	.5.1.3.1	.5.1.4.1	.5.1.4.2	.5.1.5.1	5.1.5.2
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	QEVCP-w	QEVCP-w		QNCP-w	QNCP-w
RGS v2		RGS *	RGS *	RGS *	RGS *					
Extension	**Crit.**	**Description**								
Authority Key Ident.	No	CA public key identifier								
Subject Key Ident.	No	Public key identifier of the server								
Subject Alt. Name	No	FQDN of domains to protect. « _ » character is not present in any dNSName entry								
Key Usage	**Yes**	Digital sign. / Key Enciph.		Digital signature		Digital signature / Key Encipherment				
Extended Key Usage	No	id-kp-serverAuth		id-kp-clientAuth		id-kp-serverAuth / id-kp-clientAuth				
Certificate Policies	No No No	.5.1.1.1	.5.1.1.2	.5.1.2.1	.5.1.2.2	.5.1.3.1	.5.1.4.1	.5.1.4.2	.5.1.5.1	5.1.5.2
		2.23.140.1.2.2 (OVCP)				2.23.140.1.1 (EVCP)			2.23.140.1.2.2	
				0.4.0.2042.1.7 (OVCP)		0.4.0.194112.1.4 (QEVCP-w)	0.4.0.19495.3.1 (QCP-w-psd2)		0.4.0.194112.1.5 (QNCP-w)	
		CPS= https://www.certigna.fr/autorites/								
CRL Distribut. Points	No	URL=http://crl.certigna.fr/servicesca.crl URL=http://crl.dhimyotis.com/servicesca.crl								
Authority Info. Access	No	If issued by the root « Certigna » (before 2026-01-14) 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				If issued by the root « Certigna Root Ca » (From 2026-01-14) caIssuers=https://autorite.certigna.fr/servicesca_rootca.der caIssuers=http://autorite.dhimyotis.com/servicesca_rootca.der URL=http://servicesca.ocsp.certigna.fr URL=http://servicesca.ocsp.dhimyotis.com				
Basic Constraints	**Yes**	cA = FALSE								
Cabf Org. Id. 2.23.140.3.1	No					Info. Entité [2]	Info. Entité [2]		Info. Entité [2]	Info. Entité [2]
Certif. Transparency	No	List of SCTs. *Only for certificates containing one or more FQDNs.*								
QC Statement	No					QcCompliance				
						QcEuPDS				
						QcType 3 (web)				
							PSD2QcType [3]			

[1] The OrganizationIdentifier (OI) field is used to provide the registration number of the entity attached to the certificate. In the case where this number is issued by the NCA, this field will be composed as follows:

- "PSD" as 3 character legal person identity type reference;
- 2 character country code representing the NCA country;
- hyphen-minus "-" :
- 2-8 character NCA identifier without country code;
- hyphen-minus "-" ; and
- PSP identifier (authorization number as specified by the NCA. There are no restrictions on the characters used).

Example: the "OI" field containing this character series "PSDFR-APCR-123456789" means a certificate issued to a PSP whose registration number is 123456789 and whose authorization is provided by a French NCA which is the Prudential Supervisory and resolution Authority whose identifier is "FR-APCR". Other examples can include use of non-alphanumeric characters such as "PSDBE-NBB-1234.567.890" and "PSDFI-FINFSA-1234567-8" and "PSDMT-MFSA-A 12345" (note space character after "A").

Note: PSP Identifier can contain prefix, followed by colon ":", including type of institution, as listed in PSD2 where needed to ensure uniqueness (i.e. where there are numbering schemes for different types of institutions with the possibility of the same number being allocated to different institutions). This prefix would then consist of one of the following strings, followed by the ":" character:

- Credit institution - CI
- Payment institution - PI
- Electronic money institution (or e-money institution) - EMI
- Account information service provider exempted under Article 33 of PSD2 – RAISP

[2] Information about entity under the following form:

registrationSchemeIdentifier = NTR / VAT / PSD
registrationCountry = Country of entity's domiciliation
registrationStateOrProvince = State or province of the entity jurisdiction (if applicable)
registrationReference = A unique identifier assigned to a Legal Entity

[3] PSD2QcType content:

- **rolesOfPSP** {
    - **roleOfPspOid** = One or more of the following values:
        - 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** = One or more of the following values:
        - 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** = Name of the NCA in English

- **nCAId** = NCA identifier

Note: The attributes of the subject present in the DN of the final certificates do not contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable. Attributes within the subject other than those listed in CA/Browser Forum "Baseline Requirements" contain information that has been verified by the CA.

7.1.12.6.3 Pre-certificates

As part of the implementation of the requirements of the RFC 6962 about « Certificate Transparency », the CA issues pre-certificates. These pre-certificates are not considered to be a "certificate" subjected to the requirements of RFC 5280 and to this CP and are used only for obtaining SCTs to be included in the extension of certificates issued and containing FQDN. We invite you to consult RFC 6962 for more information on this plan. The SCTs are collected dynamically from the authorized logs.

7.1.12.7 Profile of Certificates issued by Certigna Wild CA

7.1.12.7.1 Basic Fields

CERTIGNA WILD CA					
Usage		**multi-domains Server authentication**		**Wildcard multi-domains Server authentication**	
OID 1.2.250.1.177.2		.7.1.1.1	.7.1.1.2	.7.1.2.1	.7.1.2.2
ETSI 319 411		OVCP	OVCP	OVCP	OVCP
RGS v2					
Fields		**Description**			
Version		V3			
Serial Number		Unique serial number output from a CSPRNG. Between 128 and 160 bits			
Signature		CA signing algorithm identifier / SHA-256 minimum			
Subject Public Key Info		RSA 2048	RSA >=3072	RSA 2048	RSA >=3072
Validity		398 days maximum			
Issuer DN	CN =	Certigna Wild CA			
	OU =	0002 48146308100036			
	OI =	NTRFR-48146308100036			
	O =	DHIMYOTIS			
	C =	FR			
Subject DN	CN =	One FQDN of the SAN Extension			
	OU =	ICD + identifier of the entity linked to the server (Field prohibited and absent since 09/01/2022)			
	O =	Name of the entity linked to the seal service			
	L =	City or town of entity's domiciliation (2.5.4.7)			
	C =	Country of entity's domiciliation			

The attributes of the subject present in the DN of the final certificates do not contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable. Attributes within the subject other than those listed in CA/Browser Forum "Baseline Requirements" contain information that has been verified by the CA.

7.1.12.7.2 Extensions

CERTIGNA WILD CA					
Usage		**multi-domains Server authentication**		**Wildcard multi-domains Server authentication**	
OID 1.2.250.1.177.2		.7.1.1.1	.7.1.1.2	.7.1.2.1	.7.1.2.2
ETSI 319 411		OVCP	OVCP	OVCP	OVCP
RGS v2					
Fields	**Critical**	**Description**			
Authority Key Identifier	No	CA public key identifier			
Subject Key Identifier	No	Public key identifier of the server			
Subject Alt. Name	No	FQDN of domains to protect. « _ » character is not present in any dNSName entry			
Key Usage	**Yes**	Digital signature / Key Encipherment			
Extended Key Usage	No	id-kp-serverAuth / id-kp-clientAuth			
Certificate Policies	No	OID=1.2.250.1.177.2.7.1.1.1 OID=2.23.140.1.2.2 (OVCP)	OID=1.2.250.1.177.2.7.1.1.2 OID=2.23.140.1.2.2 (OVCP)	OID=1.2.250.1.177.2.7.1.2.1 OID=2.23.140.1.2.2 (OVCP)	OID=1.2.250.1.177.2.7.1.2.2 OID=2.23.140.1.2.2 (OVCP)
		CPS= https://www.certigna.fr/autorites/			
CRL Distribut. Points	No	URL=http://crl.certigna.fr/wildca.crl URL=http://crl.dhimyotis.com/wildca.crl			
Authority Info. Access	No	If issued by the root « Certigna » (before 2026-01-14) caIssuers=http://autorite.certigna.fr/wildca.der caIssuers=http://autorite.dhimyotis.com/wildca.der URL=http://wildca.ocsp.certigna.fr URL=http://wildca.ocsp.dhimyotis.com		If issued by the root « Certigna Root Ca » (From 2026-01-14) caIssuers=http://autorite.certigna.fr/wildca_rootca.der caIssuers=http://autorite.dhimyotis.com/wildca_rootca.der URL=http://wildca.ocsp.certigna.fr URL=http://wildca.ocsp.dhimyotis.com	
Basic Constraints	**Yes**	cA = FALSE			
Certificate Transparency	No	List of SCTs. *Only for certificates containing one or more FQDNs.*			

7.1.12.7.3 Pre-certificates

As part of the implementation of the requirements of the RFC 6962 about « Certificate Transparency », the CA issues pre-certificates. These pre-certificates are not considered to be a “certificate” subjected to the requirements of RFC 5280 and to this CP and are used only for obtaining SCTs to be included in the extension of certificates issued and containing FQDN. We invite you to consult RFC 6962 for more information on this plan. The SCTs are collected dynamically from the authorized logs.

7.1.12.8 Profile of Certificates issued by Certigna Server Authentication EU OVCP CA G1 & OVCP CA G1

7.1.12.8.1 Basic fields

Authority		CERTIGNA	
		CERTIGNA SERVER AUTHENTICATION OVCP EU CA G1	CERTIGNA SERVER AUTHENTICATION OVCP CA G1
Usage		Server authentication	Server authentication
OID		1.2.250.1.177.1.23.1.1.1	1.2.250.1.177.1.22.1.1.1
ETSI 319 411		OVCP	OVCP
RGS v2		RGS *	
Fields		**Description**	
Version		V3	
Serial Number		Unique serial number output from a CSPRNG. Between 128 and 160 bits	
Signature		CA signing algorithm identifier / SHA-256 minimum	
Subject Public Key Info		RSA 2048 minimum before 2025-12-31 / RSA 3072 minimum from 2025-12-31	
Validity		398 days maximum	
Issuer DN	CN = OI = O = C =	Certigna Server Authentication OVCP EU CA G1 NTRFR-48146308100036 Certigna FR	Certigna Server Authentication OVCP CA G1 NTRFR-48146308100036 Certigna FR
Subject DN	Serial Number	Series of characters consisting of a random value	
	Common Name	One FQDN of the SAN Extension	
	Organization Name	Name of the entity linked to the seal service	
	Locality Name	City or town of entity's domiciliation (2.5.4.7)	
	Country Name	Country of entity's domiciliation	

7.1.12.8.2 Extensions

Autorité		CERTIGNA	
		CERTIGNA SERVER AUTHENTICATION OVCP EU CA G1	CERTIGNA SERVER AUTHENTICATION OVCP CA G1
Usage		Server authentication	Server authentication
OID		1.2.250.1.177.1.23.1.1.1	1.2.250.1.177.1.22.1.1.1
ETSI 319 411		OVCP	OVCP
RGS v2		RGS *	
Extension	**Crit.**	**Content**	
Authority Key Ident.	No	CA public key identifier	
Subject Key Ident.	No	Public key identifier of the server	
Subject Alt. Name	No	FQDN of domains to protect. « _ » character is not present in any dNSName entry	
Key Usage	**Yes**	Digital signature / Key Encipherment	
Extended Key Usage	No	id-kp-serverAuth	id-kp-serverAuth / id-kp-clientAuth
Certificate Policies	No	1.2.250.1.177.1.23.1.1.1	1.2.250.1.177.1.22.1.1.1
		2.23.140.1.2.2 (OVCP CAB FORUM) 0.4.0.2042.1.7 (OVCP ETSI)	
		CPS= http://cps.certigna.com	
CRL Distribut. Points	No	http://crl.certigna.com/CertignaServerAuthenticationOVCPEUCAG1.crl	http://crl.certigna.com/CertignaServerAuthenticationOVCPCAG1.crl
Authority Info. Access	No	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationOVCPEUCAG1.cer	caIssuers= http://cert.certigna.com/CertignaServerAuthenticationOVCPCAG1.cer
Basic Constraints	**Yes**	cA = FALSE	
Certif. Transparency	No	List of SCTs. *Only for certificates containing one or more FQDNs.*	

7.1.12.9 Profile of Certificates issued by Certigna Server Authentication ACME CA G1 & ACME CA FR G1

7.1.12.9.1 Basic fields

Authority		CERTIGNA						
		CERTIGNA SERVER AUTHENTICATION ACME CA G1				CERTIGNA SERVER AUTHENTICATION ACME FR CA G1		
Usage		Server authentication				Server authentication		
OID 1.2.250.1.177.1		.20.1.1.1	.20.1.1.2	.20.1.1.3	.20.1.2.1	.21.1.1.1	.21.1.1.2	.21.1.1.3
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	OVCP	OVCP	OVCP
RGS v2						RGS *	RGS *	RGS *
Fields		**Description**						
Version		V3						
Serial Number		Unique serial number output from a CSPRNG. Between 128 and 160 bits						
Signature		CA signing algorithm identifier / SHA-256 minimum						
Subject Public Key Info		RSA 2048	RSA 3072	RSA 4096	>= RSA 2048	RSA 2048	RSA 3072	RSA 4096
Validity		398 jours maximum						
Issuer DN	CN = OI = O = C =	Certigna Server Authentication ACME CA G1 NTRFR-48146308100036 Certigna FR				Certigna Server Authentication ACME FR CA G1 NTRFR-48146308100036 Certigna FR		
Subject DN	Serial Number	Series of characters consisting of a random value						
	Common Name	One FQDN of the SAN Extension						
	Organization Name	Name of the entity linked to the seal service						
	Locality Name	City or town of entity's domiciliation (2.5.4.7)						
	Country Name	Country of entity's domiciliation						

7.1.12.9.2 Extensions

Autorité		CERTIGNA						
		CERTIGNA SERVER AUTHENTICATION ACME CA G1				CERTIGNA SERVER AUTHENTICATION ACME FR CA G1		
Usage		Server authentication				Server authentication		
OID 1.2.250.1.177.1		.20.1.1.1	.20.1.1.2	.20.1.1.3	.1.20.1.2.1	.21.1.1.1	.21.1.1.2	.21.1.1.3
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	OVCP	OVCP	OVCP
RGS v2						RGS *	RGS *	RGS *
Extension	**Crit.**	**Contenu**						
Authority Key Ident.	No	CA public key identifier						
Subject Key Ident.	No	Public key identifier of the server						
Subject Alt. Name	No	FQDN of domains to protect. « _ » character is not present in any dNSName entry						
Key Usage	**Yes**	Digital signature / Key Encipherment						
Extended Key Usage	No	id-kp-serverAuth / id-kp-clientAuth				id-kp-serverAuth		
Certificate Policies	No	.1.20.1.1.1	.1.20.1.1.2	.1.20.1.1.3	.1.20.1.2.1	.1.21.1.1.1	.1.21.1.1.2	.1.21.1.1.3
		2.23.140.1.2.2 (OVCP CAB FORUM) 0.4.0.2042.1.7 (OVCP ETSI)						
		CPS= http://cps.certigna.com						
CRL Distribut. Points	No	http://crl.certigna.com/CertignaServerAuthenticationACMECAG1.crl				http://crl.certigna.com/CertignaServerAuthentication ACMEFRCAG1.crl		
Authority Info. Access	No	URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/CertignaServerAuthenticationACMECAG1.cer				URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/CertignaServerAuthentication ACMEFRCAG1.cer		
Basic Constraints	**Yes**	cA = FALSE						
Certif. Transparency	No	List of SCTs. *Only for certificates containing one or more FQDNs.*						

7.1.12.10 Profile of Certificates issued by Certigna Server Authentication ACME CA G2 & ACME CA FR G2

7.1.12.10.1 Basic fields

Authority		CERTIGNA ROOT CA							
		CERTIGNA SERVER AUTHENTICATION ACME CA G2					CERTIGNA SERVER AUTHENTICATION ACME FR CA G2		
Usage		Server authentication			Server authent. Wildcard		Server authentication		
OID 1.2.250.1.177.2		.10.1.1.1	.10.1.1.2	.10.1.1.3	.10.1.2.1	.10.1.2.2	.11.1.1.1	.11.1.1.2	.11.1.1.3
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	OVCP	OVCP	OVCP	OVCP
RGS v2							RGS *	RGS *	RGS *
Fields		**Description**							
Version		V3							
Serial Number		Unique serial number output from a CSPRNG. Between 128 and 160 bits							
Signature		CA signing algorithm identifier / SHA-256 minimum							
Subject Public Key Info		RSA 2048	RSA 3072	RSA 4096	RSA 3072	RSA 4096	RSA 2048	RSA 3072	RSA 4096
Validity		398 days maximum							
Issuer DN	CN = OI = O = C =	Certigna Server Authentication ACME CA NTRFR-48146308100036 Certigna FR					Certigna Server Authentication ACME FR CA NTRFR-48146308100036 Certigna FR		
Subject DN	Serial Number	Series of characters consisting of a random value							
	Common Name	One FQDN of the SAN Extension							
	Organization Name	Name of the entity linked to the seal service							
	Locality Name	City or town of entity's domiciliation (2.5.4.7)							
	Country Name	Country of entity's domiciliation							

7.1.12.10.2 Extensions

Authority		CERTIGNA ROOT CA							
		CERTIGNA SERVER AUTHENTICATION ACME CA G2					CERTIGNA SERVER AUTHENTICATION ACME FR CA G2		
Usage		Server authentication			Server authentication Wildcard		Server authentication		
OID 1.2.250.1.177.2		.10.1.1.1	.10.1.1.2	.10.1.1.3	.10.1.2.1	.10.1.2.2	.11.1.1.1	.11.1.1.2	.11.1.1.3
ETSI 319 411		OVCP	OVCP	OVCP	OVCP	OVCP	OVCP	OVCP	OVCP
RGS v2							RGS *	RGS *	RGS *
Extension	**Crit.**	**Description**							
Authority Key Ident.	No	CA public key identifier							
Subject Key Ident.	No	Public key identifier of the server							
Subject Alt. Name	No	FQDN of domains to protect. « _ » character is not present in any dNSName entry							
Key Usage	**Yes**	Digital signature / Key Encipherment							
Extended Key Usage	No	id-kp-serverAuth / id-kp-clientAuth					id-kp-serverAuth		
Certificate Policies	No	.10.1.1.1	.10.1.1.2	.10.1.1.3	.10.1.2.1	.10.1.2.2	.11.1.1.1	.11.1.1.2	.11.1.1.3
		2.23.140.1.2.2 (OVCP CAB FORUM) 0.4.0.2042.1.7 (OVCP ETSI)							
		CPS= http://cps.certigna.com							
CRL Distribut. Points	No	http://crl.certigna.com/CertignaServerAuthenticationACMECAG2.crl					http://crl.certigna.com/CertignaServerAuthenticationACMEFRCAG2.crl		
Authority Info. Access	No	URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/CertignaServerAuthenticationACMECAG2.cer					URL=http://ocsp.certigna.com caIssuers= http://cert.certigna.com/CertignaServerAuthenticationACMEFRCAG2.cer		
Basic Constraints	**Yes**	cA = FALSE							
Certif. Transparency	No	List of SCTs. *Only for certificates containing one or more FQDNs.*							

7.2 Profile of CRL

7.2.1 Version number(s)

Certificate Revocation Lists are of type X.509 v2.

7.2.2 CRL and CRL entry extensions

		CERTIGNA SERVER AUTHENTICATION ROOT CA						
		CA	AUTO CA	AUTO FR CA	OVCP CA	AUTO OVCP CA	QCP CA	AUTO QCP CA
Fields		**Description**						
Version		V2						
Signature		CA signing algorithm identifier SHA-256 RSA 4096						
Issuer DN	CN =	Certigna Server Authentication CA	Certigna Server Authentication Auto CA	Certigna Server Authentication Auto FR CA	Certigna Server Authentication OVCP CA	Certigna Server Authentication Auto OVCP CA	Certigna Server Authentication QCP CA	Certigna Server Authentication Auto QCP CA
	OI =	NTRFR-48146308100036						
	O =	Certigna						
	C =	FR						
This Update		CRL generation date						
Next Update		Next date of CRL update [7 days maximum]						
Revoked certificates		List of revoked certificate serial number						
		ReasonCode [1]						
Extensions	**Crit.**	**Description**						
AKI	No	CA public key identifier						
CRL Nb	No	CRL serial number						
Expired CertsOnCRL	No	Date from which revoked and expired certificates are maintained in the CRL.						

[1] An extension specifying the reason for revocation may be present in accordance with the commitments of chapters 4.9.1 and 4.9.3.2.

		CERTIGNA & CERTIGNA ROOT CA		CERTIGNA		CERTIGNA SERVER AUTH. EU ROOT CA	
		SERVICES CA	WILD CA	SERVER AUTHENTICATION OVCP EU CA G1	SERVER AUTHENTICATION OVCP CA G1	SERVER AUTHENTICATION OVCP EU CA	SERVER AUTHENTICATION Auto OVCP EU CA
Fields		**Description**					
Version		V2					
Signature		CA signing algorithm identifier SHA-256 RSA 4096					
Issuer DN	CN =	Certigna Services CA	Certigna Wild CA	Certigna Server Authentication OVCP EU CA G1	Certigna Server Authentication OVCP CA G1	Certigna Server Authentication OVCP EU CA	Certigna Server Authentication Auto OVCP EU CA
	OU =	0002 48146308100036					
	OI =	NTRFR-48146308100036					
	O =	Dhimyotis		Certigna			
	C =	FR					
This Update		CRL generation date					
Next Update		Next date of CRL update [7 days maximum]					
Revoked certificates		List of revoked certificate serial number					
		ReasonCode [1]					
Extensions	**Crit.**	**Description**					
AKI	No	CA public key identifier					
CRL Nb	No	CRL serial number					
Expired CertsOnCRL	No	Date from which revoked and expired certificates are maintained in the CRL.					

[1] An extension specifying the reason for revocation may be present in accordance with the commitments of chapters 4.9.1 and 4.9.3.2.

		CERTIGNA		CERTIGNA ROOT CA	
		SERVER AUTHENTICATION ACME CA G1	SERVER AUTHENTICATION ACME FR CA G1	SERVER AUTHENTICATION ACME CA G2	SERVER AUTHENTICATION ACME FR CA G2
Fields		**Description**			
Version		V2			
Signature		CA signing algorithm identifier SHA-256 RSA 4096			
Issuer DN	CN =	Certigna Server Authentication ACME CA G1	Certigna Server Authentication ACME FR CA G1	Certigna Server Authentication ACME CA G2	Certigna Server Authentication ACME FR CA G2
	OU =				
	OI =	NTRFR-48146308100036			
	O =	Certigna			
	C =	FR			
This Update		CRL generation date			
Next Update		Next date of CRL update [7 days maximum]			
Revoked certificates		List of revoked certificate serial number			
		ReasonCode [1]			
Extensions	**Crit.**	**Description**			
AKI	Non	CA public key identifier			
CRL Nb	Non	CRL serial number			
Expired CertsOnCRL	Non	Date from which revoked and expired certificates are maintained in the CRL.			

[1] An extension specifying the reason for revocation may be present in accordance with the commitments of chapters 4.9.1 and 4.9.3.2.

7.2.3 Profile of ARL for root CAs

		Certigna Server Authentication Root CA	Certigna Server Authentication EU Root CA	Certigna Root CA	Certigna
Fields		**Description**			
Version		V2			
Signature		SHA-256 RSA 4096	SHA-384 RSA 4096	SHA-256 RSA 4096	
Issuer DN		CN = Certigna Server Authentication Root CA O = Certigna C = FR	CN = Certigna Server Authentication EU Root CA O = Certigna C = FR	CN = Certigna Root CA OU = 0002 48146308100036 O = Dhimyotis C = FR	CN = Certigna O = Dhimyotis C = FR
This Update		ARL generation date			
Next Update		Next date of ARL update [1 year maximum]			
Revoked certificates		List of revoked CA certificate serial number: - Serial number - Revocation date - Revocation reason (since 09-30-2020)			
Extensions	**Crit.**	**Description**			
AKI	No	CA public key identifier			
CRL Nb	No	ARL serial number			
Expired CertsOnCRL	No	Date from which revoked and expired certificates are maintained in the ARL.			

7.3 OCSP Profile

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extension

The singleExtensions of an OCSP response MUST NOT contain the reasonCode (OID 2.5.29.21) CRL entry extension.

7.3.3 OCSP Profile for root CAs

		Certigna Server Authentication Root CA
Fields		**Description**
Version		V3
Signature		SHA-384 RSA 4096
Validity		15 years
Issuer DN		CN = Certigna Server Authentication Root CA O = Certigna C = FR
Subject DN		CN = Certigna Server Authentication Root OCSP OI = NTRFR-48146308100036 O = Certigna C = FR
Extensions	**Crit.**	**Description**
SKI	No	CA public key identifier
AKI	No	OSCP responder public key identifier
Key Usage	Yes	Digital signature
Extended Key Usage	No	Signature OCSP (1.3.6.1.5.5.7.3.9)
Ocsp No Check	No	
Basic Constraints	Yes	cA = FALSE

7.3.4 Profile of OCSP certificates from intermediate CA

Authority		SERVER AUTHENTICATION CA	SERVER AUTHENTICATION AUTO CA	SERVER AUTHENTICATION AUTO FR CA
Fields		**Content**		
Version		V3		
Serial Number		Unique serial number output from a CSPRNG. Between 128 and 160 bits		
Signature		CA signing algorithm identifier / SHA-256 minimum		
Subject Public Key Info		RSA 4096		
Validity		3 years		
Issuer DN	CN =	Certigna Server Authentication CA	Certigna Server Authentication Auto CA	Certigna Server Authentication Auto FR CA
	OI =	NTRFR-48146308100036		
	O =	Certigna		
	C =	FR		
Subject DN	CN =	Certigna Server Authentication OCSP	Certigna Server Authentication Auto OCSP	Certigna Server Authentication Auto FR OCSP
	OI =	NTRFR-48146308100036		
	O =	DHIMYOTIS		
	C =	FR		
Extensions	**Crit.**	**Description**		
Authority Key Id.	No	CA public key identifier		
Subject Key Id.	No	OSCP responder public key identifier		
Key Usage	Yes	Digital signature		
Extended Key U.	No	Signature OCSP (1.3.6.1.5.5.7.3.9)		
Ocsp No Check	No			
Basic Constraints	Yes	cA = FALSE		

		SERVICES CA	WILD CA
Fields		**Content**	
Version		V3	
Serial Number		Unique serial number output from a CSPRNG. Between 128 and 160 bits	
Signature		CA signing algorithm identifier / SHA-256 minimum	
Subject Public Key Info		RSA 3072	
Validity		3 years	
Issuer DN	CN =	Certigna Services CA	Certigna Wild CA
	OU =	0002 48146308100036	
	OI =	NTRFR-48146308100036	
	O =	DHIMYOTIS	
	C =	FR	
Subject DN	CN =	OCSP Certigna Services CA	OCSP Certigna Wild CA
	OU =	0002 48146308100036	
	O =	DHIMYOTIS	
	C =	FR	
Extensions	**Crit.**	**Description**	
Authority Key Id.	No	CA public key identifier	
Subject Key Id.	No	OSCP responder public key identifier	
Key Usage	Yes	Digital signature	
Extended Key U.	No	Signature OCSP (1.3.6.1.5.5.7.3.9)	
Ocsp No Check	No		
Basic Constraints	Yes	cA = FALSE	

	Autorité	SERVER AUTHENTICATION ACME CA G1	SERVER AUTHENTICATION ACME FR CA G1	SERVER AUTHENTICATION ACME CA G2	SERVER AUTHENTICATION ACME FR CA G2
Fields		**Content**			
Version		V3			
Serial Number		Unique serial number output from a CSPRNG. Between 128 and 160 bits			
Signature		CA signing algorithm identifier / SHA-256 RSA 4096			
Subject Public Key Info		RSA 4096			
Validity		3 ans			
Issuer DN	CN = OI = O = C =	Certigna Server Authentication ACME CA G1 NTRFR-48146308100036 Certigna FR	Certigna Server Authentication ACME FR CA G1 NTRFR-48146308100036 Certigna FR	Certigna Server Authentication ACME CA G2 NTRFR-48146308100036 Certigna FR	Certigna Server Authentication ACME FR CA G2 NTRFR-48146308100036 Certigna FR
Subject DN	CN = OI = O = C =	Certigna Server Authentication ACME OCSP G1 NTRFR-48146308100036 DHIMYOTIS FR	Certigna Server Authentication ACME FR OCSP G1 NTRFR-48146308100036 DHIMYOTIS FR	Certigna Server Authentication ACME OCSP G2 NTRFR-48146308100036 DHIMYOTIS FR	Certigna Server Authentication ACME FR OCSP G2 NTRFR-48146308100036 DHIMYOTIS FR
Extensions	**Critiq**	**Description**			
Authority Key Id.	No	CA public key identifier			
Subject Key Id.	No	OSCP responder public key identifier			
Key Usage	Yes	Digital signature			
Extended Key U.	No	Signature OCSP (1.3.6.1.5.5.7.3.9)			
Ocsp No Check	No				
Basic Constraints	Yes	cA = FALSE			

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT

Audits and assessments concern, firstly, those made for the issuance of a qualification attestation based on the Ordinance No. 2005-1516 of 8 December 2005 and eIDAS European Regulation and, secondly, those that are carried by the CA or outsourced to ensure that all its PKI is compliant with its commitments and practices stated in this CP/CPS.

The following chapters are for audits and evaluations of the responsibility of the CA to ensure the efficiency of its PKI.

The CA aims to comply with the current version of the « Baseline Requirements documents (SSL/TLS Server Certificates) » and the « EV Guidelines for TLS Server certificate » from the CA/Browser Forum (http://www.cabforum.org).

The CA may carry out audits of its DRAs' operators as well as the staff of its PKI. It ensures among others that DRA operators respect the requirements the practices identified in its CP/CPS. To this end, the CP/CPS is given to them.

8.1 Frequency or Circumstances of Assessment

A CA compliance check was performed before the deployment of certification services relative to means and rules mentioned in this CP/CPS.

This control is conducted once a year by the CA. A qualification audit is performed every year, with an audit period which does not exceed one year in duration, so that the period during which the CA issues Certificates is divided into an unbroken sequence of audit periods. The CA maintains a complete certification and qualification audit history from cradle to grave with no gaps.

Certificates that are capable of being used to issue new certificates are either Technically Constrained and audited in line with Section 8.7 only, or Unconstrained and fully audited in line with all remaining requirements from this section. A Certificate is deemed as capable of being used to issue new certificates if it contains an X.509v3 basicConstraints extension, with the cA boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

8.2 Identity/Qualifications of Assessor

Control is assigned by the CA to a team of competent auditors in computer security and in activity of the controlled component. Annual certification and qualification audits are carried out by qualified auditors. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.4);

- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- For audits conducted in accordance with any one of the ETSI standards accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
- Bound by law, government regulation, or professional code of ethics; and
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

The audit team do not belong to the component of the controlled PKI, whatever that component, and must be duly authorized to practice the targeted controls.

8.4 Topics Covered by Assessment

The CA annually undergoes an ETSI EN 319 411-1 audit which includes normative references to ETSI EN 319 401.

For Delegated Third Parties which are not RA or DRA, then the CA obtains an audit report, issued under the auditing standards that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or the CA's Certificate Policy and/or Certification Practice Statement. If the opinion is that the Delegated Third Party does not comply, then the CA does not allow the Delegated Third Party to continue performing delegated functions.

8.5 Actions Taken as a Result of Deficiency

Following a compliance check, the audit team provide to the CA, a notice from the following: "Improvement", "remark", "minor nonconformity", "major nonconformity ".

According to the results, the consequences of control are:

- In case of 'improvement', and according to the importance of the improvement, the audit team makes recommendations to CA to improve its functioning. Improvements are left to the discretion of the CA that decides whether or not to implement them.
- In case of "remark" or "minor nonconformity", the CA sends to the component a notice specifying in what timeframe nonconformities shall be lifted. Then, a control for confirmation will verify that all critical points have been resolved.
- In case of a "major nonconformity", and according to the importance of non-conformities, the audit team makes recommendations to the CA that can be business termination (temporary or permanent), revocation of certificate of component, revocation of all certificates issued since the last positive control, etc. The choice of measurement to be used is made by the CA and must respect the internal security policies.

Each session of audit permits to consult the opinion of the audit team. A control for confirmation will verify that all critical points have been resolved on time.

8.6 Communication of Results

An "Audit attestation" is publicly available on the assessment body website. This attestation is published no later three (3) months after the end of the audit period. In the event of a delay grater than three (3) months, the CA provides an explanatory letter signed by the Qualified Auditor.

The Audit attestation contain at least the following clearly-labelled information:

- name of the organization being audited;
- name and address of the organization performing the audit;
- the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit;
- audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
- a list of the CA policy documents, with version numbers, referenced during the audit;
- whether the audit assessed a period of time or a point in time;
- the start date and end date of the Audit Period, for those that cover a period of time;
- the point in time date, for those that are for a point in time;
- the date the report was issued, which will necessarily be after the end date or point in time date; and
- (for audits conducted in accordance with any of the ETSI standards) a statement to indicate if the audit was a full audit or a surveillance audit, and which portions of the criteria were applied and evaluated;
- statement to indicate that the auditor referenced the applicable CA/Browser Forum criteria, such as this document, and the version used.

8.7 Self-Audits

Compliance checks aim to verify compliance with the commitments and practices defined in the CA's CP/CPS, as well as the resulting elements (operational procedures, resources implemented, etc.).

During the period during which the CA issues certificates, the CA monitors adherence to the requirements of this CP/CPS and strictly its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

Effective 2025-03-15, the CA use a linting process to verify the technical accuracy of certificates within a selected sample.

Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in Section 8.4, the CA strictly control the service quality of Certificates issued or containing information

verified by a Delegated Third Party by having a Validation Specialist employed by the CA perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken.

The CA reviews the practices and procedures of each delegated third party to ensure that the delegated third party is in compliance with the requirements of this CP/CPS. The CA internally audit each Delegated Third Party's compliance on an annual basis.

During the period in which a Technically Constrained Subordinate CA issues Certificates, the CA which signed the Subordinate CA monitors adherence to the CA's CP/CPS and the Subordinate CA's CP/CPS. On at least a quarterly basis, against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by the Subordinate CA, during the period commencing immediately after the previous audit sample was taken, the CA shall ensure all applicable CP are met.

The results of the compliance audits by the audit team are made available to the organization in charge of the qualification of the CA.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The issue of certificates to CM is charged according to the rates on the website or on the order form.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

The access to certificate status information and revocation is free.

9.1.4 Fees for Other Services

Other costs may be charged. In this case, charges will be brought to the attention of those to whom they apply and are available from CA.

9.1.5 Refund Policy

The certificate order cannot be cancelled once the certificate request has been made. Then, Then, each certificate issued cannot be the subject of a request for reimbursement due to implementation difficulties related in particular to the technical operating environment of the certificate (e.g. non-compliance of software or hardware storing and using the certificate with the standards and norms in force). However, in the event that the certificate does not correspond to the certificate request, following an error exclusively attributable to the CA, the CA undertakes to provide a certificate compliant, or if it is unable to do so, to proceed with the reimbursement amounts already paid under the present CP/CPS and the TCSU associated.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

The CA holds an insurance policy in the field of professional civil liability, guaranteeing direct material or immaterial consequential damages caused in the exercise of his professional activity

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

Cf. chapter 9.9.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The information considered confidential are:

- The non-public part of the CP/CPS of the CA;
- The private keys of the CA, of components and of servers private key;
- Activation Data associated with CA private key and server private Key;
- All the PKI secrets;
- Event logs of components of the PKI;
- The CM registration records;
- The causes of revocation.

9.3.2 Information not within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

Generally, confidential information is accessible only to persons concerned by such information or who have the obligation to preserve and / or treat such information.

Once confidential information is subject to a special regime governed by a legislative and regulatory text, processing, access, modification of this information is made in accordance with the applicable legislation.

The CA implements security procedures to ensure confidentiality of the information identified in chapter 9.3.1, about the final erasure or destruction of media used for their storage. In addition, when data is exchanged, the CA guarantees their integrity.

The CA is particularly obliged to respect the laws and regulations in force on the French territory. It may need to provide the registration records of CM to third parties in connection with legal proceedings. It also provides access to this information at CM, certification agents and possibly DRA's operators in connection with the CMs.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

By accepting these GCSU the Subscriber, the CM acknowledges having read the CERTIGNA Personal Data Use Policy available on the Website https://www.certigna.com/politique-dutilisation-des-donnees-personnelles/.

The data provided by the Subscriber, the CM, when registering on the Website https://www.certigna.com, when ordering and when request for certificate are Personal Data, the collection and processing of which are governed by the Aforementioned Personal Data Policy.

Electronic certificate application files containing personal data are archived for at least seven years after certificate expiration and as long as necessary for the purposes of providing proof of certification in legal proceedings, in accordance with applicable law. The personal identity information can be used as authentication data in the event of a request for revocation or information.

Application logs related to the life cycle of certificates and including personal data are archived at least seven years after the expiration of the associated certificates and as long as necessary for the purposes of providing proof of certification in legal procedures, in accordance with applicable law.

In addition, CERTIGNA retains the personal data for a period of three years from the end of the commercial relationship with the customer and 3 years from the last contact with the prospect. The delay starts from the last connection to the customer account or the last sending of an email to customer service, or from a click on a hypertext link of an email sent by CERTIGNA, a positive response to an email requesting if the client wishes to continue to receive commercial prospecting at the end of the three-year period.

In order to monitor the quality of our services, calls made to our customer service are likely to be registered and kept for a period of 30 days.

In accordance with the law n ° 78-17 of January 6, 1978 relating to data, files and freedoms, modified and the European regulation "2016/679 / EU of April 27, 2016" relating to the protection of natural persons to the processing of personal data and the free movement of such data, you have the right to access, oppose, rectify, delete and portability of your personal data. You can exercise your right by sending an email to: privacy@certigna.com, or by mail to the following address:

CERTIGNA, Service du DPO,

20 Allée de Râperie, 59 650 Villeneuve d'Ascq, France

Your request must indicate your surname and first name, e-mail or postal address, be signed and accompanied by a valid proof of identity.

9.4.2 Information Treated as Private

The information considered as personal are:

- The causes of revocation of server certificates;
- The registration files of RC, of DRA's operators and of certification agents.

9.4.3 Information not Deemed Private

No stipulation.

9.4.4 Responsibility to Protect Private Information

Cf. legislation and regulations on French territory.

9.4.5 Notice and Consent to Use Private Information

Accordance with the laws and regulations on French territory, personal information submitted by CM to CA must not be disclosed or transferred to third parties except in the following circumstances: prior consent of the CM, court order or other legal authorization.

9.4.6 Disclosure pursuant to Judicial or Administrative Process

The disclosure of confidential information is only made to the authorities empowered officially and exclusively on their specific request in accordance with French law.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

The brand "CERTIGNA" is protected by the Code of Industrial Property. The use of this trademark by the entity is allowed only in the framework of the subscription contract.

9.6 Representations and Warranties

Obligations common to the PKI components are:

- To protect and ensure the integrity and confidentiality of their secret keys and / or private;
- Only use their cryptographic keys (public, private and / or secret) for the purposes specified when issued and with the equipment as specified in the conditions set by the CA's CP/CPS and documents arising therefrom;

- Respect and implement the part of the CP/CPS incumbent upon them (this part shall be communicated to the corresponding component);
- Submit to compliance checks by the audit team mandated by the CA (See Chapter 8) and the qualifying body;
- Respect the agreements or contracts between them or with the entity;
- To document their internal operating procedures;
- Implement the means (human and technical) necessary to achieve the benefits to which they are committed under conditions that ensure quality and safety.

9.6.1 CA Representations and Warranties

The CA will:

- can demonstrate to certificate users; it has issued a certificate to a server and the corresponding CM accepted the certificate in accordance with the requirements of Section 4.4;
- Ensure and maintain the consistency of this CP/CPS;
- Take all reasonable steps to ensure that CM are aware of their rights and obligations regarding the use and management of keys, certificates or equipment and software used for PKI. The relationship between CM and the CA is formalized in a contractual relationship / regulation specifying the rights and obligations of the parties including the guarantees provided by the CA.
- At the time of issuance, implement and follow the requirements describes at sections 3.2 and 3.3 of this CP for verifying that the organization attached to the server authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Organization attached to the server.
- At the time of issuance, implement and follow the requirements describes at sections 3.2 and 3.3 of this CP/CPS for verifying the accuracy of all of the information contained in the Certificate.
- At the time of issuance, implement and follow the requirements describes at sections 3.2 and 3.3 of this CP/CPS for verifying the identity of the organization, the legal representative and the designated Certificate Manager.
- If the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements,
- If the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
- Maintain a 24 x 7 publicly accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates;
- Revoke the Certificate for any of the reasons specified at section 4.9 of this CP/CPS.
- At the time of issuance, implement and follow the requirements describes at sections 3.2 and 3.3 of this CP/CPS for verifying that the Certificate Manager either had the right to use, or had control of, the Domain Name(s) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control).

CA assumes any harmful consequences resulting from non-compliance of its CP/CPS by itself or one of its components. CA planned to meet its responsibilities in its operations and / or activities and have the financial stability and resources required to operate in accordance with this policy. In addition, the CA recognizes its liability in case of fault or negligence of itself or one of its components, regardless of the nature and gravity, which would result in reading, alteration or misuse of personal data of CM for fraudulent purposes, these data are contained in transit or in the certificate management applications of the CA.

Furthermore, the CA recognizes having to bear a general duty of supervision for the safety and integrity of certificates issued by itself or one of its components. She is responsible for maintaining the security level of technical infrastructure on which it relies to provide its services. Any changes affecting the level of security provided shall be approved by the high-level bodies of the CA.

The Root CA is responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates.

9.6.2 RA Representations and Warranties

The registration authority is committed to verify and validate the certificate requests and certificate revocation.

9.6.3 Subscriber Representations and Warranties

The CM has the following obligations:

- Make its certificate request by following all procedure steps provided on the Website https://www.certigna.fr;
- Respect the Terms and Conditions of Sale and Use (TCSU) of the requested certificate and use the certificate solely in compliance with applicable laws and solely in accordance with the TCSU;
- Know and accept that the CA is entitled to revoke the certificate immediately if the CM or the Subscriber violate the TCSU or if revocation is required by the CA's CP/CPS or applicable requirements;
- Provide accurate, complete and up-to-date information during the certificate request or its renewal;
- Send to RA, if applicable to the DRA or to a Certification Agent of the entity, by hand or by post, the registration form generated at the time of the certificate request online on the Website: or on the DRA's website where appropriate, the payment, as well as the evidence documents.
- If necessary, generate the key pair with a RSA modulus size of 2048 bits and in compliance with ESTI 119 312 specifications;
- Generate the key pair associated with the certificate in a device or cryptographic device meeting the requirements of Chapter 11 of the Associated Certification Policy.

- Evidence that the device compliance could be required by the CA durung the certificate request (in particular for a seal certificate. These evidences to provide will be at a minimum, the device's purchase invoice and the screen shots / prints of the hardware and software features of the device and the associated serial number. The CA reserves the right to refuse the certificate request if it is found that this device does not meet these requirements.
- In the case where the CA would be informed or would identified the loss of the compliance of the device, the CA will ask the the CM for proof that the key pair is stored in a device that meets the requirements of Chapter 11 of the CP/CPS associated to the certificate.
- The CM undertakes to provide these evidences (E.g: Invoice of purchase of a new device certified QSCD, Minutes of ceremony of the keys in case of key migration, Minutes of update of the device for the maintenance of the certification, etc.) within a deadline fifteen (15) days following the request. In the event that no evidence is provided or that the latter do not make it possible to determine if the storage conditions of the key pair, and transfer in another device if any, meet the requirements of the Certification Policy, the CA gives itself the right to revoke the certificate.
- Inform the RA in case of non-receipt of an e-mail confirming the certificate request or revocation request.
- Following receipt of an e-mail from the RA indicating the non-conformity of the certificate request or that the request is incomplete, make the modifications within seven (7) calendar days after receipt of this e-mail.
- Download the generated certificate, available on its customer area where appropriate, within thirty (30) days of the validation of the certificate request which is notified by e-mail to the CM. Beyond this period, the certificate is automatically revoked by the RA;
- Accept the certificate explicitly from its CERTIGNA customer area or form the DRA"s website where appropriate, or tacitly when using ACME Service. This acceptation can also be done by sending a paper form signed by the Subject or the CM on the express request of the RA. In the event of explicit non-acceptance, the certificate is automatically revoked by the RA;
- Protect the private key associated with the certificate for which he is responsible by means appropriate to its environment and in compliance with the requirements from chapter 11;
- Protect its activation data and, if necessary, implement it;
- Protect access to the certificate database of the server for server and / or client authentication certificate;
- Respect the conditions of use of the certificate and of the associated private key mentioned in chapter 4.5 of this document;
- Inform the CA of any changes to the information contained in the certificate;
- Immediately make a certificate revocation request for which it is responsible to the RA, the DRA to which the certificate request has been made or, where appropriate, the Certification Agent of the entity, in the event of loss, theft, compromise or suspected compromise of the corresponding private key, or when one of the causes of revocation of Chapter 4.9.11 is encountered ;
- Take all appropriate measures to ensure the security of the device(s) on which the certificate is installed. The CM is solely responsible for the installation of the certificate;
- Install web authentication certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate;
- Respond to the CA's instructions concerning Key Compromise or Certificate misuse within 24 hours ;

- Immediately and permanently discontinue the use of a certificate and its private key after the expiry or revocation of this certificate, and delete the associated key pair;
- no longer use a certificate if it has been revoked or if the CA that issued it has been compromised;
- Inform RA without delay of its departure from the entity or change of responsibilities and the need to register a new CM.
- Check the suitability of the certificate and its characteristics;
- Ensure that the hardware and / or software prerequisites recommended by the CA are met in view of the installation and use of the certificate;
- Have all the skills and means necessary to use the certificates;
- Implement measures to prevent any unauthorized person from physically accessing the device storing the keys and the certificate;
- Immediately notify the person in charge of the security of the information systems of his entity (example: CISO) in case of loss or theft of the device storing the keys and the certificate; and
- For applications deemed to be the most critical at the business level, implement measures to detect potentially fraudulent transactions (inconsistency of signed business data, etc.) and to provide, if necessary, an alternative procedure.
- For a server and / or client authentication certificate, and in the case where, for one or more domain names to be included in the certificate, the "DNS CAA" option is enabled, the RC must update the associated DNS records to include the CA, prior to the request for a certificate.

The relationship between the CM and the CA or its components is formalized by a commitment from the CM to certify the accuracy of the information and documents provided. This information also applies to DRA operators and Certification Agents.

The subscriber has the duty to:

- Apply for a certificate by following all the steps of the procedure appearing on the Website https://www.certigna.fr;
- Respect the Terms and Conditions of Sale and Use (TCSU) of the requested certificate and use the certificate solely in compliance with applicable laws and solely in accordance with the TCSU;
- Know and accept that the CA is entitled to revoke the certificate immediately if the CM or the Subscriber violate the TCSU or if revocation is required by the CA's CP/CPS or applicable requirements;
- Communicate exact, complete and up-to-date information for the creation of his customer account, the request for certificate or its renewal;
- Confirm that the information to be placed in the certificate is correct;
- Send to the RA, if applicable to the DRA, or to a Certification Agent of the legal entity attached to the certificate, by hand or by post (at its expense), the registration form generated during the request for certificate online on the Website or on the DRA Website where applicable, payment, as well as supporting documents.
- Comply with the conditions of use of the certificate and the associated private key set out in chapter 4.5 hereof and prohibit any unauthorized use of the certificate and the associated private key of the server, the seal service or the server;
- If necessary, generate the key pair with a 2048-bit RSA modulus and in compliance with ESTI 119 312 specifications;

- If necessary, generate the key pair associated with the certificate in a cryptographic device which complies with the security requirements of chapter 11 ;
- Supporting documents attesting to the conformity of the cryptographic device may be requested by the CA when requesting a certificate (in the case of a seal certificate). These supporting documents will be at a minimum the purchase invoice of the device and photos / screenshots of the hardware and software characteristics of the device and the associated serial number. The CA reserves the right to refuse the certificate request in the absence of supporting documents or if it has been proven that this device does not meet these requirements.
- Keep the server private key under his sole control;
- Maintain the private key of the seal or server service under the control of the associated legal person;
- Immediately inform the CA of any loss, theft or compromise of the server private key, seal or server service;
- Immediately inform the CA if control of the private key of the server has been lost due to the compromise of activation data (for example, the PIN code) or other reasons;
- Immediately inform the CA of any modification concerning the information contained in the certificate;
- Inform the RA in the event of non-receipt of an email confirming that the request for certificate or revocation has been taken into account;
- Following receipt of an email from the RA indicating the non-compliance of the certificate application or that the file is incomplete, make the changes within seven (7) calendar days after receipt of said email;
- Make sure that the certificate of the server, the seal service or the server is no longer used following the expiration or revocation of this certificate (except for encipherment keys).
- check the suitability of the certificate and its characteristics to its needs;
- Respond to the CA's instructions concerning Key Compromise or Certificate misuse within 24 hours.

9.6.4 Relying Party Representations and Warranties

Third party users must:

- Check and maintain the use for which a certificate was issued;
- For each certificate of the certification chain, from the end-entities certificate to the Certigna Root CA, verify the digital signature of the issuing CA on the certificate and check the validity of the certificate (validity date, revocation status);
- Check and respect the obligations of certificate users expressed in this CP/CPS.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.6.6 Termination

In the event of a breach by the CA or the CM to one of its obligations hereunder, the other party shall be authorized thirty (30) days after formal notice sent by registered letter with acknowledgment of receipt, had no effect, to terminate these by operation of law by registered letter with acknowledgment of receipt without prejudice to any damages and interests to which it could claim due to the deficiencies invoked.

9.7 Disclaimers of Warranties

Any certificate ordered must be accepted by the CM on the customer space created from the CA website or from one of its DRA. Before generating the certificate, the CM must verify that the information stated in his certificate request is accurate. Failing this, the CM must contact a member of the staff of the CA either by telephone at 0 806 115 115 (free service cost of a local call), or by email at the following address: contact@certigna.fr. Telephone support is available from Monday to Friday, except holidays, from 9 AM to 6 PM without interruption. The CM is aware that in case of error during the order in the nature of the certificate, no modification can be made by the CA and the CM will have to make a new certificate request. If a payment had already been made, the CA would not be required to pay any refund.

Once the certificate request validated, the certificate is generated. The CM is then brought to confirm the accuracy of said information, which means acceptance of the certificate. otherwise, the CM will have to make a new certificate request and the certificate generated will not give rise to any refund.

Once the certificate accepted, the certificate is available to the CM either on his customer area or on a cryptographic device. the installation of the certificate is done under the sole responsibility of the CM. In case of any difficulty during this last phase, the CM can contact the CA at the telephone number and the email address indicated above or via contact details available on the DRA website. The CA does not guarantee the operation of the certificate in the case of use outside the uses provided for in chapter 1.5 hereof.

The warranty is valid for the worldwide outside the USA and Canada.

9.8 Limitations of Liability

The CA is subject to a general obligation of means. The CA cannot be held liable for the CM or the Subscriber for direct damage that may be attributed to it for the services entrusted to it under these TCSU.

The CA's responsibility cannot be sought for any indirect loss, such as, in particular, loss of turnover, loss of profit, loss of orders, loss of data, loss of opportunity, disturbance to the image or any other special damage or events beyond its control or any fact not attributable to it.

The CA is only responsible for the tasks specifically assigned to it under this CP/CPS.

The CA cannot be held responsible in any way for the use made by the CM of the certificates, nor the contents of the documents and the data which are given to it by the CM or the applicant.

In any case, the responsibility of the CA cannot be sought in case of:

- Fault, negligence, omission or default of the CA, which would constitute the exclusive cause of the occurrence of the damage,
- Malfunction or unavailability of tangible or intangible property in the case where it has been provided by the CM,
- Delay in providing the data to be processed due to the CM;
- Loss of the qualification of a third-party provider that is beyond the control of CERTIGNA (ex: the supplier of cryptographic support).

By express agreement between the CA and the CM, the liability of the CA is limited, by certificate request, all damages, to the sum of two (2) times the amount paid under the certificate request.

9.9 Indemnities

CERTIGNA signed a contract of "liability insurance".

The CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others.

The CA defends, indemnifies, and holds harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy a Certificate that has expired, or a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.1 Indemnification by CM

No stipulation.

9.9.2 Indemnification by Relying Parties

No stipulation.

9.10 Term and Termination

9.10.1 Term

CA's CP/CPS remain in effect at least until the end of life of the last certificate issued under this CP/CPS.

9.10.2 Termination

The publication of a new version of the documents mentioned at chapter 1.1 may result, depending on the changes made, the need for the CA to evolve its corresponding CP/CPS. In this case, such compliance will not impose the early renewal of licenses already issued, except in exceptional cases linked to security.

Finally, the validity of the CP/CPS can happen prematurely in case of cessation of trading of the CA (see section 5.8).

9.10.3 Effect of termination and Survival

The end of validity of the CP/CPS also terminates all clauses within it.

9.11 Individual Notices and Communications with Participants

In case of change of any kind involved in the composition of the PKI, the CA will:

- Validate later than one month before the start of the operation, this change through technical expertise to assess the impacts on the quality and safety functions of the CA and its various components;
- Inform, within one month after the end of the operation, the evaluation body.

9.12 Amendments

9.12.1 Procedure for Amendment

The CA conducts any change in the specifications stipulated in the CP/CPS and / or components of the CA that appears necessary to improve the quality of certification services and the security of processes, remaining however meets the requirements of RGS and additional documents to the latter. A review and an update of the CP/CPS are annually carried out and when needed.

The CA also conducts any changes to the specifications stipulated in the CP/CPS and / or components of the CA that is made necessary by legislation, regulations or by the results of checks.

9.12.2 Notification Mechanism and Period

The CA communicates via its website https://www.certigna.com the evolution of the CP/CPS based on its amendments.

9.12.3 Circumstances under which OID Must Be Changed

The OID of the CA's CP/CPS being registered in the certificates it issues, evolution in this CP/CPS has a major impact on the certificates already issued (e.g., increase in registration requirements of subjects, which cannot be applied to certificates already issued) must result in a change of the OID, so that users can clearly distinguish which certificates correspond to which requirements. When the change of the CP/CPS is typographical or it does not impact the quality and safety of the functions of the CA and the RA, the OID of the CP/CPS are not changed.

9.13 Dispute Resolution Provisions

The validity of this CP/CPS and any other question or dispute relating to its interpretation, execution or termination will be governed by French law.

The CA and the CM commit themselves to devote their best efforts to the amicable resolution of all the questions or the litigation which could divide them, before the seizure of the jurisdiction hereinafter designated.

The CA and the CM agree, in the event that an amicable agreement is impossible to stop, that the courts of Lille will have exclusive jurisdiction to hear any dispute resulting from the validity, interpretation, execution or termination hereof, and more generally from any dispute arising herein that could divide them, notwithstanding pluralities of defendants or warranty claim.

To bring a complaint to CERTIGNA's attention, please use the contact form available at the following address https://www.certigna.com/contactez-nous/ and select the "Réclamation" reason.

You can also make a complaint to our customer service department using the following contact details:
- Contact e-mail: contact@certigna.fr ;
- Telephone: 0 806 115 115 (Free service) available Monday to Friday from 09:00 to 18:00;
- Chat on the https://www.certigna.com website, available Monday to Friday from 9am to 18:00;
- Mail addressed to

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

Information on the processing of your personal data is available in the Policy on the use of personal data, which can be accessed at the following address: https://www.certigna.com/politique-dutilisation-des-donnees-personnelles/.

9.14 Governing Law

Any dispute concerning the validity, interpretation, execution of this CP/CPS will be submitted to the courts of Lille.

9.15 Compliance with Applicable Law

This CP/CPS is subject to French law and applicable legislative texts for this CP/CPS.

The trust service practices under which the CA operates are non-discriminatory.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This document contains all the provisions governing the PKI.

9.16.2 Assignment

Cf. chapter 5.8.

9.16.3 Severability

In case of an invalid clause, the other clauses are not questioned.

In the event of a conflict between the requirements of this CP/CPS and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which the CA operates or issues certificates, CA modifies any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, CA immediately include in this section (and prior to issuing a certificate under the modified requirement) a detailed reference to the Law requiring a modification of these requirements and the specific modification to these Requirements implemented by the CA.

The CA notifies the CA/Browser Forum and ANSSI (prior to issuing a certificate under the modified requirement) of the relevant information newly added to this CP/CPS by sending a message to questions@cabforum.org (or such other email addresses and links as the Forum may designate) leading to a confirmation.

Any modification to CA practice enabled under this section is discontinued if and when the Law no longer applies, or these requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to the CP/CPS of CA and a notice to the CA/Browser Forum are made within 90 days.

9.16.4 Enforcement

No renunciation of any of his rights shall be allowed to take place tacitly. To be opposable to the AC a renunciation must have been made in writing. Such waiver shall not constitute a renunciation of future rights audits.

9.16.5 Force Majeure

The CA will not be held responsible for any delay or failure in the performance of any of its obligations under this CP/CPS, if the delay or failure is due to the occurrence of a case of force majeure usually recognized by the jurisprudence of French courts and tribunals.

9.17 Other Provisions

9.17.1 Additional testing

Certificates issued on the production environment are used for testing purpose and conform with the requirements of this document and are not used outside of the testing scope. In particular, the CA reduces the lifetime of test certificates to the duration of the tests, or revokes test certificates once the tests have been completed.

10 APPENDIX 1: SECURITY REQUIREMENTS FOR THE CA'S CRYPTOGRAPHIC MODULE

10.1 Security Objectives Requirements

The cryptographic module used by the CA to generate and implement its signature keys (for the generation of electronic certificates, CRL, and OCSP responses), must meet the following security requirements:

- Ensuring the confidentiality and integrity of the CA's signature private keys throughout their lifecycle, and ensuring their secure destruction at their end-of-life;
- Being able to identify and authenticate its users;
- Limiting access to its services per the user and role assigned;
- Ability to carry out a series of tests to verify that it is running correctly and enter in a secure status if an error is detected;
- Create a secure electronic signature to sign the certificates generated by the CA, that does not reveal the CA's private keys and that cannot be falsified without knowing these private keys;
- Creating audit records for each modification relating to security;
- If a backup and restoration function for the CA's private keys is offered, guaranteeing the confidentiality and integrity of the backed-up data and demanding at least a double control of the backup and restoration operations.

10.2 Qualification Requirements

The cryptographic module used by the CA is:

- Common Criteria at EAL 4+ level or FIPS 140-2 Level 3.

11 APPENDIX 2: SECURITY REQUIREMENTS FOR THE DEVISE USED BY THE CM

11.1 Security objectives requirements

RGS *
The device used by the server to store and implement its private key, and, where appropriate, generate its key pair, must meet the following security requirements: - If the server key pair is generated by the device, guaranteeing that this generation is implemented exclusively by authorized users and guaranteeing the cryptographic sturdiness of the generated key pair; - Ensuring the correspondence between the private key and the public key; - the generated authentication cannot be falsified without knowing the private key; - Detecting defects during the initialization, customization and operation phases, and ensuring secure techniques for the destruction of the private key in case of re-generation of the private key; - Guaranteeing the private key's confidentiality and integrity; - Ensuring the public key's authenticity and integrity when exported outside of the device; - Ensuring for the legitimate server the authentication function and the session symmetric keys encipherment function and protecting the private key against any usage by third parties. - Ensure the authenticity and the integrity of the session symmetric key, after encipherment, during its export from the device to the data encipherment application.

11.2 Qualification Requirements

No stipulation.

Certigna

www.certigna.com

© Certigna, Services de confiance numérique