CERTIFICATION POLICY and PUBLIC CERTIFICATION PRACTICE STATEMENT

CERTINOMIS WEB ROOT CA
CERTINOMIS CA WEB G2 / G3
CERTINOMIS CA SAFE G2 / G3
CERTINOMIS CA ACME

ISSUER	RECIPIENTS	CC
CERTINOMIS	PUBLIC	

Certinomis

Docaposte Certinomis SAS with a capital of €40,156.

Head office: 45-47, Boulevard Paul Vaillant-Couturier

94200 Ivry sur Seine – France. Créteil Trade and Companies Register B 433 998 903

History of the versions

DATE	VERSION	DEVELOPMENTS	AUTHOR
05/12/2024	1.0	Initial version	CERTINOMIS
24/12/2024	1.1	Corrected version following the qualification audit	CERTINOMIS
05/03/2025	1.2	Update of archive retention period in chapter 5.5.2.3	CERTINOMIS
06/10/2025	1.3	Paragraph 5.7.2 updated to indicate the mass revocation procedure. Added registration manager and revocation manager trust roles in chapters 5.2.1 and 5.2.4 Update of the CA hierarchy in §1.1 Addition of the G3 CA and ACME chain Update of OCSP certificate templates Update of the EV certificates template	CERTINOMIS
20/02/2026	1.4	Corrections following the LSTI audit: - Update under the CP/CPS - Time difference between OCSP response and CRL (chapter 2.1) - Identification of the OIDs of eIDAS-qualified certificate policies (chapter 1.2) - Addition to paragraph 1.1 of adherence to the latest version of the Chrome Root Store and CCADB programme policies	CERTINOMIS
26/02/2026	1.5	Implementation of the new 200-day certificate validity period	CERTINOMIS

Table of contents

WARNING

1 INTRODUCTION

1.1 OVERVIEW

1.1.1 Certinomis PKI

Certinomis is an Electronic Certification Service Provider (ECSP) whose business is the guarantee of identity in the broadest sense in electronic exchanges: identity of natural persons acting on their own behalf or in the name of a legal entity, or identification of a legal entity responsible for the implementation of an IT application.

The ECSP carries out its missions by issuing electronic certificates through various Certification Authorities (CA) that are part of a Public Key Infrastructure (PKI), a set of technical, human, documentary and contractual resources made available to users to ensure, with asymmetric cryptography systems, a secure environment for electronic exchanges.

The implementation of a PKI, necessary for security and trust, opens up a range of value-added services for electronic transactions (for example: commercial transactions, signature of contracts, remote procedures, etc.).

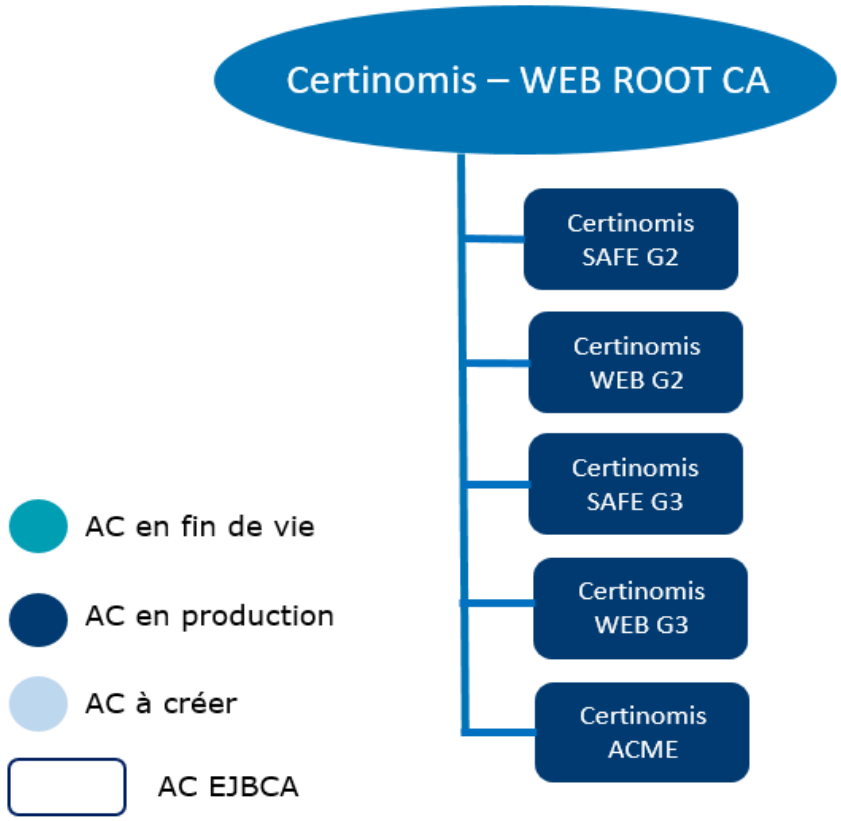
Their purpose is to ensure:

- the integrity of messages;
- identification and authentication[1];
- the authenticity of the origin;
- and confidentiality.

The Certinomis public PKI is composed of two Root Certification Authorities. This CP concerns the Root CA "CERTINOMIS WEB ROOT CA" and its five intermediate CAs. This hierarchy is dedicated to the certificate issuance service for server authentication.

Certinomis adheres to the requirements of the latest versions of the CCADB policies (https://www.ccadb.org/policy) and Chrome Root Store (https://googlechrome.github.io/chromerootprogram/)

[1] With the stipulation that this is not in the sense of official documents, as governed by articles 1317 et seq of the Civil Code, but in the technical sense of cryptographic authentication



French	English
AC en fin de vie	CA at the end of life
AC en fin de production	CA at the end of production
AC à créer	CA to be created
AC EJBCA	EJBCA CA

Figure 1: SSL CA hierarchy

1.1.2 Purpose of the document

The purpose of this Certification Policy and Public Certification Practice Statement is to enable the issuance of certificates identifying IT applications and the legal entity responsible for their implementation, and which will be used to authenticate the applications they identify or to protect the confidentiality of exchanges.

It concerns the Root CA "CERTINOMIS WEB ROOT CA" and its five intermediate CAs.

This Certification Policy and Public Certification Practice Statement details, as its name suggests, certain certification practices to the public in order to comply with the requirements expressed by the Cab Forum in this regard.

The Certification Policy and Public Certification Practice Statement defined in this document is intended to be used by companies, associations, ministries, administrative or governmental entities and groups of any kind, as well as individuals. The people consulting and using this document can obtain additional implementation details from the issuer CA.

The Certification Policy and Public Certification Practice Statement covers the management and use of certificates, according to their classes, containing the public keys used for the functions of verification, authentication, integrity and matching of keys.

The Certification Policy and the Public Certification Practice Statement also cover the management and use of certificates containing public keys used for confidentiality functions. The certificates issued under this policy ensure the confidentiality of information considered private or sensitive by their owners. The certificates are not used to protect classified information.
The delivery of a public key certificate pursuant to the present policy does not mean that the customer or beneficiary is authorised in any way to carry out commercial or other transactions in the name of the organisation using the CA.

The CA will be subject to the laws and regulations applicable within the French Republic, as well as to the applicable European standards and international agreements ratified by France, that relate to the application, preparation, interpretation and validity of the certification policies mentioned in the present document.

The CA reserves the right not to sign a cross-certification agreement with an external certification authority.

1.2 DOCUMENT IDENTIFICATION

The Object Identifier (OID) designation of this document is: 1.2.250.1.86.2.6.0.100.1
This document covers several certification policies, for each of which an OID has been assigned. The ETSI policy adopted as the basis is specified in the table below for each Certinomis PC.

Root CA: 1.2.250.1.86.2.6.0.100.1		
AC SAFE G2		
OID	*Usage*	*ETSI / RGS Compliance*
1.2.250.1.86.2.6.8.63.1	Server authentication	EN 319 411-2 QEVCP-w (0.4.0.194112.1.4) eIDAS Qualified Certificate
1.2.250.1.86.2.6.8.62.1	Server authentication	EN 319 411-2 QNCP-w (0.4.0.194112.1.5) eIDAS Qualified Certificate
WEB CA G2		
OID	*Usage*	*ETSI / RGS Compliance*
1.2.250.1.86.2.6.7.20.1	Server authentication	RGS 1 star, EN 319 411-1 OVCP (0.4.0.2042.1.7)
1.2.250.1.86.2.6.7.61.1	Server authentication	EN 319 411-1 OVCP (0.4.0.2042.1.7)
1.2.250.1.86.2.6.7.60.1	Server authentication	EN 319 411-1 DVCP (0.4.0.2042.1.6)
AC SAFE G3		
OID	*Usage*	*ETSI / RGS Compliance*
1.2.250.1.86.2.6.19.63.1	Server authentication	EN 319 411-2 QEVCP-w (0.4.0.194112.1.4) eIDAS Qualified Certificate
1.2.250.1.86.2.6.19.62.1	Server authentication	EN 319 411-2 QNCP-w (0.4.0.194112.1.5) eIDAS Qualified Certificate
WEB CA G3		
OID	*Usage*	*ETSI / RGS Compliance*
1.2.250.1.86.2.6.18.20.1	Server authentication	RGS 1 star, EN 319 411-1 OVCP (0.4.0.2042.1.7)

1.2.250.1.86.2.6.18.61.1	Server authentication	EN 319 411-1 OVCP (0.4.0.2042.1.7)
1.2.250.1.86.2.6.18.60.1	Server authentication	EN 319 411-1 DVCP (0.4.0.2042.1.6)
CA ACME		
OID	*Usage*	*ETSI / RGS Compliance*
1.2.250.1.86.2.6.17.20.1	Server authentication	RGS 1 star, EN 319 411-1 OVCP (0.4.0.2042.1.7)
1.2.250.1.86.2.6.17.61.1	Server authentication	EN 319 411-1 OVCP (0.4.0.2042.1.7)
1.2.250.1.86.2.6.17.60.1	Server authentication	EN 319 411-1 DVCP (0.4.0.2042.1.6)

1.3 ENTITIES INVOLVED IN THE PKI

When a service provider supplies certification services, i.e. it provides certificates or supplies other services related to digital signatures, one must distinguish between several professions or functions, that result in distinct roles and responsibilities.

The certification process and management of the certificate's lifecycle require a broad range of participants in the trust chain:

- Certification authority,
- Registration authority,
- Beneficiaries of the Certification Authority (Certificate Manager),
- Subject of the certificate provided by the Certification Authority,
- Third party users.

1.3.1 Certification authorities

The Certification Authority is responsible to its customers, but also to everyone relying on a certificate that it has issued, for the entire certification process, and therefore the validity of certificates that it issues. As such, it determines the Certification Policy and validates the Certification Practices Declaration that are followed by the various components of the Public Key Infrastructure.

The guarantee provided by the Certification Authority results from the quality of the implemented technology, but also from the regulatory and contractual framework that it defines and undertakes to comply with.

The CA provides management services for the certificates throughout their lifecycle (generation, dissemination, renewal, revocation…), and therefore relies on a technical infrastructure: a key management infrastructure (PKI).

The CA's services are the results of various functions that correspond with the various steps in the lifecycle of the key pairs and certificates (cf. below).

Registration Authority (RA) - This function verifies the identification information of the future subject of a certificate, as well as possibly other specific attributes, before sending the corresponding request to the appropriate PKI function, depending on the services rendered and the PKI organisation (see below). When necessary, the RA also looks after re-verifying information about the certificate's subject, when the certificate of the latter is being renewed.

Certificate generation function - This function generates (creation of the format, electronic signature with the CA's private key) the certificates from the information transmitted by the registration authority and the subject's public key originating either from the beneficiary or from the function generating the beneficiary's secret elements, if it is the latter that generates the certificate's key pair.

Function generating the beneficiary's secret elements - This function generates the secret elements intended for the beneficiary, and prepares them prior to their delivery to the beneficiary (for example, customisation of the smart card intended for the subject, secure letter with the activation code, etc.). These secret elements are directly the certificate's key pair, the codes (activation / release) are linked to the storage device for the beneficiary's private key.

Beneficiary delivery function - At the very least, this function provides the certificate to the beneficiary, and possibly other elements provided by the CA (cryptographic device, subject's private key, activation codes...).

Publication function - This function provides the various parties in question with the general terms, policies and practices published by the CA, the CA's certificates and all other relevant information intended for the beneficiaries and/or users of the certificates, excluding information on the status of the certificates. The CA does not provide the valid certificates of its beneficiaries.

Revocation management function - This function deals with revocation requests (notably identification and authentication of the requester) and determines the actions to be undertaken. The results of the processes are disseminated via the function that provides information on the status of the certificates.

Certificate status information function - This function provides certificate users with information on the status of the certificates (revoked, suspended, etc.). This function is carried out on the basis of an information publication mode that is updated at regular intervals: CRL, LRCC.

A certain number of entities / natural persons outside of the PKI interact with the latter. This notably relates to:

Subject - The natural person identified in the certificate and who holds the private key corresponding with the public key that is in this certificate.

Certificate Manager (CM) - The person in charge of and responsible for the electronic certificate of the application service used for the server's stamping or authentication.

Certification Agent (CAG) - The certification agent is appointed by and placed under the responsibility of the customer entity. He is in direct contact with the RA. For the latter, he provides a certain number of verifications regarding the identity and, possibly, the attributes of this entity's beneficiaries (he notably carries out the face-to-face meeting in order to identify the beneficiaries, when this is required).

Certificate user - The entity or natural person who receives a certificate and who relies on it in order to verify an electronic signature coming from the certificate's beneficiary.

Authorised person - This is a person other than the beneficiary and the certification agent, who is authorised by the CA's Certification Policy or by contract with the CA to perform certain actions on behalf of the beneficiary (requesting a revocation, renewal, ...). Typically, in a company or administration, this can be a hierarchical manager of the beneficiary or a human resources manager.

1.3.2 Registration authority

The Registration Authority applies procedures for identifying natural or legal persons, in compliance with the rules defined by the Certification Authority. Its aim is to establish that the requester has the identity and qualities that will be indicated in the certificate. These identification procedures are variable according to the confidence level that we intend to provide to the verification.

The Registration Authority is the link between the Certification Authority and the beneficiary. Whether or not it is directly in physical contact with the beneficiary, it remains the custodian of the personal information.

It can only be held liable by the Certification Authority. The Certification Authority has a duty to control and audit the Registration Authorities.

The role of the RA is to identify the future subject of the certificate. For this purpose, the RA carries out the following tasks:

- the acknowledgment and verification of the information regarding the future subject and its attachments entity, and the preparation of the corresponding registration file;
- if relevant, the acknowledgment and verification of the information regarding the future CAG and their reporting entity, and the preparation of the corresponding registration file;
- where applicable, the consideration and verification of the information of the future CM and the IT server, as well as their reporting entity and the creation of the corresponding registration file;
- the preparation and transmission of the certificate request to the appropriate PKI function according to the latter's organisation and the available services;
- the archiving of the elements from the registration file (or dispatch to the component in charge of archiving);

- the retention and protection, in full confidentiality and integrity, of the beneficiary's authentication personal data or, if relevant, that of the CAG, including during exchanges of such data with the other PKI functions (it notably complies with the legislation relative to the protection of personal data).

Only the Certinomis RA has the ability to validate an internet domain name (FQDN) with a view to issuing an SSL/TLS server certificate publicly recognised in the root authority program of internet browser publishers (in particular those members of the CAB Forum http://www.cabforum.org/forum.html). This validation function may not under any circumstances be delegated to a third party. This function is performed by the validation specialist trust role.

1.3.3 Certificate Manager

In the context of this CP, a CM is a natural person who is responsible for the use of the certificate of the computer server identified in the certificate and the private key corresponding to this certificate, on behalf of the entity also identified in this certificate. The CM has a contractual / hierarchical / regulatory link with this entity.

The CM complies with the conditions incumbent upon him as defined in this CP.

It should be noted that since the certificate is attached to the IT server and not to the CM, the latter may change during the validity of the certificate: departure of the CM from the entity, change of assignment and duties in the entity, etc.

The entity must inform the CA beforehand, except in exceptional cases and in this case without delay, of the departure of a CM from office and appoint a successor. A CA will revoke a server certificate for which there is no longer an explicitly identified CM.

1.3.4 Certificate users

The certificate's user can be:

- An entity or natural person who receives a certificate and who relies on it in order to verify an electronic signature coming from the certificate's beneficiary.
- Server under the responsibility of a natural or legal person, that uses a certificate and signature verification system in order to verify the electronic signature placed on data or a message by the certificate subject. The application implements the security policy and practices determined by the application manager.

Before trusting the said certificate, the third party user must absolutely verify its validity with Certinomis, by checking the most recent appropriate Lists of Revoked Certificates, and while verifying its intrinsic validity, most notably its expiry date and signature, and the validity of any certificate on the trust itinerary. Should this obligation not be met, the third party user assumes all risks for any actions not compliant with the present policy's requirements, with Certinomis therefore no longer guaranteeing the legal value of the certificates that it has issued and that could have been revoked or that might no longer be valid.

1.3.5 Other participants

1.3.5.1 Certification agent

An entity is not required to avail itself of a certification agent (CAG). A given entity can have one or more CAGs.

If it appoints one, the CAG must be formally designated by a legal representative of the entity in question. The CAG is in direct contact with the PKI's RA.

The CAG is a person who, directly by law or by delegation, has the power to authorise a certificate request bearing the organisation's name. This person may also have other powers in the organisation's name, notably for revocation.

In the context of an organisation, a CAG may be appointed to perform the actions necessary for the issuance of a certificate in place of the customers.

By default, the legal representative of the organisation is considered to be CAG.

The CAG must:

- be a natural person duly authorised to act on behalf of an organisation;
- correctly and independently perform the identity controls of the future subjects from the entity for which he is the CAG;
- respect the parties of the CP and CPS of the CA that are incumbent upon him.

The CAG may refer to a data-entry operator. This operator is in charge of entering the data collected within the organisation that the CAG represents. By contract, he undertakes to maintain the strictest confidentiality regarding the data of which he may learn while performing this task.

The CAG signs the data entered by the data entry operator before any transmission to the Registration Authority.

The entity must inform the CA, beforehand if possible but at least as quickly as possible, of the resignation of a CAG from their office while assigning a successor.

1.4 USE OF THE CERTIFICATES

1.4.1 Applicable usage domains

1.4.1.1 Key pairs and issued certificates

The certificates issued in accordance with the present policy are suitable for establishing the link that exists between an identity and a public key.

Some digital exchange applications may require certificates for testing or acceptance purposes. The same requirements must be taken into account for these certificates; no distinction is made between them and "production" certifications.

SSL Server authentication
Usage of the server stamp
System or application that uses an identified entity's certificate in order to • Establish a secure session between two servers.

1.4.1.2 Key pairs and certificates of the CA and components

The CA generates and signs various types of objects: certificates, CRL / LRCC.

The CA uses a key pair in order to sign these objects.

The CA has a single key pair, and the corresponding certificate is attached to a higher level CA (hierarchy of the CA).

The CA's key pairs and certificates are used to sign certificates and CRL / LRCC, and only for this purpose. They are not used for confidentiality or authentication purposes.

1.4.2 Forbidden usage domains

Nothing technically prevents the implementation of applications considered to be forbidden in terms of the criteria listed below. However, anyone undertaking these operations would do so at their sole risk and peril, and would be held solely liable for any consequences.

If a beneficiary uses their certificates outside of the appropriate applications, and most notably in a forbidden application as defined within the terms of the present policy or of the CPS, he does so under their sole liability, and at their entire risks and perils.

If a certificate's third party user relies on this certificate even though the application is forbidden or restricted in terms of the present policy or CPS, he assumes all risks for doing so.

The certificates issued by Certinomis can under no circumstances be used to sign other certificates (for persons or organisations, or for any identified entity). Certinomis would be entitled to seek the civil and criminal liability of any offender.

Under none of the above hypotheses can the CA be held liable in any way.

No one is authorised to use the private key associated with a certificate to sign another certificate or a CRL as a CA.

1.5 MANAGEMENT OF THE CP

The present policy applies to the CAs and to partners, to their managers and personnel, to the certificates issued by the CAs, to the Certificate Revocation Lists issued by the CA, to the customers and beneficiaries of the CAs and to third party users of certificates issued by the CAs.

This policy is reviewed and updated annually.

1.5.1 Entity managing the CP

The present certification policy is under the responsibility of the Certinomis company.

1.5.2 Contact point

Certinomis general manager
45-47, Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine

Telephone: 0810 184 956
Email: ld-politiquecertification@certinomis.fr

1.5.3 Entity determining the compliance of an internal CPS with this CP

The Certinomis Management determines the compliance of the internal CPS with this certification policy, either directly or indirectly by calling on independent experts specialised in the field of security and PKIs.

The management of Certinomis has appointed a compliance officer from among the company's employees, responsible, among other things, for regularly monitoring changes in the requirements of the Cab Forum (BRG and EVCG) of the CCADB and the Chrome Root Store programme.

1.5.4 Internal CPS compliance approval procedures

The CA guarantees the application of the internal CPS with the Certification Policy.

The CA is in charge of managing (updates, revisions) the internal CPS. Any request for an update of the internal CPS follows the established approval process.

A PMA can ask to examine the internal CPS in compliance with the applicable procedures.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Acronyms

The following acronyms are used in the present CP:

- CA Certification Authority
- RA Registration Authority
- PMA Policy Management Authority
- TA Time-stamp Authority
- DN Distinguished Name
- CPS Certification Practice Statement
- ETSI European Telecommunications Standards Institute
- PKI Public Key Infrastructure
- LRCC List of revoked CA Certificates
- CRL Certificate Revocation List
- CAG Certification Agent
- MPIC Multi-Perspective Issuance Corroboration
- OID Object Identifier
- CP Certification Policy
- ECSP Electronic Certification Service Provider
- CM Application Service Certificate Manager
- RSA Rivest Shamir Adelman
- PS Publication Service
- ISS Information Systems Security
- URL Uniform Resource Locator

1.6.2 Definitions

Certification Authority (CA):

Within an ECSP, a Certification Authority looks after, in the name and under the responsibility of this ECSP, the application of at least one Certification Policy and is therefore identified as the issuer (certificate's "issuer" field), in the certificates issued pursuant to this certification policy. As part of this CP, the term ECSP is not used elsewhere than in the present chapter and chapter 1.1, while only the term CA is used. It refers to the CA in charge of the certification policy's application, in response to the requirements of the present CP, within the ECSP wishing to qualify the corresponding family of certificates.

Registration authority (RA): Cf. chapter 1.3.1.

Policy Management Authority (PMA):

For the uses that relate to it, the Policy Management Authority determines the security-related needs and requirements in the overall process for the certification and usage of the certificates. It determines the guidelines, possibly in the form of a Certification Policy framework, that must be respected by all of the Certification Authorities

that it accredits. It validates and monitors any change to the certification policies of the Certification Authorities that it accredits.

It plays the role of a moral authority, and its accreditation indicates the trust that one can put in a Certification Authority.

Certificate:

Electronic attestation that links the data related to the encryption or verification of signatures, exchanges, messages and electronic documents to a subject, in order to ensure their confidentiality or to ensure their authentication and integrity.

Topic:

Identities contained within the certificate. The topic can contain the identity of a person, server or organisation.

Beneficiary:

Natural person identified by the RA, who is responsible for the certificates delivered to him. The beneficiary may be the bearer or the CM.

Subject:

Natural person in possession of a certificate in which he is the subject. The subject is the beneficiary of their own certificate.

System or application (also known as the Server):

Hardware or software that can use certificates in order to automatically establish its own security context. For example, a Web server or router uses a certificate in order to authenticate itself during exchanges.

Certification Policy (CP):

Set of rules identified by a name (OID), that defines the requirements with which a CA must comply when setting up and providing its services, and that indicates a certificate's applicability to a specific community and/or to a class of applications having common security requirements. If necessary, a CP can also identify the obligations and requirements weighing on the other participants, notably the beneficiaries and users of certificates.

Internal Certification Practice Statement (Internal CPS):

An internal CPS identifies the practices (organisation, operational procedures, technical and human means) applied by the CA as part of providing its electronic certification services to users, in compliance with the certification policy or policies that it undertakes to respect.

Electronic Certification Service Provider (ECSP):

Any person or entity that is responsible for the management of electronic certificates throughout their life cycle, vis-à-vis the beneficiaries and users of these certificates. An ECSP can provide various families of certificates corresponding with different purposes and/or different security levels. An ECSP has at least one CA, but can have several based on its organisation. An ECSP's various CAs can be independent of one another and or linked by hierarchical or other links (Root CAs / Daughter CAs). An ECSP is identified in a certificate for which it is responsible through its CA that issued this certificate, which is itself directly identified in the certificate's "issuer" field.

2 RESPONSIBILITIES REGARDING THE PROVISION OF INFORMATION HAVING TO BE PUBLISHED

2.1 ENTITIES IN CHARGE OF PROVIDING INFORMATION

The CA's publication function provides information on the status of certificates by means of the "CRL" files and an OCSP responder.

The access points for the LRCCs and the CRLs are specified in chapter 7 of this PC.

The access point of the OCSP responder is specified in chapter 7 of this CP.

The CRLs and LRCCs are also accessible for download, directly on the public WEB server:
www.certinomis.fr in the heading "Documents and links / Our revocation lists".

The time required to issue and publish the CRL may cause a temporary discrepancy between a certificate's revocation status in the CA's CRL and that reported by the OCSP responder.
In such a case, the OCSP response should take precedence; a maximum delay of one hour should be expected between that response and the publication of a new CRL containing the same information.

2.2 INFORMATION HAVING TO BE PUBLISHED

The CA is required to publish at least the following information for CMs and certificate users:

- its certification policy;
- its certification practice statement;
- the status of the certificates issued by the CA;
    - the valid certificates of the CA;
    - if the CA is attached to a CA hierarchy, the valid certificates of the CAs in this hierarchy and the various corresponding certification policies, up to the Root CA;
    - for self-signed CA certificates (Root CA), the information allowing certificate users to verify the origin of these certificates (see chapter VI.1.4) and their status (see chapter IV.10);
- the forms necessary for the management of the certificates (registration request, revocation request, etc.).

The Certification Policy, the CA's certificates, the certificate request forms, the contracts and general terms and conditions under which the certificates are issued, are either available on the CA's website at the following address http://www.certinomis.fr, or communicated as part of the commercial negotiation.
A copy can also be obtained by e-mail.

For the clauses applicable to TLS/SSL server offers, Certinomis complies with the current version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (BR) published on the website http://www.cabforum.org. In case of inconsistency between this document and the CABForum BR requirements, the CABForum BR requirements shall apply.

For the clauses applicable to TSL/SSL EV server offers, Certinomis complies with the current version of the "Guidelines for the Issuance and Management of Extended Validation Certificates" (EVCG) published on the website http://www.cabforum.org. In case of inconsistency between this document and the EVCG requirements of the CABForum, the EVCG requirements of the CABForum are applicable

In addition, given the complexity of reading a CP for subjects or users of certificates who are not specialists in the field, the CA also publishes general terms and conditions of use on its website http://www.certinomis.fr in the section: “Documents and links / Our general usage terms”.

The Certificate Revocation List is provided by the CA that ensures its publication on its public site, within the limits of the elements authorised by its customers and beneficiaries.

2.3 PUBLICATION TIMEFRAMES AND FREQUENCIES

The information related to the PKI (new version of the CP, forms, etc.) must be published as soon as necessary so that the consistency between the information published and the actual commitments, resources and procedures of the CA is ensured at all times. In particular, any new version must be communicated to the CM or CAG at the time of a key renewal request and must be the subject of a new agreement. Systems publishing this information must be available at least on working days.

CA certificates must be distributed prior to any distribution of corresponding application service certificates and/or CRLs and the systems publishing them must have 24/7 availability.

The deadlines and frequencies for publication of certificate status information as well as the availability requirements of the systems publishing them are described in chapters IV.9 and IV.10.

It should be noted that a loss of integrity in the information made available (the presence of the information and the integrity of its content) is considered to render that information unavailable.

The Certification Policy must be updated on the CCADB website within 7 (seven) days of its coming into effect.

2.4 PUBLISHED INFORMATION ACCESS CONTROL

All information published for the intention of certificate users can be freely accessed in read-only mode.

Edit access to publication systems (addition, deletion, modification of published information) must be strictly limited to authorised internal functions of the PKI, at least via long-password access control based on a strict password management policy.

3 IDENTIFICATION AND AUTHENTICATION

This chapter defines the requirements in terms of the registration of the certificate request, i.e. of the customers, beneficiaries and identified entities. It also defines the verification requirements in terms of powers, representation and mandates.

3.1 NAMING

3.1.1 Types of names

The names used must comply with the specifications of standard [X.500].

In each certificate compliant with standard [X.509], the issuing CA (issuer) and the server authentication service (subject) are identified by a Distinguished Name (DN) meeting the requirements of standard [X.501].

3.1.2 Necessary usage of explicit names

The names chosen to designate the application services in the certificates must be explicit.

The format of the DN is specified in chapter 7.1.2.2 of this CP.

The CA defines its naming policy and, as such, it reserves the right to make all decisions regarding the names of persons or organisations, whether operating under public law or private law, and for all other entities identified within the framework of the signed certificates. A party requesting a certificate must be able to prove that it has the right to use a particular name.

A party requesting a certificate must have the right to use the name that it wishes to have included therein.

3.1.3 Pseudonymisation of identities

The certificates described in the present CP can under no circumstances be anonymous.

The entity's identifier in its certificate cannot be a pseudonym.

3.1.4 Rules for interpreting the various types of names

Not applicable.

3.1.5 Uniqueness of the names

The distinctive names are unique for all identified entities of a CA. Thus, the DN of the beneficiary certificates contains a specific field (serialNumber) composed of numbers separated by a dash in order to guarantee the uniqueness of the distinctive name.

For DVCP certificates, the serialNumber field is not present.

3.1.6 Identification, authentication and roles of registered trademarks

The right to use a name that is a trade mark for goods, trade or services (trade name, sign, company name) within the meaning of Articles L. 711-1 et seq. of the French Intellectual Property Code (codified by law no. 92-957 of 1

July 1992 and its subsequent amendments) belongs to the legitimate holder of this trademark, trade or service mark, or of this distinctive sign, or to its licensees or assignees.

The CA cannot be held liable in case of the unlawful usage by its customers and beneficiaries of registered trademarks, well-known marks and distinctive signs, or of domain names.

3.2 INITIAL IDENTITY VALIDATION

The RA must verify the identification of the organisation, its legal representative and any persons designated by the latter, directly or indirectly, to represent it vis-à-vis the CA or the RA. The legal representative and these persons, who it will have designated by giving the scope of their mandate, are the certification agents.

In the absence of designation, the legal representative is the sole certification agent.

At the time of registration, the organisation must provide proof of its existence, of its legal representative's identity and of the chain of mandates providing the certification agents with their powers.

The supporting documents used to prove these elements must not be older than 398 days in the context of a request for EVCP certificates (in accordance with EVCG chapter 3.2.2.14.3).

The RA must archive all relevant information regarding this registration.

General
The certificate request may be sent to the RA in paper, hand-signed format or in electronic format, if possible signed using an advanced electronic signature process.

3.2.1 Method for proving possession of the private key

The CA must not generate server keys; it must verify that the requester is truly in possession of the private key associated with the public key that will be noted in its certificate. This verification must be carried out from a certificate request in PKCS#10 format signed using the said private key.

Certificate requests in PKCS#10 format must use a signature algorithm based on a hash algorithm from the SHA-2 family.

3.2.2 Validation of an institution's identity

Except for DVCP certificates, for which only domain name information (FQDN) is verified, checks on the identity of the organisation are carried out by the RA.

The certificate must always contain the name of the identified entity (except for DVCP certificates) and, where applicable, any additional information allowing its holder to be unambiguously identified.

General (except DVCP)
Verification of the identity of an organisation

The RA must verify that the request contains the following documents:
• An issue authorisation signed and dated within the last 3 months, by a legal representative of the entity or by the certification agent, identifying the future beneficiary subject to whom the certificate must be delivered,
• A certificate request signed and dated within the last 3 months, by the future beneficiary subject,
• The general usage terms signed by the future beneficiary subject.
• EITHER for a company registered in the French trade and companies register
  ○ a K-Bis extract issued by the registry.
  ○ any document certifying the capacity of the signatory of the certificate request
• OR for a French institution listed in the SIRENE directory
  ○ a situation notice in the SIRENE directory justifying the registration number
  ○ a copy of the articles of association / general meeting minutes, or any other currently valid document bearing the signature of the organisation's representatives
  ○ ELECTED REPRESENTATIVES: a copy of the minutes / discussions appointing the Mayor, Chairman, etc. This copy will have to bear your organisation's stamp and the indication "certified true copy of the original".
  ○ APPOINTED REPRESENTATIVES: copy of the official journal or gazette that certifies this appointment (please highlight the line in question, if the page contains a great deal of text).
 	
For companies registered in the French Commercial Register, the RA may, where applicable, obtain by its own means a K-Bis extract issued by the registry.
 	
The RA must keep the documents received for the registration of the beneficiary, examine the documents and documents submitted with reasonable care and verify whether or not they appear to be compliant and valid.

DBA and trade name verification
If the beneficiary identity information must include a DBA or trade name, the RA must verify the applicant's right to use the DBA[2] / trade name by using one of the methods defined in the [BRG] repository in chapter 3.2.2.2.
Country verification
If the "subject:countryName" field is present in the certificate, the RA must verify the association of the country with the beneficiary using one of the methods defined in the [BRG] repository in chapter 3.2.2.3.

[2] The trade name (in English DBA, "doing business as") is an overlay that refers to the official name of your company

Only for QEVCP-w certificates
Verification of the legal existence of an organisation
The RA must verify that the organisation exists and corresponds to the request using official databases. For private organisations, the RA verifies the accuracy and consistency of the following: - Legal existence: the entity is legally recognised, and its status is not “inactive”, “invalid” or “obsolete” - The name of the organisation: the officially registered name is indeed the same as in the request - Registration number: or, if applicable, the date of incorporation or registration of the organisation - The legal representative: name and address of the legal representative For public entities: - Legal existence: the entity is a legally recognised government body, existing in the political subdivision in which it operates - The name of the entity: the registered official name is the same as in the request - Registration number: the date of incorporation or registration of the entity, or the identifier of the legislative act that created the government entity, if applicable. If these elements are not available, the DN will clearly mention that it is a public entity For commercial entities: - Legal existence: the entity carries out a commercial activity under the name submitted in the request - The name of the entity: the registered official name is indeed the same as in the request - Registration number: the registration number, or the date of registration of the entity, if applicable - The legal representative: the identity of the entity’s representative For non-commercial entities: - Legal existence: the entity is legally recognised as an international organisation - The name of the entity: the registered official name is indeed the same as in the request - The registration number: the date of incorporation, or the identifier of the legislative act that created the entity, if applicable. If these elements are not available, the DN will clearly mention that the entity is an international organisation
Verification of the physical existence of the entity
The RA must verify that the physical address provided in the request is used directly or indirectly by the organisation. The RA uses one of the methods defined in the [EVCG] repository in chapter 3.2.2.4.1.
Verification of the entity’s means of communication
The RA must verify an entity’s means of communication using one of the methods defined in chapter 3.2.2.5.2 of the [EVCG] repository.
Verification of the operational existence of the entity
The RA must verify the operational existence of the entity using one of the methods defined in the [EVCG] repository in chapter 3.2.2.6.2.
Entity domain name verification
See chapter 3.2.3.6 of this CP.

3.2.3 Validation of an individual's identity

For any certificate request submitted with regard to affiliation with an organisation, the said request must be signed by the certification agent, and the supporting documents must be sent to Certinomis.

The CA manager must submit any certificate request to the RA. All requests are the subject of a key ceremony script, and a key ceremony report, certificate of the generation of CA keys.

The validation of an individual's identity concerns the following persons:

- Certificate Manager (CM)
- Certification Agent (CAG)
- Legal representative

3.2.3.1 Registration of a CM without A CAG for an application service certificate to be issued

The registration of the future CM representing an entity requires the identification of that entity, the identification of the "natural person" of the future CM, verification of their authorisation to act as the CM for the relevant application service and entity, proof that the server's domain name (FQDN) belongs to the entity, and justification of the existence of an application within the entity.

The identification of the natural person responsible for the system (or CM) is described below.

For OVCP, QNCP-w and QEVCP-w certificates
The RA must verify that the request contains the following documents: • A mandate signed and dated less than 3 months ago by the legal representative authorising the future CM to be responsible for the application service for which the certificate is to be issued. This mandate must be signed by the legal representative of the entity and co-signed by the future CM for acceptance. • A valid official identity document for the future CM, bearing an ID photograph (for example, a national identity card, passport or residence permit). • The email address allowing the CA to contact the CM. The RA must verify the photocopy of at least one valid official identity document of the CM bearing their photo and signature. If the request is submitted electronically, the RA must verify that the documents are signed using an electronic signature process and that the signature is valid at the time of registration. The RA must keep the documents received for the registration of the beneficiary, examine the documents and exhibits submitted with reasonable care and verify whether or not they appear to be compliant and valid. If the registration file is sent in paper format, the RA must verify the photocopy of at least one valid identity document of the future beneficiary or a professional card issued by an administrative authority, bearing an identity photograph (notably national identity card, passport or residence permit). If the registration file is electronic, the RA must verify that it is signed using an electronic signature process that complies with the requirements of the RGS level (*) and that the signature is valid at the time of registration. The RA must keep the documents received for the registration of the beneficiary, examine the documents and documents submitted with reasonable care and verify whether or not they appear to be compliant and valid.

Only for QNCP-w and QEVCP-w certificates
The RA must check either: • Face-to-face, i.e. in the presence of the CM, an original of a valid official identity document of the CM including their photo and signature; • That the CM has provided in their request file an electronic certificate of the identity of the future beneficiary issued by an eID notified at least at the substantial level by a Member State of the European Union and issued in a face-to-face procedure; • The CM's identity verified by a Remote Identity Verification Provider (RIVP) certified by ANSSI. For QEVCP-w certificates, the following must also be checked during the face-to-face meeting: - A personal statement that includes the following information: o Full name o Residential address where he/she may be located o A statement that all the information contained in the certificate request is correct - At least two secondary supporting documents, one of which must be from a financial institution o Acceptable documents of a financial institution ▪ Unexpired credit card ▪ Unexpired debit card ▪ Mortgage statement from a recognised lender dated within the last six months ▪ Bank statement of a regulated financial institution less than six months old o Acceptable non-financial documents ▪ Recent original utility invoices or certificates from a utility company confirming agreement to pay for services at a fixed address ▪ Copy of proof of payment of a lease less than six months old ▪ Certified copy of a court order, such as a divorce certificate, of cancellation documents or adoption documents
Only for DVCP certificates
Only the verification of the identity of the device described in chapter 3.2.3.6 is necessary for DVCP-level certificates

3.2.3.2 Registration of a new CM without a CAG for an already issued certificate

The registration of the new CM (natural person) representing an entity requires the identification of the natural person and verification of their authorisation as representative of the entity to which the application service is attached and as CM for the application service in question.

The identification of the new CM is described in chapter 3.2.3.1.

3.2.3.3 Registration of a Certification Agent

A RA will have to prepare a registration file for a Certification Agent in response to the following needs:

- Usage of the CAG file as a reference for the identification data of the entity of all of the beneficiaries presented by the CAG;
- Provision of a certificate to the CAG so that he can sign the application service certificate registration files of the entity he represents and send them in electronic form.

Identification of the future CAG representing an entity requires, on the one hand, the identification of this entity and, on the other hand, the identification of the natural person.

The entity must be identified in accordance with the terms of article 3.2.2.

General

The RA must verify that the request contains the following documents:
• A mandate designating the CAG, signed and dated within the last 3 months, from the entity's legal representative. This mandate must be signed by the CAG for acceptance, containing:
  • A commitment from the CAG to the CA, that he will correctly and independently perform the verifications of the files of the requesters,
  • A commitment of the CAG to inform the RA of their resignation from the entity,
• A currently valid official identity document for the CAG, that includes an identity photograph (notably national identity card, passport or residence card), that is provided to the RA that retains a copy.
 	
The RA must verify the photocopy of at least one valid official identity document of the CAG, showing the holder's photo and signature.
 	
If the request is submitted electronically, the RA must verify that the documents are signed using an electronic signature process that complies with the requirements of the RGS level (*) and that the signature is verified and valid at the time of registration.
 	
The RA must keep the documents received for the registration of the beneficiary, examine the documents and documents submitted with reasonable care and verify whether or not they appear to be compliant and valid.

Only for QNCP-w and QEVCP-w certificates

The RA must check either:
• Face to face, i.e. in the presence of the CAG, an original valid official identity document of the CAG including their photo and signature;
• That the CAG has provided in their request file an electronic certificate of the identity of the future beneficiary issued by an eID notified at least at a substantial level by a Member State of the European Union and issued in person;
• The identity of the CAG using a Remote Identity Verification Provider (RIVP) certified by ANSSI.
 	
For QEVCP-w certificates, the following must also be checked during the face-to-face meeting:
- A personal statement that includes the following information:
  ○ Full name
  ○ Residential address where he/she may be located
  ○ A statement that all the information contained in the certificate request is correct
- At least two secondary supporting documents, one of which must be from a financial institution
  ○ Acceptable documents of a financial institution
  ▪ Unexpired credit card
  ▪ Unexpired debit card
  ▪ Mortgage statement from a recognised lender dated within the last six months
  ▪ Bank statement of a regulated financial institution less than six months old
  ○ Acceptable non-financial documents
  ▪ Recent original utility invoices or certificates from a utility company confirming agreement to pay for services at a fixed address
  ▪ Copy of proof of payment of a lease less than six months old
  ▪ Certified copy of a court order, such as a divorce certificate, of cancellation documents or adoption documents

3.2.3.4 Registration of a CM via a CAG for the issuance of the certificate

The CM registration file must be submitted to the CAG, which will forward it to the RA. When CM files are sent by the CAG, they must be authenticated by the RA:

- Either by means of an electronic certificate issued by the CA;
- Or in person
- Or by the CAG's initials affixed to the various pages of the request file, completed by their signature on the main pages

General
The RA must verify that the request contains the following documents: • A mandate signed, and dated within the last 3 months, by the CAG authorising the future CM to take responsibility for the application service for which the certificate is to be issued. This mandate must be signed by the CAG and co-signed by the future CM for acceptance. • A valid official identity document for the future CM, bearing an ID photograph (for example, a national identity card, passport or residence permit). • The email address allowing the CA to contact the CM. The RA must verify the photocopy of at least one valid official identity document of the CAG, showing the holder's photo and signature. If the request is submitted electronically, the RA must verify that the documents are signed using an electronic signature process that complies with the requirements of the RGS level (*) and that the signature is verified and valid at the time of registration. The RA must keep the documents received for the registration of the beneficiary, examine the documents and documents submitted with reasonable care and verify whether or not they appear to be compliant and valid.
Only for QNCP-w and QEVCP-w certificates
The CAG must check either: • In person, i.e. in the presence of the CM, the original of a valid official identity document of the CM bearing their photo and signature; • That the CM has provided in their request file an electronic certificate of the identity of the future beneficiary issued by an eID notified at least at a substantial level by a Member State of the European Union and issued face to face; • The CM's identity verified by a Remote Identity Verification Provider (RIVP) certified by ANSSI. For QEVCP-w certificates, the following must also be checked during the face-to-face meeting: - A personal statement that includes the following information: o Full name o Residential address where he/she may be located o A statement that all the information contained in the certificate request is correct - At least two secondary supporting documents, one of which must be from a financial institution o Acceptable documents of a financial institution ▪ Unexpired credit card ▪ Unexpired debit card ▪ Mortgage statement from a recognised lender dated within the last six months ▪ Bank statement of a regulated financial institution less than six months old o Acceptable non-financial documents ▪ Recent original utility invoices or certificates from a utility company confirming agreement to pay for services at a fixed address ▪ Copy of proof of payment of a lease less than six months old ▪ Certified copy of a court order, such as a divorce certificate, of cancellation documents or adoption documents

3.2.3.5 Registration of a new CM for a certificate already issued

Should a CM have to be changed while a server certificate is still valid, the new CM must be registered as such by the CA, as a replacement for the former CM.

The identification of a new CM (natural person) representing an entity requires the identification of the natural person and the verification of their authorisation as representative for the entity to which the server is attached, and as the CM for the server in question. (see chapiter 3.2.3.1).

3.2.3.6 Registration of a system or application

The identification of the future system (or application) representing an entity requires firstly the identification of this entity, and secondly the identification of the natural person in charge and of the system, and finally of the system's identity.

The entity and the person responsible for the system must be identified in accordance with the provisions of article 3.2.3.1 and if the entity designates a CAG in accordance with Article 3.2.3.2.

The RA must verify that the requester is authorised to receive certificates for the system or application. The person or organisation that submits a request must provide proof of its right to use the system or application that will be mentioned in the certificate. In particular in case of a Web server, it must provide proof that the domain name belongs to it.

Verification of the system's identity
The RA must verify that the request contains the following documents: • An issue authorisation signed and dated within the last 3 months, by a legal representative of the entity or by the certification agent, identifying the future CM as being authorised to be the CM for the IT server for which the server certificate is to be delivered. • A certificate application signed and dated within the last 3 months, by the future beneficiary CM and including the identity of the server concerned by this acceptance request. • The general usage terms signed by the future CM. The RA must verify the entity's possession of the domain name corresponding to the FQDN(s) for server authentication certificate requests. The RA must use one of the following validation methods defined in the [BRG]: o 3.2.2.4.7: DNS change The RA must perform a verification of the CAA registrations as defined in RFC 8659 for each domain name present in the "subjectAltName" extension of the certificate to be issued. The RA must document claim rejections due to CAA verification. The use of an IP address in the subjectAltName field extension is prohibited. The use of a domain name ".onion is prohibited. The RA must retain the documents received for registration of the system, examine the documents and exhibits submitted with reasonable care and verify whether or not they appear to be compliant and valid. Each check is performed by corroborating the results of a DNS query obtained from different network perspectives (MPIC).

3.2.4 Unverified information

Not applicable.

3.2.5 Validation of the requester's authority

This step is performed at the same time as a validation of the identity of the natural person (directly by the RA or by the CAG).

3.2.6 Interoperability criteria

No cross-certification is established with other CAs.

3.3 IDENTIFICATION AND VALIDATION OF A KEY RENEWAL REQUEST

The renewal of a certificate's key pair automatically results in the generation and provision of a new certificate. Moreover, a new certificate cannot be provided to the beneficiary without the renewal of the corresponding key pair (cf. chapter 5.6).

3.3.1 Identification and validation for a current renewal

For any renewal request, the initial application procedure applies.

3.3.2 Identification and validation for a renewal after revocation

After a certificate's definitive revocation, for any reason whatsoever, the identification and validation procedure for the renewal request is identical with the initial registration procedure.

3.4 IDENTIFICATION AND VALIDATION OF A REVOCATION REQUEST

The request for revocation of a beneficiary certificate may be made on the Certinomis website by the beneficiary or the authorised representative. The RA must authenticate the request before processing: verification of one or two pieces of basic information about the requester (address, telephone number, etc.) and the requester's authority in relation to the certificate to be revoked.

The request may also be sent by post. It must then be signed by the requester and the service in charge of managing revocations must verify the requester's identity (verification of the handwritten signature in relation to a previously registered signature) and this person's authority relative to the certificate to be revoked.

4 OPERATIONAL REQUIREMENTS ON THE LIFECYCLE OF CERTIFICATES

The present chapter defines the operational practices relative to the management of keys and certificates.

4.1 CERTIFICATE REQUEST

4.1.1 Origin of a certificate request

On its website, the CA publishes all of the procedures and requirements regarding a certificate request. Certificate requesters must comply with the published procedures.

For beneficiaries (CM), a certificate may be requested by a legal representative of the entity or a CAG duly authorised for this entity, with in all cases the prior consent of the future beneficiary.

4.1.2 Process and responsibilities for submitting a certificate request

4.1.2.1 CA certificates

The requests are made by the CA manager, as part of the Key Ceremony.

4.1.2.2 Beneficiary certificates

The electronic identification request sent to the RA must at least contain the requester's email address.

Each request must be associated with elements, also transmitted to the RA, that serve to prove the identity and powers of the future beneficiaries in compliance with the applicable procedures according to the type of requested certificate (articles 3.2.2, 3.2.3 and 3.3), notably:

- the proof of the requester's identity;
- proof of the powers for the requested attributes, for example affiliation with an institution or company, or possession of a domain name;
- the customer contract or the reference to a pre-existing customer contract

For an organisation, for each request, there must be an issuance authorisation signed by an identified certification agent and a customer contract signed by an authorised representative who may not be a certification agent. This contract must mention the beneficiary's information obligations amongst its obligations.

4.2 PROCESSING OF A CERTIFICATE REQUEST

4.2.1 Performance of the identification and request validation processes

A certificate request does not in any way oblige the CA to issue a certificate.
The issuance of a certificate by a CA indicates that the CA has definitively and fully approved the certificate request.

If the certificate request could not be validated after 3 months, it will be cancelled by Certinomis (the supporting documents will have exceeded their validity period of 3 months).

As part of the implementation of the control of CAA-type DNS records, this policy only recognises issuers (CAA issue / issuewild) whose value is "www.certinomis.com" (https://ccadb-public.secure.force.com/mozilla/CAAIdentifiersReport).

The RA then keeps a record of the identity documents presented.

4.2.2 Request acceptance or rejection

Upon receiving a certificate request, the CA must:

- ensure that the request has been properly taken into account by a RA that it has recognised and that the said RA has processed the request and provided an attributable trace of its opinion;
- check that the domain names contained in the request are not internal names (only public FQDNs are authorised for TLS/SSL certificates).
- generate and sign the certificate.

In case of the request's rejection, the RA so informs the beneficiary, and/or the CAG if relevant, while justifying the rejection.

4.2.3 Certificate preparation timeframe

Once the certificate request has been validated, the certificate must be issued as soon as possible.

4.3 DELIVERY OF THE CERTIFICATE

4.3.1 Actions of the CA regarding the delivery of the certificate

After the origin authentication and the verification of the integrity of the request coming from the RA, the CA initiates the process for the generation and preparation of the various elements intended for the beneficiary:

- The beneficiary generates the keys and sends the CSR to the CA.
- The CA generates the certificate.
- The certificate is created in the CA system and assigned a unique number.
- The beneficiary is sent an e-mail containing their self-revocation code.

The conditions for the generation of keys and certificates and the safety measures to be followed are stipulated in chapters 5 and 6 below, notably the separation of the trust roles (cf. chapter 5.2).

4.3.2 Notification by the CA of the certificate's delivery to the CM

The certificate may be sent electronically to an address provided by the holder, or the URL to download the certificate may be sent to such an address.

4.4 ACCEPTANCE OF THE CERTIFICATE

4.4.1 Certificate acceptance procedure

Once the certificate has been transmitted, the beneficiary must verify the content of the certificate. The beneficiary has a period of 15 days following the date of issue of the certificate to express their non-consent to the CA (by

telephone, e-mail or ordinary letter). The first use of the certificate constitutes tacit acceptance of the said certificate. Otherwise, the certificate is tacitly accepted 15 days after issuance.

By accepting a certificate, the beneficiary expressly acknowledges that it consents to the contractual terms and conditions of use and, more generally, to all the elements published in this Certification Policy.

4.4.2 Publication of the certificate

Apart from the pre-certificates recorded in the "Certificate Transparency" logs, the certificates issued are not published by the CA.

4.4.3 CA notification to the other entities of the delivery of the certificate

The CA informs the RA of the issuance of the certificate, and the RA is responsible for informing the CAG if necessary.

4.5 USES OF THE KEY PAIR AND OF THE CERTIFICATE

4.5.1 Use of the private key and the certificate by the CM

The beneficiaries must strictly comply with the authorised uses of the key pairs and certificates. In the opposite case, they could be held liable.

The authorised use of the key pair and the associated certificate is also indicated in the certificate itself, via the extensions concerning the uses of the keys.

The usage of the subject's private key and of the associated certificate is strictly limited to the service defined by the OID of its policy (cf. chapter 1.4.1.1).

4.5.2 Usage of the public key and of the certificate by the certificate user

See the paragraph above and chapter 1.4.

The certificate users must strictly comply with the authorised uses of the certificates. In the opposite case, they could be held liable.

4.6 CERTIFICATE RENEWAL

Note -In compliance with [RFC3647], the notion of "certificate renewal" corresponds with the delivery of a new certificate for which only the validity dates have been modified, with all other information being identical with the previous certificate (including the public key).

The present CP requires the certificates and corresponding key pairs to have the same lifespan, meaning that a certificate cannot be renewed without renewing the key pair.

4.6.1 Circumstance for the renewal of a certificate

Not applicable.

4.6.2 Origin of a renewal request

Not applicable.

4.6.3 Processing a renewal request

Not applicable.

4.6.4 Notification of the issuance of a new certificate

Not applicable.

4.6.5 Terms of acceptance of a new certificate

Not applicable.

4.6.6 Publication of the certificate renewal by the CA

Not applicable.

4.6.7 Notification of issuance by the CA to the other entities

Not applicable.

4.7 DELIVERY OF A NEW CERTIFICATE AFTER CHANGE OF THE KEY PAIR

Note - In accordance with [RFC3647], this chapter deals with the issuance of a new certificate to the beneficiary related to the generation of a new key pair.

4.7.1 Possible causes for changing a key pair

The key pairs must be periodically renewed in order to minimise the possibility of cryptographic attacks. Thus, the server key pairs, and the corresponding certificates, must be renewed at least every 200 days.
The key pairs of the CAs must be renewed at least every 6 years.

Moreover, a key pair and certificate can be renewed early, after the certificate's revocation (cf. chapter 4.9, and notably chapter 4.9.1.1 for the various possible revocation causes).

4.7.2 Origin of a new certificate request

Any application for a certificate shall be considered and treated as an initial request.
See chapter 4.1.1.

4.7.3 Processing procedure for a new certificate request

See chapter 4.2.

4.7.4 Notification for the beneficiary of the preparation of a new certificate

See chapter 4.3.2.

4.7.5 New certificate acceptance initiative

See chapter 4.4.1.

4.7.6 Publication of the new certificate

See chapter 4.4.2.

4.7.7 CA notification to the other entities of the delivery of the new certificate

See chapter 4.4.3.

4.8 CERTIFICATE MODIFICATION

Note - In accordance with [RFC3647], the modification of a certificate corresponds to modifications of information without changing the public key (see chapter 4.7) and other than only the modification of validity dates (see chapter 4.6).

The present CP does not authorise certificate modifications.

4.8.1 Circumstance for the amendment of a certificate

Not applicable.

4.8.2 Origin of a certificate modification request

Not applicable.

4.8.3 Processing a certificate change request

Not applicable.

4.8.4 Notification of the issuance of a new certificate

Not applicable.

4.8.5 Procedure for accepting an amended certificate

Not applicable.

4.8.6 Publication of the certificate modified by the CA

Not applicable.

4.8.7 CA notification to the other entities of the delivery of the certificate

Not applicable.

4.9 REVOCATION AND SUSPENSION OF CERTIFICATES

4.9.1 Possible causes of a revocation

4.9.1.1 Beneficiary certificates

The following circumstances may cause the electronic certificate to be revoked:

- the information concerning the service contained in the certificate is no longer consistent with its identity or intended use in the certificate (e.g. modification of the FQDN), prior to the certificate's normal expiry;
- the CA obtains proof that the validation of the authorisation or control of the domain should not be relied on for any FQDN present in the certificate;
- the CM has not complied with the applicable terms of use of the certificate;
- the CM and/or, as the case may be, the CAG / the entity have not complied with their obligations arising from the CA's CP;
- an error (whether intentional or not) has been detected in the registration file;
- the private key of the application service is suspected of being compromised, is compromised, is lost or is stolen (possibly the associated activation data);
- the CA is informed of a demonstrated or proven method that can easily calculate the private key of the application service on the basis of the certificate's public key;
- the CM or an authorised entity (e.g. legal representative of the entity or CAG) requests the certificate to be revoked (in particular in the event of destruction or alteration of the private key of the application service and/or its support);
- the CM informs the CA that the certificate request has not been authorised and does not grant retroactive authorisation;
- the definitive shutdown of the application service or the cessation of activity of the CM entity to which the application service is attached;
- There is no longer any CM identified for the electronic certificate.

When one of the above circumstances arises and the CA learns of it (having been informed or having obtained the information during one of its verifications, notably during the delivery of a new certificate), the certificate in question must be revoked.

4.9.1.2 Certificates of a PKI component

The following circumstances can bring about the revocation of the certificate of one of the PKI components (including a CA certificate for the generation of certificate, or of CRLs):

- suspicion of compromise, compromise, loss or theft of the component's private key;
- decision to change the PKI component following the detection of a non-compliance of the procedures applied within the component with those announced in the CP or CPS (for example, following a negative qualification or compliance audit);
- cessation of activities of the entity operating the component.

4.9.2 Origin of a revocation request

4.9.2.1 Beneficiary certificates

Only the following can request a certificate's revocation:

- the beneficiary, in charge of the certificate;
- the certification agent or the entity's legal representative;
- the personnel of the issuing CA;
- the personnel of the RA that registered the beneficiary's request.

The beneficiary is informed of the people / entities that can submit a revocation request for his certificate, within the general usage terms and on the Certinomis website.

4.9.2.2 Certificates of a PKI component

The revocation of a CA certificate can only be decided upon by the entity in charge of the CA or by the judicial authorities by means of a legal decision.

The revocation of the other certificates of components is decided upon by the entity in charge of the CA.

4.9.3 Processing procedure for a revocation request

The reasons for a given certificate's revocation are never disclosed to third parties, except with the written approval of the beneficiary or customer.

During the audit and controls to which the CA is subject pursuant to the present certification policy, elements regarding the revocation reasons can be provided, but without being identified and not related to a certificate. In more general terms, these elements can be used for statistical purposes.

4.9.3.1 Revocation of one of the beneficiary's certificates

The CA offers a quick means for accessing, whether electronically or by telephone, the revocation service that will authenticate the request under the conditions contained in chapter 3. This revocation service can be carried out directly by the CA or by a RA recognised by the CA.

The revocation request must contain identification information on the certificate that is to be revoked. The request can also contain a detailed description of the revocation causes, and possibly the reasons behind such causes. The revocation procedure is detailed on this website: https://www.certinomis.fr/revoquer-votre-certificat.

If the procedure to request a certificate's revocation is justified and proceeds correctly, the revocation will be initiated. All of the operations and measures taken by the CA must be logged and saved.

Irrespective of the causes behind the certificate's revocation, the beneficiary must always receive a notification of the revocation of the certificate in question. In case of an organisation, the certification agent can also be notified. This notification must indicate the date when the certificate's revocation takes effect. It can be in the form of an e-mail message.

4.9.3.2 Revocation of a certificate of a PKI component

In the event of revocation of one of the certificates in the certification chain, the CA must inform all the beneficiaries concerned as soon as possible and by any means (and if possible in advance) that their certificates are no longer valid. For this purpose, for example, the PKI can send receipts to the RAs and CAGs. The latter must inform the certificate beneficiaries by explicitly indicating that their certificates are no longer valid since one of the certificates in the certification chain is no longer valid.

The revocation of the CA's certificate is facilitated by the signing of a LRCC by the root certificate authority.

The point of contact identified on the site and the CCADB must be informed immediately in the event of revocation of one of the certificates in the certification chain.

4.9.4 Time limit granted to the CM to make the revocation request

As soon as the beneficiary (or an authorised person) learns that one of the possible revocation causes under his responsibility has occurred, he must forthwith prepare a revocation request.

4.9.5 Timeframe for the CA to process a revocation request

4.9.5.1 Revocation of one of the beneficiary's certificates

By its very nature, a request for revocation must be handled urgently.

The revocation management function must be available 24/7.

This function must have a maximum downtime per service interruption (breakdown or maintenance) of 1 hour and a maximum total downtime per month of 4 hours.

Any request for revocation of a certificate must be processed within a period of less than 24 hours, this period being understood between the receipt of the authenticated revocation request and the provision of the revocation information to users.

If, however, the request for revocation could not be processed within the 24-hour period stipulated above, a new revocation deadline will be calculated based on the circumstances encountered, and the requester will be contacted before the expiry of the stipulated period to inform them of the new exceptional deadline.

4.9.5.2 Revocation of a certificate of a PKI component

A certificate of a PKI component must be revoked as soon as an event described in the possible revocation causes for this type of certificate is detected. The certificate's revocation takes effect when the certificate's serial number is added to the revocation list of the CA that had issued the certificate.

The revocation of one of the CA's signature certificates (signing of certificates, of CRLs / LRCCs) must be performed immediately, particularly if the key has been compromised.

4.9.6 Revocation verification requirements applicable to the certificate users

Before any use of certificates, in particular when said certificates create legal effects, the third party user must check the validity of the certificates on which it intends to rely from Certinomis, by consulting the most recent valid Lists of Revoked Certificates as well as by checking the intrinsic validity of the certificate, in particular its signature, and the validity of the issuer's certificate.

The validity of a CRL is checked by means of verifying its signature as well as the validity of the issuer's certificate.

4.9.7 Frequency of issuance and validity periods of the LRCCs / CRLs

A new LRCC must be issued at least once a year. A new LRCC must be issued following the revocation of a CA certificate.

A new CRL must be issued at least every 24 hours. A new CRL may be issued following the revocation of a beneficiary certificate.

4.9.8 Maximum timeframe for the publication of a LRCC/CRL

A CRL or an LRCC should be published within 30 minutes of its generation.

4.9.9 Availability of an online system for verifying the revocation and status of certificates

An additional publication according to the OCSP protocol is available for beneficiary certificates.

4.9.10 Online verification requirements for the revocation of certificates

See chapter 4.9.6 and 4.9.9 above.

4.9.11 Other available information means regarding revocations

No other means are available.

4.9.12 Specific requirements in case of compromise of the private key

In the event of a proven or suspected compromise of the private signature key of a CA, the CA must immediately notify all the authorities that accredit it.

If the client or beneficiary becomes aware of the actual or suspected compromise of the private key, this entails an obligation to immediately verify the revocation of the associated certificate and to request it as soon as possible if it has not been revoked.

The revocation procedure for a CA must be carried out by a key ceremony.

4.9.13 Possible causes of a suspension

The present CP does not authorise certificate suspensions.

4.9.14 Origin of a suspension request

Not applicable.

4.9.15 Processing procedure for a suspension request

Not applicable.

4.9.16 Limits to a certificate's suspension period

Not applicable.

4.10 CERTIFICATE STATUS INFORMATION FUNCTION

4.10.1 Operational characteristics

The CA must provide certificate users with the information enabling them to verify and validate, prior to its use, the status of a certificate and the entire corresponding certification chain (up to and including the Root CA), i.e. also verify the signatures of the chain's certificates, the signatures guaranteeing the origin and integrity of the CRLs/LRCCs and the status of the Root CA's certificate.

When an CRL/LRCC service is offered, they must be in V2 format.

4.10.2 Availability of the certificate status information function

The certificate status information function must be available 24/7.

This function must have a maximum downtime per service interruption (breakdown or maintenance) of 2 hours and a maximum total downtime per month of 8 hours.

4.10.3 Optional systems

No optional system is available.

4.11 END OF THE RELATIONSHIP BETWEEN THE CM AND THE CA

In the event of the end of the contractual / hierarchical / regulatory relationship between the CA and the entity to which the application service is attached, before the certificate expires, for one reason or another, the certificate must be revoked.

In addition, the CA must revoke a certificate for which there is no longer an explicitly identified CM.

4.12 KEY ESCROW AND RECOVERY

The private keys of the beneficiaries must not be escrowed.

CA's private keys must not be escrowed.

4.12.1 Policy and practices for the recovery of keys by escrow

Not applicable.

4.12.2 Policy and practices for the recovery of session keys by encapsulation

Not applicable.

5 NON-TECHNICAL SECURITY MEASURES

5.1 PHYSICAL SECURITY MEASURES

The technical rooms, which house the means of certification and in particular its private signature key, must be highly protected against intrusions.

The level of protection of the technical rooms is essential in guaranteeing the security of the certification means and their operation.

5.1.1 Geographical location and construction of the sites

The present CP includes no specific requirement regarding the geographical location.

The construction of the sites must comply with the regulations and standards in force and, where applicable, specific requirements in the face of risks such as earthquakes or explosions (proximity to an area of factories or warehouses of chemical products, etc.).

5.1.2 Physical access

In order to avoid any loss, damage and compromise of the PKI's resources and interruption of the CA's services, access to the premises of the various PKI components must be controlled.

Access must be strictly limited to persons authorised to enter the premises and the traceability of access must be ensured. Outside working hours, security must be reinforced by the implementation of physical and logical intrusion detection means.

In order to ensure the availability of the systems, access to the machines must be limited only to persons authorised to perform operations requiring physical access to the machines.

Note - Machines mean all servers, cryptographic boxes, stations and active elements of the network used to implement these functions.

5.1.3 Power supply and air conditioning

The characteristics of the electrical power supply and air conditioning equipment must make it possible to comply with the conditions of use of the PKI equipment as set by their suppliers.

They must also make it possible to comply with the requirements of this CP, as well as the commitments made by the CA in its CPS, in terms of the availability of its functions, in particular the functions of management of revocations and information on the status of certificates.

5.1.4 Vulnerability to water damage

The means of protection against water damage must make it possible to comply with the requirements of the present CP, as well as the commitments made by the CA in its CPS, in terms of the availability of its functions, in particular the functions of management of revocations and information on the status of certificates.

5.1.5 Fire prevention and protection

The fire prevention and firefighting resources must make it possible to comply with the requirements of the present CP, as well as the commitments made by the CA in its CPS, in terms of the availability of its functions, in particular the functions of management of revocations and information on the status of certificates.

5.1.6 Safekeeping of media

As part of the risk analysis, the various information involved in the activities of the PKI must be identified and their security needs defined (confidentiality, integrity and availability).

The CA must maintain an inventory of this information. The CA must put in place measures to avoid the compromise and theft of this information.

The media (paper, hard disk, floppy disk, CD, etc.) corresponding to this information must be managed according to procedures that comply with these security requirements. In particular, they must be handled securely in order to protect the media against damage, theft and unauthorised access.

Management procedures must protect these media against obsolescence and deterioration during which the CA undertakes to retain the information they contain.

5.1.7 Media taken out of service

At their end-of-life, the media must be either destroyed or reinitialised for reuse, depending on the confidentiality level of the corresponding information.

The procedures and means of destruction and reset must comply with this level of confidentiality.

5.1.8 Backups

The components of the PKI in charge of the functions of management of revocations and information on the status of certificates must implement remote backups allowing for the rapid resumption of these functions following the occurrence of a disaster or an event that seriously and sustainably affects the performance of these services (destruction of the site, etc.).

The backed-up information must comply with the same requirements of this CP in terms of protecting the confidentiality and integrity of this information.

5.2 PROCEDURAL SECURITY MEASURES

5.2.1 Trust roles

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

Security Manager - The Security Manager is responsible for implementing the component security policy. They manage the controls on the physical access to the component's system hardware. They are authorised to review the archives and are in charge of analysing the event logs in order to detect any incident, anomaly, attempted compromise, etc.

Application Manager - The application manager is responsible, within the component to which they report, for implementing the certification policy and declaring the PKI's certification practices at the level of the application for which they are responsible. Their responsibility includes all of the functions provided by this application and the corresponding performances.

Registration manager – Responsible for verifying the information required to issue certificates and approve applications for certification.

Revocation Manager – Responsible for managing certificate status changes.

System Engineer - They are in charge of the start-up, configuration and technical maintenance of the component's IT hardware. They provide the technical administration of the component's systems and networks.

Operator - Within a PKI component, on the basis of their 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 Operator - The registration operator combines the functions of registration officer and revocation officer. They are responsible for validating certificate requests and processing revocations of beneficiary certificates.

Validation Specialist – The validation specialist is responsible for performing the verifications required by the [BRG] and [EVCG].

In addition to these trust roles within each PKI component, the CA's trust roles also include the roles of the bearer of the PKI's secret shares: see chapters 6.1 and 6.2.

These bearers of secret shares are responsible for ensuring the confidentiality, integrity and availability of the shares entrusted to them.

5.2.2 Number of persons required per task

Depending on the type of operation undertaken, the number and capacity of the persons that must be present, as participants or witnesses, can be different.

For security reasons, sensitive functions are allocated between several persons. The present CP defines a certain number of requirements regarding this distribution, notably for operations linked to the PKI's cryptographic modules (cf. chapter 6).

The CPS indicates the operations requiring the involvement of several persons, as well as the constraints that these persons must respect.

5.2.3 Identification and authentication for each role

All CA personnel members must have their identity and authorisations verified before:

- their names can be added to the list for accessing the CA's premises; or
- their names can be added to the list of persons authorised to physically access the CA's system.

All persons intervening within the CA's system or that of another PKI component must have their identity and authorisation verified before:

- a certificate can be provided to them in order to carry out their assigned role; or
- a system account can be opened in their name.

Each of these certificates and accounts (except for the CA signature certificate):

- is assigned directly to a person;
- must not be shared;
- must only be used for **authorised** tasks for the assigned role; a control mechanism is in place.

Remote operators intervening within the CA system must be identified by means of strong cryptographic mechanisms.

The CA and the PKI components ensure that all of the verification processes that they use make it possible to supervise all of the activities of all their personnel members who have preferential roles.

5.2.4 Roles requiring a separation of duties

Several roles can be assigned to a given person, provided that this accumulation of duties does not compromise the security of the implemented functions.

With regard to trust roles, the following positions must not be aggregated:

- security manager and system engineer / operator
- controller and any other role
- system engineer and operator
- Revocation manager or registration manager and controller

5.3 SECURITY MEASURES RELATIVE TO THE PERSONNEL

5.3.1 Required qualifications, skills and authorisations

The CA manager must ensure that all members of staff who perform tasks relating to the operation of a CA, whether they report directly to the CA or to the RA:

- are appointed to a position with a detailed and written description;
- are linked by contract or by law to the positions that they occupy;
- have received the necessary training to perform their tasks;
- are bound by contract or by law not to disclose information relating to the security of the CA, the customers or the beneficiaries; the employment contracts of CA personnel members formally include a confidentiality clause;

Identical obligations are incumbent upon the RA, that must inform the CA of the results.

5.3.2 Background verification procedures

Each entity operating a component of the PKI must implement all legal means at its disposal to ensure the integrity of its staff working within the component. In particular, these members of staff must not have a criminal conviction that is incompatible with their duties.

In this respect, the employer may ask these employees to provide a copy of bulletin no. 3 of their criminal record.

The employer may decide, if the employee refuses to provide this copy or if there is a court ruling incompatible with the employee's duties, to withdraw those duties from the employee.

Persons with a trust role must not be affected by conflicts of interest that are detrimental to the impartiality of their duties.

These checks must be conducted prior to being assigned to a trust role and reviewed regularly (at least every 3 years).

5.3.3 Requirements regarded to initial training

Staff must be previously trained in the software, hardware and internal operating and security procedures that they implement and must comply with, corresponding to the component in which they operate.

Personnel must be aware of and understand the implications of the operations for which they are responsible.

5.3.4 Continuing training requirements and frequency

The personnel concerned must receive adequate information and training prior to any changes in the systems, procedures, organisation, etc., depending on their nature.

5.3.5 Rotation frequency and sequence between the various duties

Not applicable.

5.3.6 Penalties in case of unauthorised actions

The sanctions must be specified in the CPS.

5.3.7 Requirements relative to the personnel of external service providers

Staff from external service providers working on the premises and/or on the components of the PKI must also comply with the requirements of this chapter 5.3. This must be translated into adequate clauses in contracts with these service providers.

5.3.8 Documentation provided to the personnel

Each staff member must have at least adequate documentation regarding the specific operational procedures and tools they implement and the general policies and practices of the component in which they work. In particular, the security policy(ies) that affect it must be provided to it.

5.4 AUDIT DATA ESTABLISHMENT PROCEDURES

The logging of events involves making a record of these events, either manually or electronically by means of input or automatic generation.

The resulting files, in paper or electronic form, make it possible to trace and attribute the operations carried out.

5.4.1 Types of events to be logged

With regard to the systems linked to the functions that are implemented within the framework of the PKI, each entity operating a PKI component must at least log the events as described below, in electronic form. Logging must be automatic, from the start of a system and without interruption until the system stops.

- creation / modification / deletion of user accounts (access rights) and of the corresponding authentication data (passwords, certificates, etc.);
- start-up and shutdown of the IT systems and applications;
- events related to the logging: start-up and shutdown of the logging function, modification of the logging parameters, actions taken after a fault involving the logging function;
- connection / disconnection of users having trust roles, and any corresponding unsuccessful attempts.

Other events must also be collected, by electronic or manual means. These concern security and are not automatically produced by IT systems, in particular:

- the physical access points;
- the maintenance activities and changes to system configurations;

- changes to personnel;
- destruction and resetting of media containing confidential information (keys, activation data, personal information on CM, etc.).

In addition to these logging requirements common to all components and functions of the PKI, events specific to the different functions of the PKI must also be logged, in particular:

- receipt of a certificate application (initial and renewal);
- validation / rejection of a certificate request;
- events related to signature keys and CA certificates (generation (key ceremony), backup/recovery, revocation, renewal, destruction, etc.);
- where applicable, generation of the application service's secret elements (key pair, activation codes, etc.);
- generation of application service certificates;transmission of certificates to CMs and, as the case may be, explicit acceptances / rejections by CMs;
- where applicable, delivery of the protection system for the application service to the CM ;
- publication and updating of information related to the CA (CP, CA certificates, general terms and conditions of use, etc.);
- receipt of a request for revocation;
- validation/rejection of a revocation request;
- generation and subsequent publication of CRLs (and possibly delta CRLs) or OCSP requests / responses;

Each record of an event in a log must contain at least the following fields:

- type of event;
- name of the operator or reference of the system triggering the event;
- date and time of the event (the exact time of the significant events of the CA concerning the environment, key management and certificate management must be recorded);
- outcome of the event (failure or success).

The accountability for an action lies with the person, organisation or system that executed it. The name or identifier of the executor must be explicitly indicated in one of the fields of the event log.

In addition, depending on the type of event, each record must also contain the following fields:

- recipient of the transaction;
- name of the requester of the operation or the reference of the system that made the request;
- name(s) of the people present (if this is an operation requiring several people);
- cause of the event;
- any information characterising the event (for example, for the generation of a certificate, the serial number of that certificate).

Logging operations must be carried out during the process.
In the case of manual entry, the entry must be made, subject to exceptions, on the same working day as the event.

The specific events and data to be logged must be documented by the CA.

5.4.2 Processing frequency for event logs

See chapter 5.4.8.

5.4.3 Retention period for events logs

Event logs must be kept on site for at least one (1) month. They must be archived as soon as possible after their generation and at the latest within one (1) month (overlap possible between the on-site retention period and the archiving period).

5.4.4 Protection of the events logs

Logging must be designed and implemented in such a way as to limit the risks of circumvention, modification or destruction of event logs. Integrity control mechanisms must be in place to detect any voluntary or accidental modification of these logs.

Event logs must be protected to ensure availability (against partial or total loss and destruction, whether deliberate or not).

The event dating system must comply with the requirements of chapter VI.8.

The definition of the sensitivity of event logs depends on the nature of the information processed and the profession. It may result in a need for confidentiality protection.

5.4.5 Backup procedure for events logs

Each entity operating a PKI component must implement the required measures to ensure the integrity and availability of event logs for the component in question, in accordance with the requirements of this CP.

5.4.6 Collection system for event logs

Not applicable.

5.4.7 Notification of an event's logging to the person responsible for the event

Not applicable.

5.4.8 Evaluation of vulnerabilities

Each entity operating a PKI component must be able to detect any attempt to violate the integrity of the component in question.

Event logs must be checked once (1) per business day, in order to identify anomalies related to failed attempts.

The logs must be analysed in their entirety at least once every two weeks and as soon as an anomaly is detected.

This analysis will result in a summary in which the important elements are identified, analysed and explained. The summary must show the anomalies and falsifications found.

Furthermore, a reconciliation between the various function event logs that interact with each other (registration authority and generation function, revocation management function and certificate status information function, etc.) must be carried out at least once a month, in order to verify the concordance between dependent events and thus contribute to revealing any anomaly.

5.5 DATA ARCHIVING

5.5.1 Types of data to be archived

Archiving arrangements must also be made by the CA. This archiving must ensure the sustainability of the logs constituted by the various components of the PKI.

It must also allow the storage of paper documents related to certification operations, as well as their availability if necessary.

The data to be archived are at least the following:

- software programs (executables) and configuration files for IT hardware;
- the CPs;
- the CPSs;
- general conditions of use;
- the contractual agreements with other CAs;
- the certificates and CRLs as issued or published;
- the receipts or notifications (for informational purposes);
- the signed commitments of the CAGs;
- the proofs of identity of the beneficiaries and, if relevant, of the entity to which they are attached;
- proofs of identity for the application services;
- the event logs of the various PKI entities (in particular the life cycle of the CA certificates and keys).

5.5.2 Retention period of the archives

5.5.2.1 Certificate request files

Any accepted certificate request file must be archived for as long as necessary, and for at least seven (7) years, for the purposes of providing proof of certification in legal proceedings, in accordance with French law.

Where CMs are registered by a registration authority in a country other than that in which the CA is established, the registration authority should apply the regulations of its own country.

When CAGs are also in another country, then the contractual and legal requirements applicable to these CAGs should also be taken into account.

The retention period for registration files must be brought to the attention of the CM or CAG.

During this period of enforceability of the documents, the certificate request file must be made available by the CA upon any request from the authorised authorities.

This file, supplemented by the information recorded by the RA or the CAG, must make it possible to find the real identity of the responsible CM, at a time "t" of the application service designated in the certificate issued by the CA.

5.5.2.2 Certificates, CRLs and OCSP responses issued by the CA

Application-service certificates and CA certificates, as well as CRLs/LRCCs, must be archived for at least five (5) years after their expiry.

OCSP responses produced must be archived for at least three months after their expiration.

5.5.2.3 Event logs

The event logs covered in chapter 5.4 must be archived for ten (10) years from the date of their creation. The measures put in place by the CA for archiving them must provide the same level of security as that envisaged at the time of their creation. In particular, the integrity of records must be ensured throughout their life cycle.

5.5.3 Protection of the archives

For the entire duration of their retention, the archives and their backups must:

- be protected intact;
- be accessible to authorised persons;
- to be re-read and reused

The CA will specify in its internal CPS the means implemented to archive the documents securely.

A copy of all archived or backed up IT materials is protected either solely by physical security measures, or by a combination of physical and cryptographic measures. The archiving site adequately protects the materials against natural dangers, for example excess temperatures, humidity and magnetism.

The CA will verify the integrity of its archives at least every six (6) months.

Moreover, the information retained or saved by the CA can be subject to applicable laws and regulations, pertaining to archiving and retention.

5.5.4 Backup procedure for the archives

The level of protection of backups must be at least equivalent to the level of protection of the archives.

5.5.5 Data time-stamping requirements

Cf. chapter 5.4.4 for the dating of events logs.

Chapter 6.8 presents the requirements with regard to dating / time-stamping.

5.5.6 Archive collection system

The record collection system, whether internal or external, must comply with the requirements for the protection of the archives concerned.

5.5.7 Archive recovery and verification procedures

It must be possible to recover the archives (paper and electronic) within less than two (2) working days, bearing in mind that only the CA can access all the archives (as opposed to an entity operating a PKI component which can only retrieve and consult the archives of the component in question).

5.6 CHANGE OF THE CA'S KEY

The CA cannot generate a certificate having an ending date that is after the expiry date of the CA's corresponding certificate. For this purpose, the validity period of this CA certificate must be longer than that of the certificates it signs.

With regard to the end date of validity of this certificate, its renewal must be requested within a period at least equal to the lifetime of the certificates signed by the corresponding private key.

As soon as a new CA key pair is generated, only the new private key must be used to sign certificates.

The previous certificate can still be used to validate certificates issued using that key, until such time as all of the certificates signed with the corresponding private key have expired.

The certificate cannot be extended beyond its validity date. As such, the issuing of a new certificate will require a renewal of the keys.

5.7 RECOVERY AFTER COMPROMISE AND DISASTER

5.7.1 Procedure for forwarding and handling incidents and compromising

Each entity operating a component of the PKI must implement procedures and means for reporting and processing incidents, in particular through awareness-raising and training of its personnel and through the analysis of the various event logs. These procedures and resources must make it possible to minimise damage due to security incidents and malfunctions.

In the case of a major incident, such as the loss, suspicion of compromise, compromise, theft of the CA's private key, the triggering event is the observation of this incident at the level of the component concerned, which must immediately inform the CA. In the event of a major incident, it must be dealt with immediately upon detection, and, if applicable, information on certificate revocation must be published urgently by any available means (press, website, acknowledgement of receipt, etc.). The CA must also directly and immediately notify the contact point identified on the website https://cyber.gouv.fr.

Any practice that does not comply with the applicable internal CP or CPS must be considered an incident. A major non-compliance in the context of a certification audit must also be considered an incident.

Every incident must be reported and communicated to the appropriate authority.

The incident handling procedure must be specified in the internal CPS.

If one of the algorithms, or associated parameters, used by the CA or its servers becomes insufficient for its remaining intended use, then the CA must:

- inform all CMs and third party users of certificates with which the CA has entered into agreements or other forms of established relationships. In addition, this information must be made available to other certificate users;
- revoke any relevant certificate.

5.7.2 Recovery procedures in case of corruption of IT resources (hardware, software and/or data)

Each component of the PKI must have a business continuity plan to meet the availability requirements of the various PKI functions arising from the RGS Type CP, the CA's commitments in its own CP, particularly with regard to the functions related to the publication and / or revocation of certificates.

This plan must be tested at least once every two years.

In addition, a mass revocation procedure is drafted and tested annually, in order to be carried out if necessary.

5.7.3 Recovery procedures in case of compromise of a component's private key

The compromise of an infrastructure key or a component control key must be addressed in the component's continuity plan (see chapter 5.7.2) as an incident.

In the event of compromise of a CA key, the corresponding certificate must be immediately revoked: see chapter IV.9.

In addition, the CA must at least comply with the following commitments:

- inform the following entities of the compromise: all CMs, CAGs and other entities with which the CA has entered into agreements or has other forms of established relationships, including third party users and other CAs. In addition, this information must be made available to other third-party users;
- Indicate that certificates and revocation status information issued using this CA key may no longer be valid.

5.7.4 Business continuity capacities after a disaster

The various components of the PKI must have the necessary resources to ensure the continuity of their activities in accordance with the requirements of this CP.

5.8 END-OF-LIFE OF THE PKI

One or more components of the PKI may cease their activity or transfer it to another entity for a variety of reasons.

The CA must take the necessary measures to cover the costs to meet these minimum requirements in the event that the CA is bankrupt or for other reasons is unable to cover these costs on its own, as far as possible, depending on the constraints of the applicable bankruptcy legislation.

Transfer of activity is defined as the end of activity of a component of the PKI which does not affect the validity of the certificates issued prior to the transfer in question and the resumption of such activity organised by the CA in collaboration with the new entity.

Cessation of activity is defined as the end of activity of a component of the PKI affecting the validity of the certificates issued prior to the cessation in question.

5.8.1 Transfer of activity or cessation of activity affecting a component of the PKI.

In order to ensure a constant level of confidence during and after such events, the CA must, among other obligations,:

- Put in place procedures whose objective is to ensure a constant service in particular in terms of archiving (in particular, archiving of beneficiary certificates and information relating to certificates);
- Ensure the continuity of the revocation (taking into account a revocation request and publication of the CRLs), in accordance with the availability requirements for its functions defined in the CP.
- In so far as the changes envisaged may have repercussions on commitments vis-à-vis the subjects or users of certificates, the CA informs them thereof as soon as possible within one month;

- The CA must communicate to the contact point identified on the website https://cyber.gouv.fr/, the principles of the action plan implementing the technical and organisational means intended to deal with a cessation of activity or to organise the transfer of activity. It shall in particular present in it the systems put in place in respect of archiving (keys and information relating to the certificates) in order to carry out this function or to have it carried out throughout the period initially provided for in its CP. The CA must communicate to the ANSSI, according to the different components of the PKI concerned, the terms of the changes that have occurred. The CA will measure the impact and make an inventory of the consequences (legal, economic, functional, technical, communication, etc.) of this event. It shall present a plan of action designed to remove, or reduce the risk for the applications and any difficulties for subjects and users of certificates;
- The CA must keep the ANSSI informed of any obstacles or additional delays encountered in the progress of the process.

5.8.2 Cessation of activity affecting the CA

Cessation of activity may be total or partial (for example : cessation of activity for a given family of certificates only). The partial cessation of activity is gradual so that only the obligations referred to below are to be performed by the CA, or a third-party entity that takes over the activities, upon expiry of the last certificate issued by it.

In the event of total cessation of activity, the CA or, in the event of impossibility, any entity that would replace it by the effect of a law, a regulation, a court decision or an agreement previously concluded with this entity, must ensure the revocation of the certificates and the publication of the CRLs in accordance with the commitments made in this CP.

The CA must set out in its practices the measures taken in the event of cessation of service. They must include:

- Notification of the entities affected;
- Transfer of its obligations to other parties;
- Management of the revocation status for unexpired certificates that were issued.

During the cessation of the service, the CA shall:

- Refrain from transmitting the private key that allowed it to issue certificates;
- Take all the measures needed to destroy it or render it inoperative;
- Revoke their certificate;
- Revoke all certificates it has signed and which are still valid;
- Inform (for example by receipt) all CAGs and/or subjects of certificates revoked or to be revoked, as well as their entity to which they are attached, if applicable.

6 TECHNICAL SECURITY MEASURES

The purpose of the present chapter is to define the management provisions for the key pairs of the CA, of the CA's personnel, of the delegated RAs and of the beneficiaries.

6.1 GENERATION AND INSTALLATION OF KEY PAIRS

6.1.1 Generation of key pairs

6.1.1.1 CA keys

The generation of the CA's signature keys must be performed within a secure environment (see chapter 5).

The CA's signature keys must be generated and implemented within a cryptographic module that complies with the requirements of chapter 11 below, with regard to the security level in question.

The generation of the CA's signature keys must be performed under perfectly controlled circumstances, by personnel members within trust roles (see chapter 5.2.1), within the framework of "key ceremonies". These ceremonies must take place according to pre-defined scripts.

The initialisation of the PKI and/or the generation of the CA signature keys can be accompanied by the generation of PKI secret shares. These secret shares are data that are used, after the key ceremony, notably to manage and manipulate the CA's signature private keys, and to be able to subsequently initialise new cryptographic modules using the CA's signature keys.

These secret shares must be generated according to a Shamir threshold diagram (n parts among m are necessary and sufficient to reconstitute the secret). This secret triggers the secure loading, in a new cryptographic module, of the CA private key(s) saved during the key ceremony.

Following their generation, the secret shares must be handed over to holders of secret shares designated in advance and authorised to this trust role by the CA. In whatever form (paper, magnetic medium or confined within a smart card or a USB key), a single bearer cannot hold more than one secret share from a given CA at any one time. Each secret share must be implemented by its bearer.

Key ceremonies must take place under the supervision of at least two persons with trust roles and in the presence of several witnesses, at least one of whom is a qualified auditor within the meaning of the [BRG].

Both objectively and factually, the witnesses confirm the performance of the ceremony relative to the pre-defined scripts.

6.1.1.2 Application service keys generated by the CA

Not applicable.

6.1.1.3 Application service keys generated at service level

When the key pair is generated at the server level, this generation must be carried out in a device meeting the requirements of chapter 12 below. The CA must ensure this with the CM, through a contractual commitment from the server manager to the CA.

Requests for which the key pairs do not correspond to the types and sizes of keys authorised in this CP in chapter 7 must be rejected.

6.1.2 Transmission of the private key to the CM

Not applicable.

6.1.3 Transmission of the public key to the CA

In the event of transmission of the application service certificate request in PKCS10 format, or any other container offering the same security guarantees, to a component of the CA (where the key pair is generated at the application service level), the key must be protected to ensure its integrity and its origin must be authenticated.

6.1.4 Transmission of the CA's public key to the certificate users

The CA's public keys for signature verification must be disseminated to certificate users by a means that ensures their end-to-end integrity and authenticates their origin.

A public CA key can be distributed in a certificate that is either a self-signed root certificate or a certificate attached to a hierarchy from CA to a root CA (see chapter I.4.1.2 above).

A self-signed root certificate does not in itself guarantee that the corresponding public key belongs to the CA in question. Its dissemination must be accompanied by the dissemination, via sources of trust, of the digital fingerprint of the certificate, and possibly the public key, as well as a declaration that it is indeed a public key of the CA.

The CA's public key, as well as the corresponding information (certificate, digital fingerprints, declaration of affiliation) must be easily retrievable by certificate users.

6.1.5 Sizes of the keys

The CA and application service keys must comply with the characteristics requirements specified below:

Root CA keys
Key type: RSA Key size: 4096 bits
Intermediate CA keys
Key type: RSA Key size: 4096 bits
Beneficiary certificate keys
Key type: NIST P-256 Key size: 256 bits or Key type: RSA Key size: minimum 3072 bits

6.1.6 Verification of the generation and quality of the parameters of the key pairs

The key pair generation method must use parameters that comply with the international security standards specific to the algorithm in question. In particular, the parameters of the key pairs must comply with the specifications of document [SOGIS-CRYPTO].

For RSA-type keys, the public exponent must be an odd number greater than 2^{16}. The module size must be at least 3072 bits for a certificate issued on or after 1 January 2026.

For elliptical curve keys, the following curves are permitted: NIST P-256, NIST P-384, NIST P-512.

6.1.7 Key usage objectives

The various possible uses of public keys are defined and therefore limited by the usage of a certificate extension X.509 v.3 (KeyUsage field).

The CA's verification public key is the only key that can be used to verify the signature of certificates.

The use of a CA private key and the associated certificate is strictly limited to the signing of certificates, CRLs/LRCCs and/or OCSP responses (see chapter 1.4.1.2 and 7.1.2).
The use of the private key and the associated issued certificate is strictly limited to the service defined in chapters 1.4.1.1, 4.5 and 7.1.2.

6.2 SECURITY MEASURES FOR THE PROTECTION OF PRIVATE KEYS AND FOR CRYPTOGRAPHIC MODULES

The beneficiary must protect their private keys so that they are not disclosed. they will be responsible for ensuring that special maintenance is carried out on the server used; in particular the stability of the system, the absence of viruses, worms and Trojan horses. He must also select hardware and software that offers efficient security to ensure the protection and usage of his private keys in compliance with the provisions of the present chapter 6.

6.2.1 Security standards and measures for cryptographic modules

6.2.1.1 The CA's cryptographic modules

The cryptographic modules used by the CA for the generation and implementation of its signature keys, as well as, where applicable, for the generation of keys for future certificates, must be cryptographic modules meeting at least the requirements of chapter 11 below.

6.2.1.2 Cryptographic devices of the application service

The usage and protective mechanisms for the private keys of the servers must, for the implementation of their private keys, comply with the requirements of chapter 12 below.

When the cryptographic device is provided by the client, the CA must check with the server manager the compliance of the device implemented by the server, through a clear and explicit contractual commitment from the CM to the CA.

6.2.2 Verification of the private key by several persons

This chapter relates to the verification of the CA's private key for export / import out of / into a cryptographic module. The key pair's generation is covered in chapter 6.1.1.1, the private key's activation in chapter 6.2.8 and its destruction in chapter 6.2.10.
The control of the CA's private signature keys must be ensured by trusted personnel (bearer of PKI secrets) and through a tool implementing secret sharing (systems where n operators among m must authenticate, with n at least 3).

6.2.3 Escrowing of the private key

Neither the CA private keys nor the application services private keys must under any circumstances be escrowed.

6.2.4 Backup copy of the private key

The private keys of application services or of the CA may be backed up.
These copies may be made either in a cryptographic module compliant with the requirements of chapter 11 below, or outside a cryptographic module but in this case in encrypted form and with an integrity control mechanism. The

corresponding encryption mechanism must offer a level of security equivalent to or higher than storage within the cryptographic module and, in particular, be based on an algorithm, a key length and a mode of operation capable of resisting cryptanalysis attacks for at least the lifetime of the key thus protected.

The encryption and decryption operations must be carried out inside the cryptographic module so that the CA's private keys are never in plaintext outside the cryptographic module.

The control of encryption / decryption operations must comply with the requirements of chapter 6.2.2.

6.2.5 Archiving of the private key

The CA's private keys must not be archived under any circumstances.

The private keys of the application services must not under any circumstances be archived by the CA or by any of the components of the PKI.

6.2.6 Transfer of the private key to / from the cryptographic module

6.2.6.1 Private keys of the Authorities:

For CA private keys, all transfers must be made in encrypted form, in accordance with the requirements of chapter 6.2.4.

6.2.6.2 Server private keys

Not applicable.

6.2.7 Primary key storage in a cryptographic module

It is recommended to store the CA private keys in a cryptographic module at least the requirements of chapter 11 below for the security level considered.

However, in the case of backup copies, storage may be carried out outside a cryptographic module subject to compliance with the requirements of chapter 6.2.4.

Regardless of the means used, the CA must ensure that its private keys are not compromised during their storage or transport.

6.2.8 Private key activation method

6.2.8.1 CA private keys

The method for activating the CA private keys in a cryptographic module must meet the requirements defined in chapter 11 for the security level in question.

The activation of the CA private keys in the cryptographic module must be controlled via activation data (see chapter 6.4) and must involve at least two people in trusted roles (for example, security manager and operator).

6.2.8.2 Private keys for application services

Not applicable.

6.2.9 Private key deactivation method

6.2.9.1 CA private keys

The deactivation of CA private keys in a cryptographic module must be automatic as soon as the module environment changes: shutdown or disconnection of the module, disconnection of the operator, etc. A private CA key may also be deactivated after a certain period of inactivity. These deactivation conditions must meet the requirements defined in chapter XI for the security level in question.

6.2.9.2 Private keys for application services

Not applicable.

6.2.10 Destruction method for private keys

6.2.10.1 CA private keys

The method for destroying CA private keys must meet the requirements defined in chapter 11 for the security level in question.

At the end of a CA private key's life, whether normal or premature (revocation), it must be systematically destroyed, along with any copies and any material that would allow it to be reconstructed.

6.2.10.2 Private keys for application services

The destruction of the beneficiaries' private keys is the responsibility of the beneficiary.

6.2.11 Cryptographic module security evaluation level

For CA keys, the evaluation level of the cryptographic module is specified in chapter 11.

The level of evaluation of the cryptographic modules of the application services is specified in chapter 12 below.

6.3 OTHER ASPECTS OF THE MANAGEMENT OF KEY PAIRS

6.3.1 Archiving of public keys

The issuing CA archives or sees to the archiving of all verification public keys in compliance with article 5.5.

6.3.2 Lifespan of the key pairs and certificates

The usage of a particular key length is determined according to the threat and risk evaluation that takes into account the development of attack technologies.

6.3.2.1 Key pairs and CA certificates

The key pair and the Root CA certificate must have a maximum lifespan of 25 years.

The key pairs and certificates of intermediate CAs must have a maximum lifespan of 6 years.

6.3.2.2 Key pairs and beneficiary certificates

The key pairs and certificates of the application services must have a maximum lifespan of 200 days.

6.4 ACTIVATION DATA

6.4.1 Generation and installation of activation data

6.4.1.1 Generation and installation of activation data corresponding with the CA's private key

The generation and installation of the activation data of a cryptographic module of the PKI must be done during the initialisation and customisation phase of this module. If the activation data are not chosen and entered by those responsible for these data themselves, they must be transmitted to them in a way that guarantees their confidentiality and integrity. These activation data must only be known by the managers identified by name in the context of the roles assigned to them (see chapter 5.2.1).

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

Not applicable.

6.4.2 Activation data protection

6.4.2.1 Protection of activation data corresponding with the CA's private key

The activation data generated by the CA for the PKI cryptographic modules must be protected in integrity and confidentiality until it is delivered to its recipient. This recipient is then responsible for ensuring their confidentiality, integrity and availability.

6.4.2.2 Protection of activation data corresponding to the private keys of the application services

Not applicable.

6.4.3 Other aspects related to activation data

Not applicable.

6.5 SECURITY MEASURES FOR IT SYSTEMS

6.5.1 Technical security requirements specific to IT systems

A minimum level of security assurance offered on the PKI's IT systems must be defined in the CA's internal CPS. It must meet at least the following security objectives:

- identification and strong authentication of users for system access (two-factor authentication, physical and/or logical),
- user rights management (enabling implementation of the access-control policy defined by the CA, in particular the principles of least privilege, multiple controls and separation of duties),

- management of user sessions (disconnection after a period of inactivity, access to files controlled by role and user name),
- protection against computer viruses and all forms of compromising or unauthorised software and updates,
- management of user accounts, including the rapid modification and deletion of access rights,
- protection of the network against any intrusion by an unauthorised person,
- protection of the network in order to ensure the confidentiality and integrity of the data passing through it,
- audit functions (non-repudiation and nature of the actions performed),
- if necessary, management of retries on error.

Applications using component services may have additional security requirements.
The protection of confidentiality and integrity of private or secret infrastructure and control keys (see chapter 1.4.1.2) must be subject to specific measures, which may result from the risk analysis.
Monitoring devices (with automatic alarms) and procedures for auditing system settings (in particular routing elements) must be put in place.

The CA must bring its practices into line with the ANSSI documents relating to the protection of the RA application workstation and the CA workstation.

In particular, the CA must apply all the rules defined in the IT hygiene guide published by the ANSSI for the "standard" level.

6.5.2 IT systems security evaluation level

Not applicable.

6.6 SECURITY MEASURES FOR THE SYSTEMS DURING THEIR LIFECYCLE

6.6.1 Security measures linked to the development of the systems

The implementation of a system for implementing the components of the PKI must be documented and must comply, as far as possible, with the modelling and implementation standards. The system configuration of the PKI components as well as any modifications and upgrades must be documented and controlled.
The CA must:

- guarantee that the safety objectives are defined during the specification and design phases,
- use reliable systems and products that are protected against modification.

6.6.2 Measures related to security management

Any significant change to a system or to a component of the PKI must be reported to the CA for validation. It must be documented, included in the internal operating procedures of the relevant component, and comply with the conformity assurance maintenance scheme for evaluated products.

6.6.3 Security evaluation level of the systems lifecycle

Not applicable.

6.7 NETWORK SECURITY MEASURES

Interconnection to public networks must be protected by security gateways configured to accept only the protocols necessary for the operation of the component within the PKI.

The CA must guarantee that the components of the local network (routers, for example) are kept in a physically secure environment and that their configurations are periodically audited in order to verify their compliance with the requirements specified by the CA.

In addition, exchanges between components within the PKI may require the implementation of specific measures depending on the level of sensitivity of the information (use of separate/isolated networks, implementation of cryptographic mechanisms using infrastructure and control keys, etc.).

6.8 TIME-STAMPING / DATING SYSTEM

Several requirements of this CP require the different PKI components to date events related to the PKI's activities (see chapter 5.4).

To date these events, the various components of the PKI may use:

- either a time-stamping authority, internal or external to the PKI, compliant with the requirements of the ETSI EN 319 421 reference;
- or by using the PKI system time by synchronising the clocks of the PKI systems with each other, at least to the nearest minute, and in relation to a reliable source of UTC time, at least to the nearest second. For operations performed offline (e.g. administration of a Root CA), this synchronisation accuracy in relation to the UTC time is not required. However, the system must be able to order events with sufficient precision. For synchronisation with respect to UTC time, it is recommended to refer to a system comprising at least two independent time sources.

7 PROFILES OF THE CERTIFICATES, OCSP AND OF THE CRLS

The content of the certificates and CRLs complies with the requirements of RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

7.1 PROFILE OF CERTIFICATES

7.1.1 CA certificates

7.1.1.1 Root CA

Field	C	Content/Present/Absent
Version	N	3 (0x2)
Serial Number	N	*Random value generated by the CA*
Signature Algorithm	N	Sha256WithRSAEncryption
Issuer DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web Root CA
Subject DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web Root CA
Validity	N	25 years
Subject Public Key Info	N	RSA 4096 bits
Key Usage	O	keyCertSign, cRLSign
Basic Constraints	O	cA=True
Authority Key Identifier	N	*Identifier of the Root CA public key*
Subject Key Identifier	N	*Identifier of the Root CA public key*

7.1.1.2 Intermediary CA

7.1.1.2.1 CA Web G2

Field	C	Content/Present/Absent
Version	N	3 (0x2)
Serial Number	N	*Random value generated by the CA*
Signature Algorithm	N	Sha256WithRSAEncryption
Issuer DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web Root CA
Subject DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web CA G2
Validity	N	6 years maximum
Subject Public Key Info	N	RSA 4096 bits
Key Usage	O	keyCertSign, cRLSign
Basic Constraints	O	cA=True pathLen = 0

Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ac-racine-web-root-ca.cer
Authority Key Identifier	N	*Identifier of the Root CA public key*
Subject Key Identifier	N	*Identifier of the CA's public key*
Certificate Policies	N	Policy = X509v3 AnyPolicy
CRL Distribution Points	N	URI=http://www.certinomis.com/publi/crl/ac-racine-web-root-ca.crl
Extended Key Usage	N	id-kp-serverAuth, id-kp-clientAuth

7.1.1.2.2 Safe CA G2

Field	C	Content/Present/Absent
Version	N	3 (0x2)
Serial Number	N	*Random value generated by the CA*
Signature Algorithm	N	Sha256WithRSAEncryption
Issuer DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web Root CA
Subject DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Safe CA G2
Validity	N	6 years maximum
Subject Public Key Info	N	RSA 4096 bits
Key Usage	O	keyCertSign, cRLSign
Basic Constraints	O	cA=True pathLen = 0
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ac-racine-web-root-ca.cer
Authority Key Identifier	N	*Identifier of the Root CA public key*
Subject Key Identifier	N	*Identifier of the CA's public key*
Certificate Policies	N	Policy = X509v3 AnyPolicy
CRL Distribution Points	N	URI=http://www.certinomis.com/publi/crl/ac-racine-web-root-ca.crl
Extended Key Usage	N	id-kp-serverAuth, id-kp-clientAuth

7.1.1.2.3 CA ACME

Field	C	Content/Present/Absent
Version	N	3 (0x2)
Serial Number	N	*Random value generated by the CA*
Signature Algorithm	N	Sha256WithRSAEncryption
Issuer DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web Root CA
Subject DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – ACME CA

Validity	N	6 years maximum
Subject Public Key Info	N	RSA 4096 bits
Key Usage	O	keyCertSign, cRLSign
Basic Constraints	O	cA=True pathLen = 0
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ac-racine-web-root-ca.cer
Authority Key Identifier	N	*Identifier of the Root CA public key*
Subject Key Identifier	N	*Identifier of the CA's public key*
Certificate Policies	N	Policy = X509v3 AnyPolicy
CRL Distribution Points	N	URI=http://www.certinomis.com/publi/crl/ac-racine-web-root-ca.crl
Extended Key Usage	N	id-kp-serverAuth

7.1.1.2.4 CA Web G3

Field	C	Content/Present/Absent
Version	N	3 (0x2)
Serial Number	N	*Random value generated by the CA*
Signature Algorithm	N	Sha256WithRSAEncryption
Issuer DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web Root CA
Subject DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web CA G3
Validity	N	6 years maximum
Subject Public Key Info	N	RSA 4096 bits
Key Usage	O	keyCertSign, cRLSign
Basic Constraints	O	cA=True pathLen = 0
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ac-racine-web-root-ca.cer
Authority Key Identifier	N	*Identifier of the Root CA public key*
Subject Key Identifier	N	*Identifier of the CA's public key*
Certificate Policies	N	Policy = X509v3 AnyPolicy
CRL Distribution Points	N	URI=http://www.certinomis.com/publi/crl/ac-racine-web-root-ca.crl
Extended Key Usage	N	id-kp-serverAuth

7.1.1.2.5 Safe CA G3

Field	C	Content/Present/Absent
Version	N	3 (0x2)
Serial Number	N	*Random value generated by the CA*

Signature Algorithm	N	Sha256WithRSAEncryption
Issuer DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web Root CA
Subject DN	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Safe CA G3
Validity	N	6 years maximum
Subject Public Key Info	N	RSA 4096 bits
Key Usage	O	keyCertSign, cRLSign
Basic Constraints	O	cA=True pathLen = 0
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ac-racine-web-root-ca.cer
Authority Key Identifier	N	*Identifier of the Root CA public key*
Subject Key Identifier	N	*Identifier of the CA's public key*
Certificate Policies	N	Policy = X509v3 AnyPolicy
CRL Distribution Points	N	URI=http://www.certinomis.com/publi/crl/ac-racine-web-root-ca.crl
Extended Key Usage	N	id-kp-serverAuth

7.1.2 Beneficiary certificates

7.1.2.1 Base fields

The following x509 fields are common to all beneficiary certificates:

Field	C	Content/Present/Absent
Version	N	3 (0x2)
Serial Number	N	*Random value generated by the CA*
Signature Algorithm	N	Sha256WithRSAEncryption
Validity	N	*200 days maximum*
Subject	N	*See 7.1.2.2*
Issuer	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = *Common name of the issuing CA (Certinomis – Safe CA G2 or Certinomis – Safe CA G3 or Certinomis Web CA G2 or Certinomis Web CA G3 or Certinomis ACME CA)*
Subject Public Key Info	N	*Elliptic Curve P-256, RSA 3072 bits, or RSA 4096 bits*
Key Usage	O	digitalSignature and keyEncipherment (QNCP-W)
Authority Key Identifier	N	*Identifier of the issuing CA's public key*
Subject Key Identifier	N	*Identifier of the bearer's public key*
Basic Constraints	O	False
Subject Alternative Name (Address RFC822: DNS)	N	*All FQDNs of the requested and validated domains*
CT Precertificate SCTs	N	*List of SCT entries.*

7.1.2.2 Unique names of bearers

The unique names of the bearers (Subject DN) are defined according to the following table:

	QNCP-w	QEVCP-w	OVCP RGS *	OVCP	DVCP
countryName	Country in which the entity of the bearer is registered				
stateOrProvince	Department for the domiciliation of the bearer's entity				
localityName	Municipality of the bearer entity's domicile				
organizationName	Name or business name of the bearer entity				
commonName	One of the FQDNs present in the SAN extension				
organizationIdentifier	Identifier of the bearer's entity as defined in section 5.1.4 of the ETSI EN 319 412-1 standard.				
serialNumber	Unique number generated by the CA				

In addition to these elements, the DN of the QEVCP-w certificates includes the following fields:

businessCategory	"Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending on the bearer's legal entity type
jurisdictionLocalityName	Municipality with jurisdiction over the bearer entity (if relevant)
jurisdictionStateOrProvinceName	Department of jurisdiction of the bearer entity (if relevant)
jurisdictionCountryName	Country of jurisdiction of the bearer entity

Note: this information is entered by the registration operator
For EV certificates, the cabfOrganizationIdentifier extension will contain the ID of the bearer entity as defined in section 7.1.2.2 of the EVCG

7.1.2.3 Pre-certificates

The Certinomis CA issues pre-certificates prior to the issuance of any bearer certificate. These pre-certificates contain all the fields and extensions that will be present in the final certificate, with the exception of the "CT Precertificate SCTs" extension. The SCT obtained upon publication of the pre-certificate is included in the final certificate in this extension.

7.1.2.4 OID 1.2.250.1.86.2.6.8.62.1 – QNCP-w

Field	C	Content/Present/Absent
Certificate Policies	N	2.23.140.1.2.2 1.2.250.1.86.2.6.8.62.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-safe-g2.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-safe-g2.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/

Extended Key Usage	N	id-kp-serverAuth
Qc Compliance	N	id-etsi-qcs-QcCompliance id-etsi-qcs-QcPDS = https://www.certinomis.fr/documents-et-liens/nos-conditions-generales-dutilisation id-etsi-qcs-QcType = id-etsi-qct-web

7.1.2.5 OID 1.2.250.1.86.2.6.19.62.1 – QNCP-w

Field	C	Content/Present/Absent
Certificate Policies	N	2.23.140.1.2.2 1.2.250.1.86.2.6.19.62.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-safe-g3.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-safe-g3.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth
Qc Compliance	N	id-etsi-qcs-QcCompliance id-etsi-qcs-QcPDS = https://www.certinomis.fr/documents-et-liens/nos-conditions-generales-dutilisation id-etsi-qcs-QcType = id-etsi-qct-web

7.1.2.6 OID 1.2.250.1.86.2.6.8.63.1 – QEVCP-W

Field	C	Content/Present/Absent
Certificate Policies	N	2.23.140.1.1 1.2.250.1.86.2.6.8.63.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-safe-g2.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-safe-g2.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth
Qc Compliance	N	id-etsi-qcs-QcCompliance id-etsi-qcs-QcPDS = https://www.certinomis.fr/documents-et-liens/nos-conditions-generales-dutilisation id-etsi-qcs-QcType = id-etsi-qct-web

7.1.2.7 OID 1.2.250.1.86.2.6.19.63.1 – QEVCP-W

Field	C	Content/Present/Absent
Certificate Policies	N	2.23.140.1.1 1.2.250.1.86.2.6.19.63.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-safe-g3.crl

Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-safe-g3.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth
Qc Compliance	N	id-etsi-qcs-QcCompliance id-etsi-qcs-QcPDS = https://www.certinomis.fr/documents-et-liens/nos-conditions-generales-dutilisation id-etsi-qcs-QcType = id-etsi-qct-web

7.1.2.8 OID 1.2.250.1.86.2.6.7.20.1 – OVCP RGS *

Field	C	Content/Present/Absent
Certificate Policies	N	2.23.140.1.2.2 1.2.250.1.86.2.6.7.20.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-web-g2.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-web-g2.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth

7.1.2.9 OID 1.2.250.1.86.2.6.17.20.1 – OVCP RGS *

Field	C	Content/Present/Absent
Certificate Policies	N	2.23.140.1.2.2 1.2.250.1.86.2.6.17.20.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-acme.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-acme.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth

7.1.2.10 OID 1.2.250.1.86.2.6.18.20.1 – OVCP RGS *

Field	C	Content/Present/Absent
Certificate Policies	N	2.23.140.1.2.2 1.2.250.1.86.2.6.18.20.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-web-g3.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-web-g3.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth

7.1.2.11 OID 1.2.250.1.86.2.6.7.61.1 – OVCP

Field	C	Content/Present/Absent
Certificate Policies	N	2.23.140.1.2.2 1.2.250.1.86.2.6.7.61.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-web-g2.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-web-g2.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth

7.1.2.12 OID 1.2.250.1.86.2.6.17.61.1 – OVCP

Field	C	Content/Present/Absent
Certificate Policies	N	2.23.140.1.2.2 1.2.250.1.86.2.6.17.61.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-acme.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-acme.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth

7.1.2.13 OID 1.2.250.1.86.2.6.18.61.1 – OVCP

Field	C	Content/Present/Absent
Certificate Policies	N	2.23.140.1.2.2 1.2.250.1.86.2.6.18.61.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-web-g3.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-web-g3.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth

7.1.2.14 OID 1.2.250.1.86.2.6.7.60.1 – DVCP

Field	C	Content/Present/Absent
Certificate Policies	N	2.23.140.1.2.1 1.2.250.1.86.2.6.7.60.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-web-g2.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-web-g2.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/

Extended Key Usage	N	id-kp-serverAuth

7.1.2.15 OID 1.2.250.1.86.2.6.17.60.1 – DVCP

Field	C	Content/Present/Absent
Certificate Policies	N	2.23.140.1.2.1 1.2.250.1.86.2.6.17.60.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-acme.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-acme.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth

7.1.2.16 OID 1.2.250.1.86.2.6.18.60.1 – DVCP

Field	C	Content/Present/Absent
Certificate Policies	N	2.23.140.1.2.1 1.2.250.1.86.2.6.18.60.1 CPS = https://www.certinomis.fr/documents-et-liens/nos-politiques
CRL Distribution Points	N	URI = http://www.certinomis.com/crl/ca-web-g3.crl
Authority Information Access	N	CA Issuers = http://www.certinomis.com/publi/cer/ca-web-g3.cer id-ad-ocsp = http://ocsp-pki.certinomis.com/
Extended Key Usage	N	id-kp-serverAuth

7.1.2.17 OCSP Certificates

Field	C	Content/Present/Absent
Version	N	3 (0x2)
Serial Number	N	*Unique number generated by the CA*
Signature Algorithm	N	Sha256WithRSAEncryption
Validity	N	*3 years maximum*
Subject	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = CERTINOMIS - WEB G2 OCSP (or CERTINOMIS – SAFE G2 OCSP, CERTINOMIS – SAFE G3 OCSP or CERTINOMIS – WEB G3 OCSP or CERTINOMIS – ACME OCSP)
Issuer	N	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = *Common name of the issuing CA (Certinomis – Safe CA G2 or KB_OCSP_SAFEG3 or Certinomis Web CA G2 or KB_OCSP_WEBG3 or KB_OCSP_ACME)*
Subject Public Key Info	N	*Elliptic Curve P-256, RSA 3072 bits, or RSA 4096 bits*
Key Usage	O	digitalSignature
Authority Key Identifier	N	*Identifier of the issuing CA's public key*

Subject Key Identifier	N	*Identifier of the certificate's public key*
Basic Constraints	N	False
Subject Alternative Name (Address RFC822: DNS)	N	
Authority Information Access	N	
Extended Key Usage	N	id-kp-OCSPSigning

7.2 PROFILE OF THE CRLS /LRCCS

7.2.1 Profile of the LRCCs

7.2.1.1 Base fields

Field	Content
Version	2 (0x1)
Signature	Sha256WithRSAEncryption
Issuer	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web Root CA
This Update	*Issue date of the* LRCC
Next Update	*Issue date of the next LRCC (maximum one year after the issue date)*
Revoked Certificates	- userCertificate: *unique serial number of the revoked certificate* - revocationDate: *revocation date* - revocationCause: *revocation cause*

7.2.1.2 Extensions

Field	C	Content
Authority Key Identifier	N	*Identifier of the public key of the CA issuing the CRL*
CRL Number	N	*CRL serial number*

7.2.2 Profile of the CRLs

7.2.2.1 AC SAFE G2

7.2.2.1.1 Base fields

Field	Content
Version	2 (0x1)
Signature	Sha256WithRSAEncryption
Issuer	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Safe CA G2
This Update	*Date of issue of the CRL*
Next Update	*Issue date of the next CRl (maximum 7 days after the issue date)*
Revoked Certificates	- userCertificate: *unique serial number of the revoked certificate* - revocationDate: *revocation date* - revocationCause: *cause of the revocation (field present only if the cause of the revocation is one of the following: keyCompromise, privilegeWithdrawn, cessationOfOperation, affiliationChanged, superseded)*

7.2.2.1.2 Extensions

Field	C	Content
Authority Key Identifier	N	*Identifier of the public key of the CA issuing the CRL*
CRL Number	N	*CRL serial number*
ExpiredCertsOnCRL	N	*Date from which revoked and expired certificates are kept in the CRL*

7.2.2.1 AC SAFE G3

7.2.2.1.1 Base fields

Field	Content
Version	2 (0x1)
Signature	Sha256WithRSAEncryption
Issuer	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Safe CA G3
This Update	*Date of issue of the CRL*
Next Update	*Issue date of the next CRl (maximum 7 days after the issue date)*
Revoked Certificates	- userCertificate: *unique serial number of the revoked certificate* - revocationDate: *revocation date* - revocationCause: *cause of the revocation (field present only if the cause of the revocation is one of the following: keyCompromise, privilegeWithdrawn, cessationOfOperation, affiliationChanged, superseded)*

7.2.2.1.2 Extensions

Field	C	Content
Authority Key Identifier	N	*Identifier of the public key of the CA issuing the CRL*
CRL Number	N	*CRL serial number*
ExpiredCertsOnCRL	N	*Date from which revoked and expired certificates are kept in the CRL*

7.2.2.2 WEB CA G2

7.2.2.2.1 Base fields

Field	Content
Version	2 (0x1)
Signature	Sha256WithRSAEncryption
Issuer	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web CA G2
This Update	*Date of issue of the CRL*
Next Update	*Date of issue of the next CRL*
Revoked Certificates	- userCertificate: *unique serial number of the revoked certificate* - revocationDate: *revocation date*

7.2.2.2.2 Extensions

Field	C	Content
Authority Key Identifier	N	*Identifier of the public key of the CA issuing the CRL*
CRL Number	N	*CRL serial number*

7.2.2.1 WEB CA G3

7.2.2.1.1 Base fields

Field	Content
Version	2 (0x1)
Signature	Sha256WithRSAEncryption
Issuer	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – Web CA G3
This Update	*Date of issue of the CRL*
Next Update	*Date of issue of the next CRL*
Revoked Certificates	- userCertificate: *unique serial number of the revoked certificate* - revocationDate: *revocation date*

7.2.2.1.2 Extensions

Field	C	Content
Authority Key Identifier	N	*Identifier of the public key of the CA issuing the CRL*
CRL Number	N	*CRL serial number*

7.2.2.1 CA ACME

7.2.2.1.1 Base fields

Field	Content
Version	2 (0x1)
Signature	Sha256WithRSAEncryption
Issuer	C = FR O = DOCAPOSTE CERTINOMIS OI = NTRFR-433998903 CN = Certinomis – ACME CA
This Update	*Date of issue of the CRL*
Next Update	*Date of issue of the next CRL*
Revoked Certificates	- userCertificate: *unique serial number of the revoked certificate* - revocationDate: *revocation date*

7.2.2.1.2 Extensions

Field	C	Content
Authority Key Identifier	N	*Identifier of the public key of the CA issuing the CRL*
CRL Number	N	*CRL serial number*

7.3 PROFILE OF OCSP RESPONSES

7.3.1 Base fields

Field	Content
OCSP Response Status	*Response code as defined in RFC 6960*
Version	1 (0x0)
Responder Id	*OCSP responder public key ID*
Produced At	*Date the OCSP responder signed the response*
Certificate ID	- Hash Algorithm: sha1 - Issuer Name Hash: *Hash of the DN of the issuing CA* - Issuer Key Hash: *Identifier of the issuing CA's public key* - Serial Number: *Certificate serial number*
Cert Status	*Good, revoked or unknown as defined in RFC 6960*
This Update	*The most recent date on which the answer indicated is known by the respondent to be correct*

Next Update	*Date by which new information on the status of the certificate will be available (between 24 hours and 7 days after the date contained in the "This Update" field)*
Signature Algorithm	sha256WithRSAEncryption or ecdsaWithSHA256

7.3.2 Extensions

Field	C	Content
OCSP Archive Cut-off	N	*Date from which the status of expired and revoked certificates is retained by the responder*
OCSP Nonce	N	*Contains the value of the "Nonce" field if present in the OCSP query*

8 COMPLIANCE AUDIT AND OTHER EVALUATIONS

This chapter only concerns the audits and assessments of the CA's responsibility in order to ensure the proper functioning of its PKI.

8.1 FREQUENCY AND/OR CIRCUMSTANCES OF THE EVALUATIONS

Before the first commissioning of a component of its PKI or following any significant modification within a component, the CA must carry out a compliance check of this component.

The CA must also carry out an annual compliance check of its entire PKI.

8.2 IDENTITIES / QUALIFICATIONS OF THE EVALUATORS

The control of a component must be assigned by the CA to a team of auditors competent in information system security and in the field of activity of the controlled component.

8.3 RELATIONS BETWEEN EVALUATORS AND THE EVALUATED ENTITIES

The audit team cannot be part of the entity that operates the PKI components undergoing the verification, irrespective of this component, and must be duly authorised to perform the intended verifications.

8.4 TOPICS COVERED BY THE EVALUATIONS

The compliance checks relate to a PKI component (isolated verifications) or to the overall PKI architecture (periodic verifications), and are intended to verify the compliance with the commitments and practices defined in the present CP and in the CPS that is in response to it, as well as the resulting elements (operational procedures, implemented resources, etc.).

8.5 ACTIONS TAKEN AFTER THE CONCLUSIONS OF THE EVALUATIONS

At the end of a compliance check, the audit team provides the CA with one of the following opinions:

- “success”,
- “failure”,
- “to be confirmed”.

Depending on the rendered opinion, the consequences of the control are the following:

- In case of failure, and depending on the scope of the non-compliances, the audit team provides the CA with recommendations that can include cessation (temporary or definitive) of the activity, revocation of the component’s certificate, revocation of all certificates issued since the last positive control, etc. The CA decides on the measure to be applied, that must be in compliance with its internal security policies.
- In the event of a "To be confirmed" result, the CA provides the component with an opinion specifying by which time the non-conformities must be repaired. A “Confirmation” control will then serve to verify that all of the critical points have been resolved.
- In case of success, the CA provides the evaluated component with confirmation of its compliance with the requirements of the present CP and the associated CPS.

8.6 COMMUNICATION OF THE RESULTS

The results of the compliance audits are made available to the qualification institution in charge of the CA's qualification.

If the audit report contains information concerning the security of the CA or information that they consider confidential, there will be no publication. A summary or extracts of the report may be obtained in electronic form upon express request.

Compliance audit certificates are made available to the public. A copy may be obtained in electronic form upon express request.

9 OTHER BUSINESS LINE AND LEGAL ISSUES

9.1 RATES

9.1.1 Rates for the delivery or renewal of certificates

Certificate issue fees will be invoiced according to a rate schedule published by the CA on its website, or negotiated as part of a commercial contract.

9.1.2 Rates for accessing the certificates

Certificate access fees can be invoiced by the CA according to a rate schedule that is published or negotiated with the CA.

9.1.3 Rates for accessing information on the status and revocation of certificates

Fees for verifying the validity of certificates can be invoiced by the CA according to a rate schedule published or negotiated with the CA.

Third party users always have access to a free method for verifying the status of certificates (CRL downloaded from the Certinomis website).

9.1.4 Rates for other services

No fees will be charged for direct access to this Certification Policy or the CPS. However, fees can be invoiced for copies on paper or sent by electronic means.

9.1.5 Reimbursement policy

No particular requirement.

9.2 FINANCIAL LIABILITY

9.2.1 Insurance coverage

The guarantee associated with the certificate is limited to the amount indicated in the contract. For any commercial operation or electronic exchange for which the direct or indirect financial consequences are in an amount greater than the anticipated amount, the PKI actors cannot be held liable relative to customers, beneficiaries and third party users.

9.2.2 Other resources

No particular requirement.

9.2.3 Coverage and guarantee regarding the user entities

The certificates guaranteed by the present CP include a guaranteed level of insurance, indicated by contract and accessible to the user party.

9.3 CONFIDENTIALITY OF PERSONAL DATA

9.3.1 Perimeter of the confidential information

The following information is considered to be confidential:

- the private keys of the CA, of the components and of the issued certificates,
- the activation data associated with the private keys of the CA and of the issued certificates[3],
- all of the PKI's secrets
- the event logs of the PKI components,
- the customer's registration file,
- the revocation causes, in the absence of a formal publication agreement.
- Certinomis internal procedures and policies.

9.3.2 Information outside of the perimeter of confidential information

Not applicable.

9.3.3 Responsibilities for the protection of confidential information

The CA is required to apply security procedures to guarantee the confidentiality of the information identified in chapter IX.3.1, in particular with regard to the definitive erasure or destruction of the media used for their storage.

In addition, when this data is exchanged, the CA must guarantee its integrity.

The CA is required to comply with the legislation and regulations in force on French territory. In particular, it may have to make registration files for application-service certificates available to third parties as part of legal proceedings. It must also grant access to this information to the CM and the CAG.

9.4 PROTECTION OF PERSONAL DATA

9.4.1 Personal data protection policy

European Regulation (EU) 2016/679 of 27 April 2016 on the protection of personal data as well as Law No. 78-17 of 6 January 1978 on information technology, files and freedoms amended by Law No. 2004-801 of 6 August 2004 on the protection of natural persons with regard to the processing of personal data applies to all documents held or transmitted by the CA or by one of the components of the PKI (CNIL website http://www.cnil.fr).

In accordance with the law, clients and beneficiaries have the right to access, rectify and oppose the transfer of any information relating to them. This right can be exercised through the agent service, in particular the RA, that had gathered this information, at the address shown on the CA's website.

[3] The confidentiality of the activation data for the private keys of the issued certificates is guaranteed by the CA, as long as they are in its possession.

The CA rigorously complies with all applicable legal requirements and explains on its website the concrete terms of application of the law, particularly in the sections "legal notices & management of personal data".

The Certification Policy complies with the fundamental principles regarding the protection of personal data enshrined in the law, the GDPR and any other international conventions that have entered into force.

9.4.2 Personal data

All data collected and held by the CA or a RA on a natural or legal person (for example: registration procedure, revocation, other recorded events, correspondence exchanged between the beneficiary and the CA or RA, etc.) are considered confidential and may not be disclosed without the beneficiary's prior consent.

Information pertaining to the identification or other personal data of the beneficiary and that is contained in the certificates is considered to be confidential, except if the beneficiary has given its prior formal consent to any disclosure.

The Certificate Revocation Lists only contain the registration numbers and revocation dates of the certificates. The causes of certificate revocation are republished.

9.4.3 Non-personal data

Not applicable.

9.4.4 Responsibility for the protection of personal data

Cf. legislation and regulations in effect within France (notably cf. chapter 10 below)

9.4.5 Notification and consent to use personal data

Cf. legislation and regulations in effect within France (notably cf. chapter 10 below)

9.4.6 Conditions for the disclosure of personal information to legal or administrative authorities

Cf. legislation and regulations in effect within France (notably cf. chapter 10 below)

9.4.7 Other circumstances of disclosure of personal data

French law guarantees the secrecy of correspondence issued using telecommunication means. Any violation is punishable by article 226-15 of the criminal code for violations committed by an individual, and by articles 432-9 and 432-7 of the criminal code for violations committed by a person in a position of public authority.

In general, no employee of the CA and no colleague or subcontractor, as part of their participation in the certification services, has the right to intercept, open, divert, disclose, search for or use the documents submitted to the CA for anything other than the cases included in the present policy, or within the framework of the interception arrangements ordered by judicial authorities or security interceptions pursuant to law n°91-646 of 10 July 1991.

9.5 INTELLECTUAL PROPERTY RIGHTS

All intellectual property rights held by Certinomis are protected by applicable law, regulations and other international conventions. Civil and criminal liability can result from non-compliance with them. For example, in accordance with Law No. 98-536 of 1 July 1998 (Official Journal of 2 July 1998, p.10075) and European Directive 96/6/EC of 11 March 1996, the databases produced by Certinomis are protected. The text of the law can be consulted on the following website: http://www.legifrance.gouv.fr.

9.6 CONTRACTUAL INTERPRETATIONS AND GUARANTEES

This chapter contains the provisions relative to the respective obligations of the CA, of its personnel, of the various entities comprising the PKI, of the customers, the beneficiaries and the third party users. It also contains legal provisions, notably relative to the applicable law and the resolution of disputes.

The obligations common to the components of the PKI are as follows:

- protect and guarantee the integrity and confidentiality of their secret and/or private keys,
- use their cryptographic keys (public, private and/or secret) only for the purposes provided for at the time of their issuance and with the tools specified under the conditions set by the CA's CP and the resulting documents,
- comply with and apply the part of the CPS incumbent on them (this part must be communicated to the corresponding component),
- submit to the compliance checks carried out by the audit team mandated by the CA (see chapter VIII) and the qualification body,
- comply with the agreements or contracts between them or with the CMs,
- document their internal operating procedures,
- implement the (technical and human) resources necessary for the performance of the services to which they are committed under conditions guaranteeing quality and safety.

9.6.1 Certification authorities

The CA is required to:

- Be able to demonstrate to users of its certificates that it has issued a certificate for a given application service and that the corresponding CM has accepted the certificate, in accordance with the requirements of chapter IV.4 above.
- Ensure and maintain consistency between its CPS and its CP.
- Take all reasonable measures to ensure that its CMs are aware of their rights and obligations with regard to the use and management of keys, certificates, or equipment and software used for the purposes of the PKI. The relationship between a CM and the CA is formalised by a contractual / hierarchical / regulatory link specifying the rights and obligations of the parties and, in particular, the guarantees provided by the CA.

The CA is responsible for ensuring that its Certification Policy complies with the requirements in the applicable reference frameworks for the security level in question. The CA assumes any harmful consequences resulting from non-compliance with its CP, by itself or by one of its components. It must make the necessary arrangements to cover its responsibilities related to its operations and/or activities and have the financial stability and resources required to operate in accordance with this policy.

In addition, the CA acknowledges that it is liable in the event of fault or negligence, of itself or of one of its components, regardless of the nature and seriousness thereof, which would result in the unauthorised access, alteration or misappropriation of the personal data of the CM where these data are contained or in transit in the CA's certificate-management applications.

Furthermore, the CA acknowledges that it is responsible for a general duty of supervision, with regard to the security and integrity of the certificates issued by it or one of its components. It is responsible for maintaining the

Docaposte Certinomis SAS with capital of 40,156 euros.
Head office: 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry-sur-Seine. Créteil Trade and Companies
Register B 433 998 903

level of security of the technical infrastructure on which it relies to provide its services. Any changes that impact the security level provided must be approved by the CA's high-level bodies.

9.6.2 Registration service

See the relevant obligations in chapter 9.1.

9.6.2.1 Obligations of the certification agent

The certification agent must comply with all the requirements of the present Certification Policy.

He undertakes to comply with the contract that binds him to the CA.

He guarantees that the information that he provides to the CA or to a RA, for identification of the identified entity or beneficiary, is exact and complete, and that the submitted or presented documents are valid.

The certification agent must prepare and ensure compliance with a security policy for the IT stations that are used in order to implement the certificates.

If he suspects that a private key has been compromised, he must so inform the CA as quickly as possible, and according to the instructions provided by the latter.

He must protect the confidentiality and integrity of his private keys, activation codes or access codes. He must take all reasonable measures in order to avoid any loss, disclosure, compromise, modification or unauthorised usage.

9.6.3 Beneficiary of certificates

The beneficiary must comply with all requirements of the present Certification Policy.

They undertake to comply with the contract that binds them to the CA.

They guarantee that the information that he provides to the CA or to a RA, for their identification, that of the identified entity or beneficiary, are exact and complete, and that the submitted or presented documents are valid.

If the beneficiary is an organisation, it must prepare and ensure compliance with a security policy for the IT stations that are used in order to implement the certificates.
If they suspect that a private key has been compromised, they must so inform the CA as quickly as possible, and according to the instructions provided by the latter.

In no case does the beneficiary acquire ownership of the certificate issued by the CA. They only acquire a usage right. Accordingly, all certificates remain the property of the CA that had issued them.

9.6.4 Certificate users

The user must comply with all requirements of the present Certification Policy. The beneficiary must exclusively use their private keys and certificates for the purposes authorised by this Certification Policy, as well as in compliance with the laws and regulations in force.

They guarantee that the information that they provide to the CA or to a RA, for their identification or that of the identified entity, are exact and complete, and that the submitted or presented documents are valid.

They must protect the confidentiality and integrity of their private keys, activation codes or access codes, in compliance with article 6.2. They must take all reasonable measures in order to avoid any loss, disclosure, compromise, modification or unauthorised usage. They undertake to follow any requirement from the customer with regard to the security policy within the framework of the certificate's usage.

If they suspect that a private key has been compromised, they must so inform the CA as quickly as possible, and according to the instructions provided by the latter.

9.6.5 Other participants

9.6.5.1 Obligations of the third party user

Before any use of certificates, in particular when said certificates create legal effects, the third party user must have reasonable behaviour: check the validity of the certificates on which he intends to rely with Certinomis, by consulting the most recent appropriate Lists of Revoked Certificates, as well as by checking their expiry date and intrinsic validity, in particular their signature, and the validity of any certificate on the trusted route. Should this obligation not be met, the third party user assumes all risks for any actions not compliant with the present policy's requirements, with Certinomis not guaranteeing the legal value of the certificates that it has issued and that could have been revoked or that might no longer be valid.

Moreover, when verifying an electronic signature, the third party user must also verify that the certificate's public key corresponds with the private key of the employed signature.

The third party user must always verify that the certificate is used for relevant purposes and in compliance with the authorised applications.

A third party user must only use the certificates in accordance with the Trust Route validation procedure, which is specified in the X standards. 509 and PKIX and determined by ISO/IEC 9594-8.

9.7 GUARANTEE LIMIT

The issuing of certificates pursuant to the present Certification Policy does not mean that the CA, any one of the PKI components, the CA manager, the CA personnel or the PKI components are in any way a trustee, agent, guarantor or other representative in any way of the beneficiary, of the customer or of any of the other parties in question. Each party undertakes not to assume any commitment on behalf and in the name of the other party, which it can under no circumstances replace.

Accordingly, the beneficiaries, certification agents, customers and third party certificate users are legally and financially independent persons, and therefore do not have any power of representation for the purpose of entering into a binding commitment for the CA or for any PKI component, that is likely to create legal obligations, whether expressly or tacitly, in the name of the CA or of any PKI component. The certification services do not constitute a partnership and do not create any kind of legal association in any legal form that would impose any degree of liability on the basis of the actions or deficiencies of the other party. The contract constitutes neither an association, nor a company or other consortium, nor a mandate given by either of the parties to the other.

The fact that an organisation's name is contained in an electronic signature certificate does not in and of itself constitute a special or general mandate from this organisation in favour of the beneficiary.

The guarantee associated with the certificate is limited to the amount indicated in the contract. For any commercial operation or electronic exchange for which the direct or indirect financial consequences are in an

amount greater than the anticipated amount, the PKI actors cannot be held liable relative to customers, beneficiaries and third party users.

9.8 LIMIT OF LIABILITY

The CA, the CA's personnel, the PKI components, the customers, the beneficiaries and the third party users are responsible for all damages and interest resulting from non-compliance with their respective obligations as defined according to the terms of the present Certification Policy and of the associated CPS.

The CA sets out the perimeter of the liability limits within its CPS.

9.9 COMPENSATION

The parties agree that, in the event of a finding of any liability of one party towards the other, the damages and indemnities for which it is responsible, from all causes combined, shall under no circumstances exceed the liability limits set out in the framework of the contract concluded between the CA and its client.

9.10 DURATION AND EARLY END OF THE VALIDITY OF THE CP

9.10.1 Validity period

The present CP remains in effect until the end-of-life of the last certificate issued pursuant to this CP.

9.10.2 Early end of the validity

Based on the resulting modifications, the publication of a new version of the present CP can result in the need for the CA to update its corresponding CPS.

Based on the nature and scope of the changes made to the CP, the timeframe for coming into compliance will be determined according to the provisions contained in the applicable regulations.

Moreover, re-establishing compliance does not require an early renewal of previously issued certificates, barring exceptional cases related to security.

9.10.3 Effects of the end of validity and clauses remaining in effect

Not applicable.

9.11 INDIVIDUAL NOTIFICATIONS AND COMMUNICATIONS BETWEEN PARTICIPANTS

In case of any change of any kind involving the composition of the PKI, the CA must:

- at the latest one month before the start of the operation, have this change validated by means of a technical expertise, in order to assess the impact on the level of quality and security of the functions of the CA and of its various components.
- at the latest one month after the end of the operation, so inform the qualification institution.

9.12 AMENDMENTS TO THE CP

The present chapter defines the requirements in terms of the administration and management of the present certification policy.

9.12.1 Amendment procedures

The CA must ensure that any proposed modification of its CP remains compliant with the requirements of the RGS-type CP, the applicable ETSI reference documents, the requirements of the [BRG], and any additional documents. In case of a significant change, the CA will call for a technical assessment in order to verify its impact.

9.12.2 Mechanism and information period for amendments

No special requirement.

9.12.3 Circumstances in which the OID must be changed

As the OID of the CA CP is included in the certificates it issues, any evolution of this CP that has a major impact on the already issued certificates (for example, an increase in CM registration requirements, which therefore cannot apply to certificates already issued) must result in an evolution of the OID, so that users can clearly distinguish which certificates correspond to which requirements.

In particular, the OID of the CA CP must change as soon as a major change occurs in the requirements applicable to the certificate family in question.

9.13 PROVISIONS REGARDING THE RESOLUTION OF CONFLICTS

The CA must put in place policies and procedures for the handling of complaints and the resolution of disputes emanating from entities for which it provides trusted electronic services or other related matters.

9.14 COMPETENT JURISDICTIONS

The present certification policy is formally prepared, governed, applied and interpreted according to French laws and regulations, even though the activities resulting from the present Certification Policy may have legal effects that extend beyond the territory of the French Republic.

9.15 COMPLIANCE WITH LAWS AND REGULATIONS

The legislative and regulatory texts applicable to the present CP are notably the ones listed in chapter 10 below. The CA is prohibited from any discriminatory practice.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Overall agreement

Not applicable.

9.16.2 Transfer of activities

Cf. chapter 5.8.

9.16.3 Consequences of an invalid clause

The inapplicability of a provision of the Certification Policy within a given context in no way affects the validity of the other provisions, nor of this provision outside of the said context. The Certification Policy continues to apply in the absence of the inapplicable provision, in keeping with the intentions of the parties.

The headings at the start of each article are intended only to facilitate reading, and can under no circumstances provide a pretext for any interpretation or denaturing of the clauses to which they relate.

9.16.4 Application and waiver

Any notice to be given under this policy shall be deemed to have been given if it is sent by registered letter with acknowledgement of receipt or by fax sent to the address for service indicated at the start of the service contract and shall be deemed to have been received seven (7) days after the date of the postmark in the context of the registered letter with acknowledgement of receipt and one (1) day after the date of sending in the context of the fax.

9.16.5 Force majeure

Initially, force majeure situations will suspend the performance of the contract. If the duration of the force majeure situations is longer than as indicated in the contract, the contract will be automatically terminated, unless agreed otherwise between the parties. The performance of the obligations resumes its normal course once the force majeure situation has ended.

The CA cannot be held liable and assumes no commitment for any delay in the performance of obligations or for any failure to perform obligations pursuant to the present policy when the circumstances resulting in this and that could involve total or partial interruption of its activity, or its disorganisation, fall under the heading of force majeure within the meaning of article 1148 of the Civil Code.

It is formally agreed that the following will constitute cases of force majeure or fortuitous events, in addition to the situations normally accepted by the case law of the French courts and tribunals, of the contractual clauses contained in the associated Declaration of Practices, and any other agreements between the parties (for example the contract):

Total or partial strike, lockout, riot, civil disturbance, insurrection, civil or foreign war, nuclear risk, embargo, confiscation, capture or destruction by any public authority, bad weather, epidemic, blockage of transportation or procurement means for any reason whatsoever, earthquake, fire, storm, flooding, water damage, government or legal restrictions, legal or regulatory modifications to the marketing forms, computer breakdown, blockage of electronic communications, including telecommunication networks, any major scientific discovery that calls into question all or part of the principles of asymmetric cryptography, any consequence of a technological development, that is not anticipated by the CA, and that calls into question the norms and standards of its profession, as well as any case that is independent of the desire of the parties but that would prevent the normal performance of the present contract.

9.17 OTHER PROVISIONS

In accordance with articles 323-1 to 323-7 of the Criminal Code, applicable when an offence is committed within French territory, any hacking or attempted hacking of automated data processing systems will be punishable, which notably includes fraudulent access and remaining within the system, modifications, alterations, data hacking, etc.

The possible penalties vary from 2 to 5 years of imprisonment and a fine ranging from €30,000 to €375,000 for legal persons.

The infringement of trademarks, trade marks and services, designs and models, distinctive signs, copyrights (for example: software, web pages, databases, original texts, etc.) is sanctioned by Articles L. 716-1 et seq. of the Intellectual Property Code.

10 APPENDIX 1: REFERENCED DOCUMENTS

10.1 REGULATIONS

Reference	Document
[CNIL]	*Law n° 78-17 of 6 January 1978 relative to information technology, files and freedoms, modified by n° 2004-801 of 6 August 2004*
[DIRSIG]	*Directive 1999/93/EC of the European Parliament and Council of 13 December 1999, on a community framework for electronic signatures.*
[LCEN]	*Law n° 2004-575 of 21 June 2004 on confidence in the digital economy, notably its article 31 regarding the declaration of the provision of cryptology and its article 33 that stipulates the liability regime for electronic certification service providers that provide qualified electronic certificates.*
[ORDER]	*Order No. 2005-1516 of 8 December 2005 on electronic exchanges between users and administrative authorities and between administrative authorities*
[PSCO_QUALIF]	*Application note, eIDAS Regulation: compliance assessment criteria for qualified trusted service providers, version 1.2 of 05/07/2017.*
[QPSCe]	*Decree of 26 July 2004 relative to the recognition of the qualification of electronic certification service providers and to the accreditation of the institutions performing their assessment*
[DécretRGS]	*Decree in application of articles 9, 10 and 12 of order n° 2005-1516 of 8 December 2005.*
[SIG]	*Decree no. 2001-272 of 30 March 2001 in application of article 1316-4 of the Civil Code and relative to electronic signatures.*
[GDPR]	*European Regulation EU 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*

10.2 TECHNICAL DOCUMENTS

Reference	Document
[RGS]	*General Security Reference System - version 2.0.*
[PROFILS]	*Certificate profiles / CRL / OCSP and Cryptographic Algorithms DT-FL-1310-002-PC-PROFILS*
[RGS_A1]	*RGS – Rules for the implementation of security functions based on the use of electronic certificates – Version 3.0.*
[RGS_A4]	*RGS – Standard Certification Policies – Certificate, CRL and OCSP profiles and cryptographic algorithms – Version 3.0.*
[CWA14167-1]	*CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1*
[CWA14167-2]	*CWA 14167-2 (2003-10) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP). This PP has been certified EAL4+.*
[CWA14167-3]	*CWA 14167-3 (2003-10) Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)*

[CWA14167-4]	*CWA 14167-4 (2003-10) Cryptographic Module for CSP Signing Operations – Protection Profile (CMCSO-PP). This PP has been certified EAL4+.*
[CWA14169]	*CWA 14169 (2002-04) Secure Signature Creation Devices (SSCD). This PP has been certified EAL4+.*
[EN_CP]	*EN 319 411-1 V1.3.1 (May 2021) Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*
[EN_QCP]	*EN 319 411-2 V2.4.1 (November 2021) Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*
[PROG_ACCRED]	*COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – version published at www.cofrac.fr*
[RFC2560]	*IETF - Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol, RFC 2560 - June 1999*
[RFC3647]	*IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - November 2003*
[X.509]	*Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version March 2000 (supplemented by technical corrections No. 1 of October 2001, No. 2 of April 2002 and No. 3 of April 2004)*
[PP_HORO]	*DCSSI - Profil de Protection - Systèmes d'horodatage EAL3+ DCSSI PP 2008/07*
[972-1]	*DCSSI - Technical Guide for the confidentiality of information recorded on hard drives to be recycled or exported – No 972-1/SGDN/DCSSI du 17/07/2003*
[BRG]	*CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates - Current version.*
[EVCG]	*CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates - Current version.*
[SOGIC-CRYPTO]	*SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms - Current version.*

11 APPENDIX 2: SECURITY REQUIREMENTS FOR THE CA'S CRYPTOGRAPHIC MODULE

11.1 REQUIREMENTS REGARDING THE SECURITY OBJECTIVES

The cryptographic module used by the CA to generate and implement its signature keys (for the generation of electronic certificates, CRLs / LRCCs and, possibly, OCSP responses), as well as, if relevant, to generate the key pairs of the issued certificates, must meet the following security requirements:

- if the key pairs of the issued certificates are generated by this module, guaranteeing that these generations are carried out exclusively by authorised users and guaranteeing the cryptographic sturdiness of the generated key pairs;
- if the key pairs of the issued certificates are generated by this module, ensuring the confidentiality of the private keys and the integrity of the private and public keys when they are under the responsibility of the CA and during their transfer to the beneficiary's cryptographic device, and ensuring their secure destruction after this transfer;
- 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 according to the user and role assigned to the latter;
- ability to carry out a series of tests in order to verify that it is running correctly and filling out a report if an error is detected;
- making it possible to create a secure electronic signature in order to sign the certificates generated by the CA, that does not reveal the CA's private keys and that cannot be falsified with 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, guarantee the confidentiality and integrity of the backed-up data and request at least double control of the backup and restoration operations.

The CA's cryptographic module detects attempted physical alterations and fills in a report when an attempted alteration is detected.

11.2 QUALIFICATION REQUIREMENTS

The hardware cryptographic module used for the generation and implementation of CA keys is evaluated according to the Common Criteria at EAL 4+ level, and qualified at the level reinforced by ANSSI.

12 APPENDIX 3: REQUIREMENTS OF THE CRYPTOGRAPHIC DEVICE

12.1 REQUIREMENTS REGARDING THE SECURITY OBJECTIVES

The cryptographic device used by the beneficiary to store and implement its private key and, where applicable, generate its key pair, must meet the following security requirements:

- if the issued certificate's key pair is generated by the system, guaranteeing that this generation is carried out exclusively by authorised users and guaranteeing the cryptographic sturdiness of the generated key pair;
- ensuring the correspondence between the private key and the public key;
- generate a stamp or authentication that cannot be falsified without knowing the private key.

In addition, organisational, procedural or technical security measures must be put in place to:

- detect faults during the initialisation, customisation and operation phases and have secure techniques for destroying the private key in case of regeneration of the private key;
- guaranteeing the private key's confidentiality and integrity;
- making it possible to guarantee the public key's authenticity and integrity when exported outside of the system;
- Ensure, for the legitimate server only, on the one hand, the authentication function and, on the other hand, the decryption function of symmetric session keys, and protect the private key against any use by third parties;
- To guarantee the authenticity and integrity of the session symmetric key, once decrypted, when exported from the device to the data decryption application.

12.2 QUALIFICATION REQUIREMENTS

The CA does not provide the protection device for secret elements, it is recommended to use a device qualified to the reinforced level.