CERTIGNA by tessi

CERTIFICATE POLICY CERTIGNA

Publication :	09/01/22
Version :	1.4
OID :	1.2.250.1.177.1.0.1
Authors :	J. Allemandou
Classification :	Public

tessi

SUMMARY

1 INTRODUCTION

1.1 OVERVIEW

Certigna has a Certification Authority (CA) named “Certigna” to provide certificates to subordinate authorities.

This Certificate Policy (CP) describes the practices that the CA applies and agrees to respect as part of the provision of the digital signature services. The CP also identifies obligations and requirements on certificate users.

The reader's attention is drawn to the fact that the understanding of this CP guess he is familiar with the concepts related to the technology of Public Key Infrastructure (PKI).

This CP meets:

- the requirements of the document « *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* » from CA/BROWSER FORUM conforms to the current version and published at http://www.cabforum.org.
- the applicable requirements of 319 411 and 319 412 ETSI specifications.

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

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

1.2 DOCUMENT NAME AND IDENTIFICATION

This PC can be identified by the name of the « Certigna » and by its OID: 1.2.250.1.177.1.0.1.

Usage(s)	OID
Signature of ARL and intermediate CA certificates Old hierarchy	1.2.250.1.177.1.0.1.1
Signature of ARL and intermediate CA certificates New hierarchy cross signed by Certigna Root CA	1.2.250.1.177.1.0.1.2

1.2.1 Revisions

Ver.	Date	Authors	Document change
1.0	11/03/08	P. MERLIN	Creation
1.1	02/01/19	J. ALLEMANDOU	Revision of the graphic chart and commitments.
1.2	03/30/20	J. ALLEMANDOU	New TESSI graphic charter: Precisions about: - Compliance with 319 412 ETSI specifications (see 1.1, 7), - Possible causes for a certificate's revocation (see 4.9.1), - Retention of application files (see 5.5.2.1, 9.4.1), - Punctual uploading of root CAs for LAR (see 6.2.7), - Reimbursement policy (see 9.1.5), - Insurance coverage (see 9.2.1), - Termination (see 9.6.6), - Delivery and Guarantee (see 9.7), - Limitations of liability (see 9.8), - Dispute resolution procedure (see 9.13), - Renunciation and force majeure (see 9.16).
1.3	09/14/21	J. ALLEMANDOU	Revision of commitments. Update of the graphic charter with new logos
1.4	09/01/2022	J. ALLEMANDOU	Revision of the document and clarifications on: - The commitment to provide non-discriminatory services (see 9.15).

1.3 PKI PARTICIPANTS

1.3.1.1 Certification Authorities

The CA is responsible for the provision of certificate management services throughout their life cycle (generation, distribution, renewal, revocation, ...) and relies on a technical infrastructure: a PKI. The CA is responsible for the implementation of the CP to the PKI set in place.

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

The CA provides these functions directly or outsourcing them, some or all. In all cases, the CA retains responsibility.

CA is committed to respecting the obligations described in this CP.

It is also committed that the components of the PKI, internal or external to the CA, which they incumbent also respect them.

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

1.3.2 Registration Authorities

Registration authority provides the following functions, delegated by the CA under this CP:
- The acquisition and verification of future information of Subject and his entity and the constitution of the corresponding registration files;
- The acquisition and verification of information, if applicable, of the future certification agent (*) and its business entity and the constitution of the corresponding registration files;
- The establishment and transmission of the certificate request to the CA;
- The archiving of the certificate request files;
- Conservation and protection of confidentiality and integrity of the Subject’s or of the Certification Agent’s personal authentication data;
- Verification of certificate revocation requests.

The RA performs these functions directly or with the contribution of Delegate Registration Authorities. In all cases, the RA remains responsible.

Unless stated otherwise, in this document, “RA” covers the Registration Authority and Delegate Registration Authorities.

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

In all cases archiving of the registration files (electronic and / or paper) is the responsibility of the RA.

1.3.3 Subjects

As part of this CP, Certificate Subjects can only be a subordinate CA of Certigna.

1.3.4 Certificate Users

Entity or physical person who use a CA certificate and trust it to verify the origin and the validity of a certificate issued by this CA.

The certificate users must take all precautions described in this CP and in the CGVU.

1.3.5 Other Participants

No stipulation.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

1.4.1.1 Key pairs and certificates of Root CA

The Root CA key pair is used to sign:
- Intermediate CA certificates;
- Authority Revocated lists (ARL).

1.4.1.2 Key Pairs and Certificates for CA and Components

CA has one key pair and the corresponding certificate is linked to a higher-level CA (Root CA).

The key pair of the CA used to sign different types of objects it generates: subject certificates, CA OCSP certificate, LCR.

PKI operators have certificates to authenticate to the PKI. For RA operators (operators of DRA which are not involved), this certificate is used to sign the certificate requests and revocation before transmission to CA. These certificates are issued by a separate PKI, internal to Certigna, whose security level is adapted to that required for the AC.

1.4.2 Prohibited Certificate Uses

Uses other than those mentioned in the previous paragraph are prohibited.

The CA agrees to comply with these restrictions and to enforce compliance by CA and certificate users. To this end, it publishes to the CA and potential users the GCSU that can be found on the site https://www.certigna.fr before any request or use of a certificate.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

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

1.5.2 Contact Person

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

Contact by email: contact@certigna.fr

Phone number: 0 806 115 115 (Free service)

1.5.3 Person Determining CPS Suitability for the Policy

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

1.5.4 CPS approval procedures

The CPS translated into technical terms, organizational and procedural requirements of the CP based on the company's "Information security policy". The Security Committee shall ensure that the means used and described in the CPS meet these requirements as the approval process in place. A compliance check of the CPS compared to the CP is made through the internal and external audits for the CA qualification.

Any update request of the CPS also follows this process.

Any new approved version of the CPS is published without delay.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

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

Agent – Individual acting on behalf of an administrative authority.

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

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

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

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

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

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

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

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

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

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

Protection device secret elements - Refers to a storage device of secret evidence submitted to Subject (e.g. private key, PIN, ...). It can take the form of a smart card, USB key with

cryptographic capability or report to software format (ex. PKCS # 12 file).

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

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

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

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

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

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

Certificate Subject - Person identified in the certificate and is the holder of the private key corresponding to the public key.

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

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

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

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

Qualification of a security product - Act by which ANSSI attests to the ability of a product to ensure with a given level of robustness, security features purpose of qualification. The qualification certificate states in the ability of the product to participate in the realization at some level of security of one or more functions covered in the RGS. The qualification procedure for

security products is described in the decree RGS. The RGS specifies three qualification process: basic level qualification, standard level qualification and level strengthened qualification.

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

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

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

Certificate user - Entity or natural person who uses a certificate which it relies to verify an electronic signature or an authentication value from a certificate holder or encrypt data to a certificate holder.

Note - An agent of an administrative authority which conducts electronic exchange with another administrative authority is, for the latter, a user.

1.6.2 Acronyms

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

AA	Administrative Authority
ANSSI	National Agency for information systems security
ANTS	National Agency for Secure Documents
ARL	Authority Revocation List
BCP	Business Continuity Plan
CA	Certification Authority
CAG	Certification Agent
CGU	Conditions of General Use
CNIL	National Commission for Computing and Liberties
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate revocation list
CSP	Certification Service Provider
CSR	Certificate Signature Request
DN	Distinguished Name
DNS	Domain Name System
DRA	Delegate Registration Authority
ETSI	European Telecommunications Standards Institute
FQDN	Fully Qualified Domain Name
GCSU	General Conditions of Sale and Use
ICD	International Code Designator
INPI	National Institute of Industrial Property
ISS	Information systems security
OC	Certification Operator

OCSP	Online Certificate Status Protocol
OID	Object Identifier
PP	Protection Profile
PAA	Policy Approval Authority
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure
RA	Registration Authority
RSA	Rivest Shamir Adleman
SGMAP	General Secretariat for Modernisation of Public Action
SSL	Secure Sockets Layer
TA	Timestamping Authority
TLS	Transport Layer Security
TSP	Trust Service Provider
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

2.1.1 Entity in Charge of Providing Information

Dhimyotis provides to users and applications using certificates it issues, information about the revocation status of valid certificates issued by the CA. This information is published through several servers:

- http://crl.certigna.fr/certigna.crl
- http://crl.dhimyotis.com/certigna.crl

2.1.2 Information Having to be Published

The CA issues to the CA and certificate users:

- The CP;
- The general Conditions of Sale and Use (GCSU) of CA certification services;
- The various forms required for certificate management (certificate request, revocation request, ...);
- The Root CA certificate and valid intermediate CA certificate;
- The Certificate Revocation List (ARL / CRL);
- The CPS on specific request to Dhimyotis.

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

2.2 PUBLICATION OF INFORMATION

2.2.1 Publication of CP, Terms and Conditions, and Forms

The CP, the GCSU of the CA certification services and the various forms required for certificate management are published in electronic format at https://www.certigna.fr.

The CP is also published at https://www.dhimyotis.com.

2.2.2 Publication of CPS

The CA issues, to the CA and certificate users, the CPS to make possible the assessment of compliance with its certificate policy. Details on its practices are however not made public.

2.2.3 Publication of CA Certificate

The CAs and certificate users can access the CA certificates that are issued at the following addresses:

- https://www.certigna.fr/autorites,
- https://www.dhimyotis.com/autorites.

2.2.4 Publication of CRL

The certificate revocation list is published electronically at the addresses described in Section 2.1 above. These addresses are also indicated in the certificates issued by the CA.

2.2.5 Publication of ARL

The authority revocation list is published electronically at the addresse described in Section 2.1 above. This addresse is also indicated in the certificates issued by the Certigna Root CA.

2.3 TIME OR FREQUENCY OF PUBLICATION

2.3.1 Publication of Documentation

The CP, the Terms and Conditions of CA certification services and the various forms required for certificate management are updated if necessary, aim of securing at any time consistency between published information and commitments, means and procedures of the CA. The publication function based on this information (excluding certificate status information) is available on working days.

2.3.2 Publication of CA Certificates

CA certificates are first broadcast on any broadcasting certificates issued by the CA and corresponding CRL. Availability of systems publishing CA certificates is guaranteed 24/7.

2.3.3 Publication of CRL

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

2.3.4 Publication of ARL

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

2.4 ACCESS CONTROLS ON REPOSITORIES

Access to information published to users is free.

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

2.5 REPORT A MALICIOUS OR DANGEROUS CERTIFICATE

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of names

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

3.1.2 Need for Names To Be Meaningful

The DN format is defined at chapter “7.2 Profile of certificates and CRL” of this CP.

3.1.3 Anonymity or pseudonymity

The CA does not issue certificates with an anonymous identity.

3.1.4 Rules for Interpreting Various Name Forms

No interpretation is made on the name inside the certificates.

3.1.5 Uniqueness of Names

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

3.1.6 Recognition, Authentication, and Role of Trademarks

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

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

CA ensures the detention of the private key during the Key ceremony before certifying the public key.

3.2.2 Authentication of Organization Identity

Cf. chapter 3.2.3

3.2.3 Authentication of individual Identity

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

3.2.4 Non-verified information

No stipulation.

3.2.5 Validation of Authority

This step is performed simultaneously with the validation of the identity of the natural person (directly by the RA or the Certification Agent).

3.2.6 Criteria for Interoperation or Certification

No stipulation.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

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

3.3.1 Identification and Authentication for Routine Re-key

The verification of the Subject’s identity is identical to the original request.

3.3.2 Identification and Authentication for Re-key After Revocation

The verification of the Subject’s identity is identical to the original request.

3.4 Identification and Authentication for Revocation Request

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

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

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

4.1.2 Process and responsibilities for submitting a certificate request

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

4.1.3 Enrollment Process and Responsibilities

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

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

4.2.2 Approval or Rejection of Certificate Applications

No stipulation.

4.2.3 Time to Process Certificate Applications

As from the receipt of the full registration files, the certificate is issued within 30 days.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

Keys pairs of Root CA and intermediate CA are generated during the key ceremony.

4.3.2 Notification of Certificate Issuance

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

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

Root CA and intermediate certificates are published by CA. Cf. chapter 2.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Registration Authority is informed of the generation of the certificate by the CA which is responsible for issuing the certificate generated to the Subject.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subject Private Key and Certificate Usage

Permitted uses of key pairs and certificates described at chapter 1.5.

4.5.2 Relaying Party Public Key and Certificate Usage

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

4.6 CERTIFICATE RENEWAL

The CA does not issue a new certificate for previously issued key pair. Renewal involves the generation of a new key pair and a new certificate request (see section 4.1).

4.6.1 Circumstance for Certificate Renewal

No stipulation.

4.6.2 Who May Request Renewal

No stipulation.

4.6.3 Processing Certificate Renewal Requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstance for Certificate Renewal

The key pairs must be periodically renewed to minimize the possibilities of cryptographic attacks. Thus, the CA key pairs, and corresponding certificates are renewed at least every twenty years (see chapter 6.3.2 validity period).

4.7.2 Who may Request Renewal

The triggering of the provision of a new certificate is initiated by the Certification Authority (no existence of automated process).

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 CERTIFICATE MODIFICATION

The modification of certificates is not recommended.

4.8.1 Circumstance for Certificate Modification

No stipulation.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a CA Certificate

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

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

4.9.1.2 Reasons for Revoking a Certificate of a component of the PKI

The following circumstances may cause the revocation of a certificate of a component of the PKI:

- Suspicion of compromise, compromise, loss or theft of the private key;
- Feature change the PKI decision following the detection of non-compliance of the procedures applied within the component with those announced in this CP (e.g., following an audit qualification or negative Compliance);
- Cessation of activity of the entity operating the component.

4.9.2 Who Can Request Revocation

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

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

4.9.3 Procedure for Revocation Request

In case the CA decides to revoke the intermediate CA certificate (following the compromise of the private key of the CA), the latter informed by email all Subjects that their certificates are no longer valid because one of the certificates in the certificate chain is no longer valid. This information will also be relayed directly from the entities and where appropriate their Certification Agent.

The contact identified on the site of ANSSI (https://www.ssi.gouv.fr) is immediately informed in case of revocation of a certificate of the certificate chain.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time within which CA Must Process the Revocation Request

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

The revocation of the signing CA certificate (signing certificates / CRL / OCSP responses)

is performed immediately, particularly in the case of compromise of the key.

4.9.6 Revocation Checking Requirement for Relying Parties

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

4.9.7 CRL Issuance Frequency

An ARL is issued at every year. In addition, a new CRL is published systematically and immediately after the revocation of a certificate.

4.9.8 Maximum Latency for ARLs

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

4.9.9 On-line Revocation/status Checking Availability

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

OCSP responses are signed by an OCSP Responder whose certificate is signed by the CA that issued the certificate whose revocation status is being checked.

4.9.10 On-line Revocation Checking Requirements

OCSP responders operated by the CA supports the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

The CA must request the certificate revocation promptly after becoming aware of the compromise of the private key. For CA certificates, in addition to the requirements of Section 4.9.3 above, the revocation following a compromise of the private key is being clear information distributed at least on the website of the CA and possibly relayed by other means (other institutional websites, newspapers, etc.).

In case of compromise of its private key or knowledge of the compromise of the private key of the CA that issued the certificate, the Certificates Manager is obligated to immediately and permanently stop the use of the Subject certificate and private key that it is associated. Remember, this commitment is made upon acceptance of the Terms and Conditions.

4.9.13 Circumstances for Suspension

The certificates issued by the CA cannot be suspended.

4.9.14 Who can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 CERTIFICATE STATUS SERVICE

4.10.1 Operational characteristics

The CA provides to certificate users the information needed to verify and validate, prior to their use, the status of their certificates and all the corresponding certificate chain (up to and including Root CA), i.e. to also check the signatures of the certificates in the chain, signatures guaranteeing the origin and integrity of the CRL/LAR and the state of the certificate of Root CA.

The information based on the status of certificates makes available to certificates users a free consultation mechanism CRL/ARL. These CRL/ARL are in CRL V2 format published on the publication website (available with the HTTP protocol).

4.10.2 Service Availability

The information function on the status of certificates is available 24/7. This function has a maximum downtime per outage (failure or maintenance) of 2 hours and a maximum total duration of downtime per month 8 hours.

4.11 END OF SUBSCRIPTION

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

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

The escrow of private keys is prohibited.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

REMINDER - CA conducted a risk analysis to determine the specific security objectives, to cover the business risks of the entire PKI, and technical and non-technical security measures to implement. Its CPS was developed based on this analysis.

5.1 PHYSICAL SECURITY CONTROLS

5.1.1 Site Location and Construction

These informations are specified in the CPS.

5.1.2 Physical access

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

Outside working hours, the implementation of physical and logical intrusion detection means strengthening the security of the PKI. In addition, any person (external service provider, etc.) entering in this physically secure area can not be left without the supervision of an authorized person.

5.1.3 Power and Air Conditioning

Measures concerning the supply of electricity and air conditioning are taken to meet the commitments of the CA described in this CP on ensuring the level of availability of its functions, including revocations management features and information functions on the status of certificates.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

Specific measures are implemented to avoid compromise or theft of information. The assets corresponding to these information are managed according to procedures conforming to these security needs. They are handled in a secure manner to protect the assets from damage, theft and unauthorized access.

Management procedures protect media against obsolescence and deterioration during the period during which the CA agrees to keep the information contained therein.

5.1.7 Waste Disposal

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

5.1.8 Off-site Backup

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

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

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

- Security officer: The security officer is responsible of implementing the component's security policy. He manages the controls on the physical access to the component's system hardware. He is authorised to review the archives and is responsible of analysing the event logs to detect any incident, anomaly, attempted compromise, etc.
- Application manager: Within the component to which he is attached, the application manager is responsible of implementing the certificate policy and the declaration of the PKI's certification practices on the level of the application for which he is responsible. His responsibility includes all the functions provided by this application and the corresponding performances.
- System administrator: He is responsible of the start-up, configuration and technical maintenance of the component's IT hardware. He provides the technical administration of the component's systems and networks.
- Operator: Within a PKI component, based on his duties, an operator runs applications for the functions implemented by the component.
- Controller: Designated by a competent authority, this person's role is to regularly perform verifications on the compliance of the implementation of the functions provided by the

component relative to the certification policies, to the PKI's declarations of certification practices, and to the component's security policies.
- Registration Officer: Responsible for approving end entity Certificate generation and revocation.
- Secret share holder: It has the responsibility to ensure the confidentiality, integrity and availability of the secrets assigned to him.

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

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

5.2.2 Number of Individuals Required per Task

For reasons of availability, each task must be performed by at least two people.

At a minimum, each task is assigned to two different people:
- System administrator;
- Operator.

For some sensitive tasks (eg key ceremony), many people are required for security reasons and "dual control."

5.2.3 Identification and Authentication for Trusted Roles

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

5.2.4 Role Requiring Separation of Duties

About trusted roles, the following rollups are prohibited within the PKI:
- Security officer and system administrator / operator;
- Controller and any other role;
- System operator and administrator.

5.3 PERSONNEL SECURITY CONTROLS

5.3.1 Qualifications, Experiences, and Clearance Requirements

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

The management personnel, the security officer, system administrators, have the expertise necessary for the performance of their respective roles and are familiar with the security procedures applied to the operation of the PKI.

AC inform any employee involved in the PKI trusted roles of its responsibilities for PKI services and procedures related to system security and monitoring staff.

5.3.2 Background Check Procedures

The CA ensures that all employees involved on the PKI suffered no contradiction in justice conviction with their functions. The employees provide a copy of the bulletin No before their Assignment. 3 of his criminal record. This check is renewed periodically (at least every 3 years).

In addition, the CA ensures that the employees do not suffer from conflict of interests detrimental to the impartiality of their tasks.

5.3.3 Training Requirements and Procedures

Initial training to software, hardware and internal operating and safety procedures is provided to employees, in line with the role that the CA assigns.

An awareness on the implications of the operations whose they are responsible is also achieved.

5.3.4 Retraining Frequency and Sequence

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

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Controls

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

5.3.8 Documentation Supplied to Personnel

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

5.4 AUDIT LOGGING PROCEDURES

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

5.4.1 Types of Events Recorded

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

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

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

- Physical access (recorded electronically);
- The logical access to systems;
- The actions of maintenance and configuration changes in manually registered systems;
- Changes in personnel;
- Operation of disposal and reset of media containing confidential information (keys, activation data, personal information on Subscribers and Subjects).

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

- Events related to signing keys and CA certificates or activation data (generation, backup and recovery, revocation, destruction, disposal of media, ...);
- Receiving a certificate request (initial and renewal);
- Validation / reject a certificate request;
- Certificate generation;
- Transmission certificates to Subjects and, if appropriate, acceptances / explicit releases by Subjects;
- Publish and update information related to the CA (CP / CPS, CA certificates, Terms and Conditions, etc.)
- Receipt of requests for revocation;
- Validation / reject a request for revocation;
- CRL generation and publication;
- Disposal of media containing personal information on Subscribers and Subjects.

Each record of an event in a journal contains at least the following fields:

- The type of event;
- The date and time of the event (the exact time of the significant CA events on the environment, key management and certificate management is recorded);
- The name of the executant or the reference of the system that triggered the event;
- The result of the event (success or failure).

Depending on the type of event, there are also the following fields:

- The recipient of the operation;
- the name of the applicant of the operation or the reference of the system which request;
- The names of those present (for operations requiring several persons);
- The cause of the event;
- All the information characterizing the event (eg. serial number of the certificate issued or revoked).

The logging process allows real-time recording of transactions. In case of manual input, writing is made exceptions the same business day as the event.

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

5.4.2 Frequency for Processing and Archiving Audit Logs

Cf. chapter 5.4.8

5.4.3 Retention Period for Audit Logs

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

5.4.4 Protection of Audit Log

Only members dedicated CA can process these files.

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

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Log Accumulation System

Details are given in the CPS.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.8 Vulnerability Assessment

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

Event logs are analyzed in their entirety to the frequency of at least 1 every work day and upon detection of an abnormality. A summary analysis is produced for the occasion.

A reconciliation between the various logs of functions that interact with each other is made at the rate of at least 1 times per week to verify the correlation between dependent events and to reveal any abnormality. The auditor is assisted by a person with skills related to the different environments used.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

CA is archiving:

- The software (executable) constituent of the PKI;
- IT equipment configuration files;
- Event Logs of various components of the PKI;
- The CP;
- The CPS;
- The digital Certificate requests;
- The records of Certification Agent registration;
- The records of DRA operator registration;
- The certificate request files with credentials;
- The certificates issued;

- The requests for revocation;
- The CRL issued;
- The OCSP responses.

5.5.2 Retention Period for Archive

5.5.2.1 Certificates Application Files

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

5.5.2.2 Certificates, CRL / ARL and OCSP Responses Issued by the CA

Certificates of Subjects and of CA and the CRL / ARL produced (respectively by the CA and Certigna), are archived for at least seven years after their expiration.

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

5.5.2.3 Event Logs

Event logs specified in Chapter 5.4 are archived for seven years after their generation.

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-stamping of Records

The data are dated according to Chapter 6.8.

5.5.6 Archive Collection System

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

5.5.7 Procedures to Obtain and Verify Archive Information

Archives can be recovered only by the dedicated members of the CA allowed to process these files within a maximum of two working days.

Data about contractors can be retrieved on their request.

5.6 KEY CHANGEOVER

5.6.1 CA Key

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

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

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

5.6.2 Keys of the Other Components

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

5.7 COMPROMISE AND DISASTER RECOVERY

The CA establishes procedures to maintain activities, wherever possible, and described in these procedures, the steps provided in case of corruption or loss of computing resources, softwares and data.

5.7.1 Incident and Compromise Handling Procedures

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

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

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

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

5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

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

5.7.3 Recovery Procedures After Key Compromise

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

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

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

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

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

5.7.4 Business Continuity Capabilities after a Disaster

The various components of the PKI have the necessary means to ensure the continuity of their activities in accordance with the requirements of the CP (see chapter 5.7.2).

CA use the redundancy of its information systems into several sites and its Business continuity plans to ensure the services continuity.

5.8 CA OR RA TERMINATION

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

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

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

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

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

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

5.8.2 Cessation of Activity Affecting the CA

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

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

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

The contact identified on the website of the ANSSI (https://www.ssi.gouv.fr) is immediately informed in case of cessation of trading of the CA.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

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

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

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

The ceremony took place following a predefined script:

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

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

After their generation, the secrets are issued to their holders designated in advance and skills to this trusted role by CA. One carrier can hold only one secret of the same CA. Secrets are placed in sealed envelopes, placed in vaults.

6.1.1.2 RA Key Pair Generation

No stipulation.

6.1.1.3 Subject Key Pair Generation

See 6.1.1.1.

6.1.2 Private Key Delivery to Subject

The CA rejects a certificate request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key.

6.1.3 Public Key Delivery to Certificate Issuer

No stipulation.

6.1.4 CA public Key Delivery to Relying Parties

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

The public key of CA is broadcast in a certificate signed by the Certigna Root CA. The public key of the Certigna Root CA is distributed in a self-signed certificate.

These public CA keys and their control values are disseminated and retrieved by the information systems of all certificates acceptors through the Certigna website at https://www.certigna.fr.

6.1.5 Algorithm type and key sizes

6.1.5.1 Root CA Certificates

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

6.1.5.2 Subordinate CA Certificates

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

6.1.5.3 Subject Certificates

See 6.1.5.1 and 6.1.5.2.

6.1.6 Public Key Parameters Generation and Quality Checking

The parameters and signature algorithms implemented in cryptographic boxes, physical media and software are documented by CA.

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

6.1.7 Key Usage Purposes

The use of the private key of the CA and associated certificate is exclusively limited to signing certificates and CRL (cf. chapter 1.5.1).

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The cryptographic module used by the Root CA and CA for the generation and the implementation of their signing keys are compliant with the requirements of the chapter 10.

These devices are resources exclusively available for CA's servers through a dedicated VLAN.

6.2.2 Private Key Multi-person Control

Control of CA signature private key is provided by trusted personnel and with a tool implementing sharing secrets (systems where n operators of m must authenticate, with n at least equal to 2).

6.2.3 Private Key Escrow

The CA private keys are never escrowed.

6.2.4 Private Key Backup

The private key of the CA is saved:

- Inside a second cryptographic module compliant with the requirements of the chapter 10.
- Outside the cryptographic module enciphered by the module and dispatched to several persons in trusted roles.

6.2.5 Private Key Archival

The private key of the CA is never archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The CA private keys are generated in the cryptographic module. As described in 6.2.4, the CA private keys are exportable / importable from the cryptographic module in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

The root CA private key is generated in a cryptographic module described in chapter 6.2.1 and is exported in accordance with the requirements of chapter 6.2.4 in order to be continuously taken offline. The key is reconstituted in the cryptographic module to allow the annual generation of ARLs or the creation of a new intermediate authority, then deleted from the module once the operation is complete.

6.2.8 Activating Private Keys

Activation of CA private key in the cryptographic module (corresponds to the generation or restoration of keys) is controlled via activation data (see section 6.4) and involves two people with a trusted role within PKI (security manager, and operator authorized to administer the cryptographic module).

6.2.9 Deactivating Private Keys

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

6.2.10 Destroying Private Keys

End of life of a private key of CA, normal or early (revocation), the key and the secrets of shares to reconstruct are systematically destroyed. A record of destruction of the key and of the secret share is established at the end of this procedure.

6.2.11 Cryptographic Module Capabilities

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

Subject key pair protection devices are evaluated at a specified level in chapter 11.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The public keys of the CA and Subjects are stored within the archiving of relevant certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

For Certigna PKI, the validity period of the Certigna Root CA certificate is 20 years, and that of the CA certificate is 18 years.

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

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

6.4.1.1 Generation and installation of activation data corresponding to the private key of the CA

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

The activation data match the PIN of the administration smart cards for the cryptographic module.

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

In the case where the key pair is generated by the CA, activation data are transmitted:

- If the device is a token, through the client space after authentication of the Subject;
- If the device is an cryptographique module with different form of activation data (cards, secrets, etc.) through different communication channels (email, mail, phone/SMS) and at different periods of time.
- [QCP-n] In the case of another type of hardware or software equipment, via a communication channel different from the platform on which the certificate is proposed (mail, mail, telephone / SMS).

6.4.2 Activation Data Protection

6.4.2.1 Protection of activation data corresponding to the CA private key

Activation data are directly provided to secret holders during the key ceremonies. Their storage conditions ensure their availability, integrity and confidentiality.

6.4.2.2 Protection of activation data corresponding to the subject private key

If the key pair is generated by the RA, it also generates the activation data that are sent as described at chapter 6.4.1. These activation data are not backed up by RA and are modified by the Subject when accepting the certificate or in case of a cryptographic module, after hardware reception.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

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

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

Monitoring devices and audit procedures of the system settings, including routing elements, are in place.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

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

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

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

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

6.6.2 Security Management Controls

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

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

Interconnection to public networks is protected by security gateways configured to accept only the necessary protocols to the desired operation by CA.

The CA guarantees that the components of the local network are kept in a physically secure environment and their configurations are periodically audited for compliance with the requirements specified by the CA.

6.8 TIME-STAMPING

To ensure synchronization between different dating of events, the various components of the PKI synchronize their clocks with respect to a reliable source of UTC.

7 CERTIFICATE AND CRL PROFILES

The certificates and CRLs generated by the CA comply with ITU-T Recommendation X.509 v3 standard, RFC 5280 and applicable requirements of 319 412 ETSI specifications.

7.1 ROOT CA CERTIFICATE

7.1.1 Basic fields

Fields	Certigna
Version	V3
Serial Number	00 FE DC E3 01 0F C9 48 FF
Signature	SHA-128 RSA 2048
Subject Public Key Info	RSA 2048 bits
Validity	Dates and times of activation and expiry of the certificate
Issuer DN	CN = Certigna O = Dhimyotis C = FR
Subject DN	CN = Certigna O = Dhimyotis C = FR

7.1.2 Extensions

Extensions	Critical	Description
SKI	No	ID of the public key of Root CA
AKI	No	ID of the public key of Root CA
Netscape Cert type	No	SSL Certification Authority MIME Certification Authority Signature Certification Authority
Basic Constraints	**Yes**	**cA** = TRUE
Key Usage	**Yes**	Certificate signing CRL signing

7.2 SUBORDINATE CA CERTIFICATE

7.2.1 Basic fields

Fields	Signed by « Certigna »
Version	V3
Serial Number	2F 13 DA F1 87 0C D4 33 8F 18 DB FC 37 6B B2 7B
Signature	Identifier of CA signing algorithm SHA-256 RSA 4096
Subject Public Key Info	RSA 4096 bits
Validity	Dates and times of activation and expiry of the certificate
Issuer DN	CN = Certigna O = Dhimyotis C = FR
Subject DN	CN = Certigna <Name> CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR

7.2.2 Extensions

See Certification policies associated to subordinate CA.

7.2.3 Processing semantics for the critical CP extension

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

7.2.3.1 Criticality

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

If the extension is uncritical, then:

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

If the extension is critical, then:

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

7.2.3.2 Extension description

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

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

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

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

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

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

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

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

7.3 CRL PROFILE

7.3.1 Basic fields

Fields	Description
Version	V2
Signature	ID of the CA signing algortihm SHA-256 RSA 4096
Issuer	CN = Certigna O = Dhimyotis C = FR
This Update	Date of generation of ARL
Next Update	Date of next update of ARL [One year maximum]
Revoked certificates	List of serial numbers of revoked certificates

7.3.2 Extensions

Extensions	Critical	Description
Authority Key Identifier	No	ID of the public key of CA
CRL Number	No	CRL serial number
ExpiredCertsOnCRL	No	Date from which revoked and expired certificates are maintained in the CRL.

7.4 OCSP PROFILE

Profiles are described in Subordinate CA CertificatePolicy.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT

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

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

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

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

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

This control is conducted once a year by the CA. Qualification audits are perfomed every year.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

Control is assigned by the CA to a team of competent auditors in computer security and in activity of the controlled component.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4 TOPICS COVERED BY ASSESSMENT

The compliance checks are implemented to verify compliance with the commitments and practices defined in the CA's CP and the CPS, and elements thereunder (operational procedures, resources used, ...).

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

According to the results, the consequences of control are:

- In case of 'improvement', and according to the importance of the improvement, the audit team makes recommendations to CA to improve its functioning. Improvements are left to the discretion of the CA that decides whether or not to implement them.

- In case of "remark" or "minor nonconformity", the CA sends to the component a notice specifying in what timeframe nonconformities shall be lifted. Then, a control for confirmation will verify that all critical points have been resolved.
- In case of a "major nonconformity", and according to the importance of non-conformities, the audit team makes recommendations to the CA that can be business termination (temporary or permanent), revocation of certificate of component, revocation of all certificates issued since the last positive control, etc. The choice of measurement to be used is made by the CA and must respect the internal security policies.

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

8.6 COMMUNICATION OF RESULTS

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

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

The access to certificate status information and revocation is free.

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

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

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

Cf. chapter 9.9.

9.3 CONDIFENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

The information considered confidential are:

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

9.3.2 Information not within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

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

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

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

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

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

Electronic certificate application files containing personal data are archived for at least seven years after the expiration of the certificate and as long as necessary for the purposes of providing proof of certification in legal proceedings, in accordance with applicable law. The

personal identity information can be used as authentication data in the event of a request for revocation or information.

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

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

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

DHIMYOTIS, Service du DPO,

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

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

9.4.2 Information Treated as Private

The information considered as personal are:

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

9.4.3 Information not Deemed Private

No stipulation.

9.4.4 Responsibility to Protect Private Information

Cf. legislation and regulations on French territory.

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

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

9.6 REPRESENTATIONS AND WARRANTIES

Obligations common to the PKI components are:

- To protect and ensure the integrity and confidentiality of their secret keys and / or private;
- Only use their cryptographic keys (public, private and / or secret) for the purposes specified when issued and with the equipment as specified in the conditions set by the CA's PC and documents arising therefrom;
- Respect and implement the part of the CPS incumbent upon them (this part shall be communicated to the corresponding component);
- Submit to compliance checks by the audit team mandated by the CA (See Chapter 8) and the qualifying body;
- Respect the agreements or contracts between them or with the entity;
- To document their internal operating procedures;
- Implement the means (human and technical) necessary to achieve the benefits to which they are committed under conditions that ensure quality and safety.

9.6.1 CA Representations and Warranties

The CA will:

- can demonstrate to certificate users; it has issued a certificate to a Subject and the corresponding Subject accepted the certificate in accordance with the requirements of Section 4.4;
- Ensure and maintain the consistency of its CPS with its CP;
- Take all reasonable steps to ensure that Subjects are aware of their rights and obligations regarding the use and management of keys, certificates or equipment and software used for PKI. The relationship between Subjects and the CA is formalized in a contractual relationship / regulation specifying the rights and obligations of the parties including the guarantees provided by the CA.

CA assumes any harmful consequences resulting from non-compliance of its CP by itself or one of its components. CA planned to meet its responsibilities in its operations and / or activities and have the financial stability and resources required to operate in accordance with

this policy. In addition, the CA recognizes its liability in case of fault or negligence of itself or one of its components, regardless of the nature and gravity, which would result in reading, alteration or misuse of personal data of Subjects for fraudulent purposes, these data are contained in transit or in the certificate management applications of the CA.

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

9.6.2 RA Representations and Warranties

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

9.6.3 Subject Representations and Warranties

The Subject has the duty to:

- Communicate accurate and updated informations at the request or renewal of the certificate;
- Protect the Subject private key under its responsibility by means appropriate to its environment;
- Protect his activation data and, where appropriate, implement them;
- Protect access to Subject certificates;
- Respect the conditions of use of the Subject private key and certificate;
- Inform Registration Authority of any changes to the information contained in the Subject certificate;
- Make, without delay, a request for Subject certificate revocation which it is responsible to the Registration Authority, or if any of the Certificate Agent of its entity, in case of compromise or of the corresponding private key compromise.

The relationship between the Subject and the CA or its components is formalized by a commitment from the Subject to certify the accuracy of information and documents provided.

This information also applies to DRA’s operators and Certification Agents.

9.6.4 Relying Party Representations and Warranties

Third party users must:

- Check and maintain the use for which a certificate was issued;
- For each certificate of the certification chain, from the Subject certificate to the Certigna Root CA, verify the digital signature of the issuing CA on the certificate and check the validity of the certificate (validity date, revocation status);
- Check and respect the obligations of certificate users expressed in this CP.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.6.6 Termination

In the event of a breach by the CA or the Subject to one of its obligations hereunder, the other party shall be authorized thirty (30) days after formal notice sent by registered letter with acknowledgment of receipt. had no effect, to terminate these by operation of law by registered letter with acknowledgment of receipt without prejudice to any damages and interests to which it could claim due to the deficiencies invoked.

9.7 DISCLAIMERS OF WARRANTIES

Any certificate ordered must be accepted by the Subject on the customer space created from the CA website or from one of its DRA. Before generating the certificate, the Subject must verify that the information stated in his certificate request is accurate. Failing this, the Subject must contact a member of the staff of the CA either by telephone at 0 806 115 115 (free service cost of a local call), or by email at the following address: contact@certigna.fr. Telephone support is available from Monday to Friday, except holidays, from 9 AM to 6 PM without interruption. The Subject is aware that in case of error during the order in the nature of the certificate, no modification can be made by the CA and the Subject will have to make a new certificate request. If a payment had already been made, the CA would not be required to pay any refund.

Once the certificate request validated, the certificate is generated. The Subject is then brought to confirm the accuracy of said information, which means acceptance of the certificate. otherwise, the Subject will have to make a new certificate request and the certificate generated will not give rise to any refund.

Once the certificate accepted, the certificate is available to the Subject either on his customer area or on a cryptographic device. the installation of the certificate is done under the sole responsibility of the Subject. In case of any difficulty during this last phase, the Subject can contact the CA at the telephone number and the email address indicated above or via contact details available on the DRA website. The CA does not guarantee the operation of the certificate in the case of use outside the uses provided for in chapter 1.5 hereof.

The warranty is valid for the worldwide outside the USA and Canada.

9.8 LIMITATIONS OF LIABILITY

The CA is subject to a general obligation of means. The CA cannot be held liable for the Subject for direct damage that may be attributed to it for the services entrusted to it under these GCSU.

The CA's responsibility cannot be sought for any indirect loss, such as, in particular, loss of turnover, loss of profit, loss of orders, loss of data, loss of opportunity, disturbance to the image or any other special damage or events beyond its control or any fact not attributable to it.

The CA is only responsible for the tasks specifically assigned to it under this CP.

The CA cannot be held responsible in any way for the use of the certificates.

In any case, the responsibility of the CA cannot be sought in case of:

- Fault, negligence, omission or default of the CA, which would constitute the exclusive cause of the occurrence of the damage,
- Malfunction or unavailability of tangible or intangible property in the case where it has been provided by the Subject,
- Delay in providing the data to be processed due to the Subject;
- Loss of the qualification of a third-party provider that is beyond the control of CERTIGNA (ex: the supplier of cryptographic support).

By express agreement between the CA and the Subject, the liability of the CA is limited, by certificate request, all damages, to the sum of two (2) times the amount paid under the certificate request.

9.9 INDEMNITIES

9.9.1 Indemnification by CAs

Dhimyotis signed a contract of "liability insurance".

The CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others.

The CA defends, indemnifies, and holds harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier’s software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy a Certificate that has expired, or a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Subject

No stipulation.

9.9.3 Indemnification by Relying Parties

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

CA's CP remain in effect at least until the end of life of the last certificate issued under this CP.

9.10.2 Termination

The publication of a new version of the documents mentioned at chapter 1.1 may result, depending on the changes made, the need for the CA to evolve its corresponding CP. In this case, such compliance will not impose the early renewal of licenses already issued, except in exceptional cases linked to security.

Finally, the validity of the CP can happen prematurely in case of cessation of trading of the CA (see section 5.8).

9.10.3 Effect of Termination and Survival

The end of validity of the CP also terminates all clauses within it.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

In case of change of any kind involved in the composition of the PKI, the CA will:

- Validate later than one month before the start of the operation, this change through technical expertise to assess the impacts on the quality and safety functions of the CA and its various components;
- Inform, within one month after the end of the operation, the evaluation body.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The CA conducts any change in the specifications stipulated in the CP and CPS and / or components of the CA that appears necessary to improve the quality of certification services and the security of processes, remaining however meets the requirements of RGS and additional documents to the latter.

The CA also conducts any changes to the specifications stipulated in the CP and CPS and / or components of the CA that is made necessary by legislation, regulations or by the results of checks.

9.12.2 Notification Mechanism and Period

The CA communicates via its website https://www.certigna.fr the evolution of the CP based on its amendments.

9.12.3 Circumstances under which OID Must Be Changed

The OID of the CA's CP being registered in the certificates it issues, evolution in this CP has a major impact on the certificates already issued (e.g., increase in registration requirements of subjects, which cannot be applied to certificates already issued) must result in a change of the OID, so that users can clearly distinguish which certificates correspond to which requirements.

When the change of the CP is typographical or it does not impact the quality and safety of the functions of the CA and the RA, the OID of the CP and the corresponding CPS are not changed.

9.13 DISPUTE RESOLUTION PROVISIONS

The validity of this CP and any other question or dispute relating to its interpretation, execution or termination will be governed by French law.

The CA commit themselves to devote their best efforts to the amicable resolution of all the questions or the litigation which could divide them, before the seizure of the jurisdiction hereinafter designated.

The CA agree, in the event that an amicable agreement is impossible to stop, that the courts of Lille will have exclusive jurisdiction to hear any dispute resulting from the validity, interpretation, execution or termination hereof, and more generally from any dispute arising herein that could divide them, notwithstanding pluralities of defendants or warranty claim.

9.14 GOVERNING LAW

Any dispute concerning the validity, interpretation, execution of this CP will be submitted to the courts of Lille.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CP is subject to French law and applicable legislative texts for this CP.

The trust service practices under which the CA operates are non-discriminatory.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

This document contains all the provisions governing the PKI.

9.16.2 Assignment

Cf. chapter 5.8.

9.16.3 Severability

In case of an invalid clause, the other clauses are not questioned.

In the event of a conflict between the requirements of this CP and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which the CA operates or issues certificates, CA modifies any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, CA immediately include in this section (and prior to issuing a certificate under the modified requirement) a detailed reference to the Law requiring a modification of these requirements and the specific modification to these Requirements implemented by the CA.

The CA notifies the CA/Browser Forum and ANSSI (prior to issuing a certificate under the modified requirement) of the relevant information newly added to this CP by sending a message to questions@cabforum.org (or such other email addresses and links as the Forum may designate) leading to a confirmation.

Any modification to CA practice enabled under this section is discontinued if and when the Law no longer applies, or these requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to the CP and CPS of CA and a notice to the CA/Browser Forum are made within 90 days.

9.16.4 Enforcement

No renunciation of any of his rights shall be allowed to take place tacitly. To be opposable to the AC a renunciation must have been made in writing. Such waiver shall not constitute a renunciation of future rights audits.

9.16.5 Force majeure

The CA will not be held responsible for any delay or failure in the performance of any of its obligations under this CP, if the delay or failure is due to the occurrence of a case of force majeure usually recognized by the jurisprudence of French courts and tribunals.

9.17 OTHER PROVISIONS

No stipulation.

10 APPENDIX 1: SECURITY REQUIREMENTS FOR THE CA'S CRYPTOGRAPHIC MODULE

10.1 SECURITY OBJECTIVES REQUIREMENTS

The cryptographic module used by the CA to generate and implement its signature keys (for the generation of electronic certificates, CRL, and OCSP responses), must meet the following security requirements:

- Ensuring the confidentiality and integrity of the CA's signature private keys throughout their lifecycle, and ensuring their secure destruction at their end-of-life;
- Being able to identify and authenticate its users;
- Limiting access to its services per the user and role assigned;
- Ability to carry out a series of tests to verify that it is running correctly and enter in a secure status if an error is detected;
- Create a secure electronic signature to sign the certificates generated by the CA, that does not reveal the CA's private keys and that cannot be falsified without knowing these private keys;
- Creating audit records for each modification relating to security;
- If a backup and restoration function for the CA's private keys is offered, guaranteeing the confidentiality and integrity of the backed-up data and demanding at least a double control of the backup and restoration operations.
- The CA's cryptographic module must detect attempted physical alterations and enter in a secure status when an attempted alteration is detected.

10.2 QUALIFICATION REQUIREMENTS

The cryptographic module used by the CA is:

- qualified at "Enforced" level by ANSSI according the process described by the RGS;
- Common Criteria at EAL 4+ level or FIPS 140-2 Level 3.

www.certigna.com