Certification Policy
CERTIGNA WILD CA

OID :	1.2.250.1.177.2.7.1
Version :	1.8
Date :	08/31/18
Authors :	J. Allemandou
Classification :	Public

CONTENTS

DOCUMENT HISTORY

Date	Version	Authors	Document change
10/19/2015	1.0	R. DELVAL	Creation
08/01/2016	1.1	J. ALLEMANDOU	Precisions about: - email address verification (cf. 3.2), - FQDN verification (cf. 4.2.1).
12/16/2016	1.2	J. ALLEMANDOU	Revision of the graphique chart et precisions about: - The level of conformity with ESTI specifications (cf. 1.1), - The withdrawal of « Certifié conforme » (cf. 3.2.3), - The terms of a current renewal (cf. 3.3.1), - The terms of acceptance of the certificate (cf. 4.4.1), - The OCSP Stapling requirements (cf. 4.9.9), - The role of Registration officier (cf. 5.2.1), - The minimum delay for archival (cf. 5.5.2), - The issuance of the cryptographic device (cf. 6.1.2), - The CA signed by 2 Root CA (cf. 7.1), - The qualification requirement of the device (Cf. 11.2).
04/17/2017	1.3	J. ALLEMANDOU	Precisions about: - Version of applicable CAB/Forum BR (cf. 1.1), - URL for certificates testing (cf. 2.1), - Revoked and rejected certificates database (cf. 4.1.1), - gTLD management (cf. 4.2.2), - CRL and OCSP responder (cf. 4.9.9), - The value of public exponant used for RSA (cf. 6.1.6), - RFC 5280 conformity (cf. 7), - Certificates serialNumber field's format (cf. 7.2), - Profiles of OCSP certificates issued by CA (cf. 7.2.3), - Audits of processed certificate requests (cf. 8.4), - Synthesis of CA commitments (cf. 9.6.1), - Indemnity of software providers (cf. 9.9), - Periodicity of CP/CPS reviews (cf. 9.12.1), - Management of conflicting requirements (cf. 9.16.3).
09/01/2017	1.4	J. ALLEMANDOU	Addition of commitments about: - DNS CAA (cf. 4.2.1), - Certificate Transparency (cf. 7.4), Addition of « ExpiredCertsOnCRL » extension (7.3.2).
12/01/2017	1.5	J. ALLEMANDOU	Precisions about: - Email contact of Certigna (1.6.2), - Form to report a certificate (2.3), - The periodicity of ARL update (cf. 2.4.4), - Controls on high risk certificate requests (3.2.6), - The registrar used for controls (cf. 4.2.1), - Controls on TLD (4.2.2), - The request acceptance (cf. 4.2.2), - The possible causes for revocation (Cf. 4.9.1), - The physical access (cf. 5.1.2), - The diagram of the CA hierarchy (cf. 7), - The lifetime of SSL/TLS certificates to 825 days (cf. 7), - The maximum longer of serial number (cf. 7), - The qualification of CA cryptographic module (cf. 10.2), - Change of title numbers (6.2.8 to 6.2.11).
01/25/18	1.6	J. ALLEMANDOU	Precisions about the activation data issuance (cf. 6.4.1).
07/02/18	1.7	J. ALLEMANDOU	Addition of complementary controls of FQDN (cf. 3.2.6): - Constructed Email to Domain Contact; - Agreed-Upon Change to Website; - DNS Change. Precisions about: - The logs used for pre-certificates (cf. 7.6), - The personal data protection policy (cf. 9.4.1).

08/31/18	1.8	J. ALLEMANDOU	Precisions about: - The distribution of controls between the RA and the DRAs (see 1.4.5, 4.2.1), - The controls performed on the DNS CAA records (see 4.2.1), - The issuance of certificates signed by the Root CA (see 4.3.1).

1. INTRODUCTION

1.1. General presentation

Certigna has a Certification Authority (CA) named Certigna Wild CA to provide "SSL/TLS client/serveur Authentication" certificates to application services.

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 guesses he is familiar with the concepts related to the technology of Public Key Infrastructure (PKI).

This CP meets the requirements of

- The eIDAS Regulation (EU) N°910/2014 and ETSI EN 319 411-1 the OCVP / PTC levels;
- 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.

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

1.2. Document identification

This PC can be identified by the name of the « Certigna Wild CA » and by its OID: 1.2.250.1.177.2.7.1.

Usage(s)	Type de serveur	OID
Authentication of multi-domains SSL/TLS client/server	Pro (company/administration)	1.2.250.1.177.2.7.1.1.1
Authentication of wildcard multi-domains SSL/TLS client/server	Pro (company/administration)	1.2.250.1.177.2.7.1.2.1

1.3. Definitions and abbreviations

1.3.1. Abbreviations

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

AA	Administrative Authority
ANSSI	National Agency for information systems security
ARL	Authority Revocation List
BCP	Business Continuity Plan
CA	Certification Authority
CAA	Certification Authority Authorization
CAG	Certification Agent
CGU	Conditions of General Use
CNIL	National Commission for Computing and Liberties
CP	Certification 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
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
SCM	Server Certificate Manager
RSA	Rivest Shamir Adleman
SCT	Signed Certificate Timestamp
SSL	Secure Sockets Layer
TA	Timestamping Authority
TLS	Transport Layer Security
TSP	Trust Service Provider
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

1.3.2. 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 Authorization - From RFC 6844, the Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis- issue.

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

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 ESCM (eg 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.

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.

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

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

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.

1.4. Entities involved in PKI

1.4.1. Certification authority

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.

1.4.2. Registration authority

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

- The acquisition and verification of future information of Certificate Manager, of application service, and of business 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 Certificate Manager'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.

1.4.3. Server certificate managers

As part of this CP, Certificate Managers can only be a natural person. It is responsible for the use of the certificate (and associated private key) in which the application service concerned is identified and the entity for which he uses the certificate and with which it maintains a contractual / reporting relationship / regulatory.

The Certificate Managers must meet the conditions and obligations that are set in the CP and in the Terms and conditions of use.

The certificate is attached to the application service and not to the Certificate Manager. In case of change of Certificate Manager, the entity shall report it to the CA and appoint a successor. The CA revokes certificates for which there is no more Certificate Manager explicitly identified.

1.4.4. Certificate users

A user of the certifacte could be:

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

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

1.4.5. Other participants

Delegated Registration Authority

CA also relies on DRA to outsource a part of RA's functions. An operator of DRA has the power to:

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

He or she performs for the authority, in the context of issuance of the certificate, the verification of future Certicate Manager's identity under the same conditions and with the same level of safety as those required for the operator of RA. For this it is directly related to RA.

The commitments of the DRA operator against CA are specified in a written agreement with the responsible entity of the operator and in the commitment letter to be signed by the latter. Both documents include state that the operator must perform impartial and

scrupulous verification of the identity and of the possible future Certicate Manager attributes and application services. He/she must also respect the parts of the CP and CPS incumbent on him.

Certification Agent

CA offers the opportunity for the client's entity to designate one or more Certification Agents. The Certification agent has, by law or by delegation, the power to:
- request a certificate generation or renewal certificate on behalf of the entity;
- request a certificate revocation on behalf of the entity.

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

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

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

1.5. Use of the certificates

1.5.1. Applicable usage domains

Key pairs and certificates of the serveur

These certificates are used for the server authentication with people or another server, as part of establishing secure sessions, such as SSL / TLS or IPsec to establish a symmetric session key to encrypted the exchanges in this session.

The establishment of the session key can be done by an asymmetric cryptographic mechanism of RSA (the symmetric key generation by the customer and this symmetric key encryption with public key of the server) or type Diffie-Hellman (obtaining the symmetric key using an algorithm combining the client private key and public key of the server, and vice versa).

The electronic certificates are used for applications where security needs are moderate given the high risks that threaten them.

Key pairs and certificates of CA and of 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: server certificates, CA OCSP certificate, CRL.

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 CA, whose security level is adapted to that required for the AC.

1.5.2. Forbidden usage domains

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

1.6. Management of the CP

1.6.1. Entity managing the CP

CA has a Security Committee chaired by the Security Officer.

This committee is responsible for developing, monitoring, modification and validation of this CP. It shall act on any necessary changes to be made to the CP at regular intervals.

1.6.2. Contact point

Dhimyotis - Certigna
20 allée de la Râperie
Zone de la plaine
59650 Villeneuve d'Ascq
FRANCE

Contact by email: contact@certigna.fr

1.6.3. Entity determining the compliance of the CPS with the CP

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

1.6.4. CPS compliance approval procedures

The CPS translated into technical terms, organizational and procedural requirements of the CP based on the company's 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.

2. RESPONSIBILITIES REGARDING THE PROVISION OF INFORMATION HAVING TO BE PUBLISHED

2.1. Entity in charge of providing information

CA provides to users and applications using certificates it issues, informations about the revocation status of valid certificates issued by the CA. These informations are published through several servers:

- Web Servers :
  - http://crl.certigna.fr/wildca.crl
  - http://crl.dhimyotis.com/wildca.crl
- OCSP Servers :
  - http://wildca.ocsp.certigna.fr
  - http://wildca.ocsp.dhimyotis.com
- URLs to test certificates :
  - Valid certificate : valid.wildca.dhimyotis.com
  - Expired certificate: expired.wildca.dhimyotis.com
  - Revoked certificate: revoked.wildca.dhimyotis.com

2.2. Information having to be published

The CA issues to the Certificate Managers and certificate users:

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

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

2.2.1. Publication of documentation

Publication of CP, Terms and conditions, and forms

The CP, the terms and conditions of the CA certification services and the various forms required for certificate management are published in electronic format at http://www.certigna.fr. The CP is also published at http://www.dhimyotis.com.

Publication of CPS

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

Publication of CA certificate

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

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

2.2.2. 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.

2.2.3. 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. 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”.

2.4. Publication timeframes and frequencies

2.4.1. 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 these informations (excluding certificate status information) is available on working days.

2.4.2. 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.

2.4.3. Publication of CRL

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

2.4.4. Publication of ARL

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

2.5. Published information access control

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.

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 application service ("subject" field) are identified by a "Distinguished Name" conform with the requirements of the X.501 Standard.

3.1.2. Necessary usage of explicit names

The certificate DN identifies the application service and is built from the server's identity.
The certificate DN is defined at chapter “7.2 Profiles of certificates and CRL” of this CP.

3.1.3. Anonymisation or pseudonymisation

The CA does not issue certificates with an anonymous identity.

3.1.4. Rules for interpreting the various types of names

No interpretation is made on the name inside the certificates.

3.1.5. Uniqueness of the names

The combination of the country of the entity and the FQDN or the server identity uniquely identifies the certificate holder.

Throughout the lifetime of the CA, the FQDN of a server attached to an entity can be assigned to another entity

3.1.6. Identification, authentication and roles of registered trademarks

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

3.2. Initial identity validation

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

During the certificate request, the email address of the Certificate Manager is verified through sending multiple emails that allow the Certificate Manager to access to his Certigna Customer account and certain activation data enabling him to recover and to use the certificate of the server.

3.2.1. Method for proving possession of the private key

CA ensures the detention of the private key by the Certificate Manager before certifying the public key. For this, the RA or the certificate manager itself generates the key pair in a device compliant with the requirements of the chapter 11, and provides to the CA the proof of possession of the private key by signing his certificate request (Certificate signing request with the PKCS # 10 format).

3.2.2. Validation of an entity's identity

Cf. chapter 3.2.3

3.2.3. Validation of an individual's identity

Registration of a server to which a certificate should be issued is performed via the registration of the corresponding Certificate Manager.

The Certificate Manager will demonstrate that it has the right to use the domain name included in the FQDN (ownership rights over the domain or right to use the part of the entity rights holder).

A Certificate Manager may have to change valid corresponding server certificate.
In this case, any new Certificate Manager shall also be subject to a registration procedure.
The Certificate Manager is either the legal representative of the entity or a natural person formally designated by the legal representative.

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

Registration of Certificate Manager without Certification Agent for a certificate to be issued

The registration of the future Certificate Manager requires the "legal person" identity verification (the entity attached to the future Certificate Manager), and the "natural person" identity verification (the future Certificate Manager), its authorization must be considered for the server and the entity in question.

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

Certificate request form	
Subject	Designation of a legal representative of the entity and its contact informations
	Designation of the future Certificate Manager and its contact informations
	Designation of the identification informations of the entity
	Designation of applicable Terms and conditions
Date	Signed less than 3 months ago
Signature	Signed by a legal representative to mandate the future Certificate Manager Signed by the future Certificate Manager to accept this role and the Terms and conditions

Official identification document of the Certificate Manager	
Subject	A photocopy of a valid identification element of the Certificate Manager, recognized by the Member State in which is deposited the certificate request. It can be an identification, a business card issued by an administrative authority (if that authority maintaining a register of identities ensuring the link between the agent and the business card), or a reference to administrative record of the agent. This item will be valid and be genuine or assumed we must assume that there as an authoritative source. The existence of the alleged identity is known from an authoritative source and CA must assume that the person is who they claim to be.
Date	Piece valid at the time of registration

Official identification document of the legal representative	
Subject	A photocopy of an official identification document recognized by the Member State in which is deposited the certificate request (with an ID photo), and valid at the time of registration of the legal representative.
Date	Piece valid at the time of registration

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

Document identificating the company	
Subject	The provision of a valid identification element of the entity, recognized by the Member State in which is deposited the certificate request. The entity should not be known by an authoritative source as being in a situation that would stop it from acting as a legal entity. Eg: *KBIS extract or Certificate of Identification at the National Directory of Companies and of their Establishments*) or, failing that, another valid document certifying the unique identification of the company to be included in the certificate.
Date	Document valid at the time of registration

Authentication of the future Certificate Manager by the RA (RA operator or DRA operator) is achieved by sending the file either by mail or in paperless form (scanned file and then e-mailed).

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

Registration of Certificate Manager without Certification Agent for an already issued certificate

In the event of a Certificate Manager change for a valid certificate, the new Cetificate Manager is subject to a registration procedure.

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

New Certificate Manager Registration form	
Subject	Designation of a legal representative of the entity and its contact informations
	Designation of the future Certificate Manager and its contact informations
	Designation of applicable Terms and conditions
Date	Signed less than 3 months ago
Signature	Signed by a legal representative to mandate the future Certificate Manager Signed by the future Certificate Manager to accept this role and the Terms and conditions

Official identification document of the Certificate Manager	
Subject	A photocopy of a valid identification element of the Certificate Manager, recognized by the Member State in which is deposited the certificate request. It can be an identification, a business card issued by an administrative authority (if that authority maintaining a register of identities ensuring the link between the agent and the business card), or a reference to administrative record of the agent. This item will be valid and be genuine or assumed we must assume that there as an authoritative source. The existence of the alleged identity is known from an authoritative source and CA must assume that the person is who they claim to be.
Date	Piece valid at the time of registration

Official identification document of the legal representative	
Subject	A photocopy of an official identification document recognized by the Member State in which is deposited the certificate request (with an ID photo), and valid at the time of registration of the legal representative.
Date	Piece valid at the time of registration

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

The future Certificate Manager authentication is done by sending the registration files by mail or in dematerialized form (scanned file and then by e-mail).
The Certificate Manager is informed that personal identity information can be used as authentication data during a possible revocation request.

Registration of a Certification Agent

The Certification Agent must register with the RA to substitute for RA in the process of registration of certificate requests.

The registration of a Certification Agent requires the verification of the "legal person" identity of the entity for which the Certification Agent is attached, the verification of the "natural person» identity of the future Certification Agent, and the relation between the future Certification Agent and this entity.

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

Certification Agent registration form	
Subject	Designation of a legal representative of the entity and its contact informations
	Designation of the future Certification Agent and its contact informations
	Designation of applicable Terms and conditions
Date	Signed less than 3 months ago
Signature	Signed by a legal representative to mandate the future Certification Agent Signed by the future Certification Agent to accept this role

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

Official identification document of the Certification Agent	
Subject	A photocopy of a valid identification element of the Certification Agent, recognized by the Member State in which is deposited the certificate request. It can be an identification, a business card issued by an administrative authority (if that authority maintaining a register of identities ensuring the link between the agent and the business card), or a reference to administrative record of the agent. This item will be valid and be genuine or assumed we must assume that there as an authoritative source. The existence of the alleged identity is known from an authoritative source and CA must assume that the person is who they claim to be.
Date	Piece valid at the time of registration

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

Document identificating the company	
Subject	The provision of a valid identification element of the entity, recognized by the Member State in which is deposited the certificate request. The entity should not be known by an authoritative source as being in a situation that would stop it from acting as a legal entity. Eg: *KBIS extract or Certificate of Identification at the National Directory of Companies and of their Establishments*) or, failing that, another valid document certifying the unique identification of the company to be included in the certificate.
Date	Document valid at the time of registration

The certification agent is informed that the personal identifying information may be used as the authentication data during a possible revocation request.

Registration of a Certificate Manager via a Certification Agent

Registration of a Certificate Manager via a Certification Agent requires validation by the Certification Agent of "natural person" identity of the future Certificate Manager and its attachment to the entity for which the Certification Agent is involved.

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

Certificate request form	
Subject	Designation of a legal representative of the entity and its contact informations
	Designation of the future Certificate Manager and its contact informations
	Designation of the identification informations of the entity
	Designation of applicable Terms and conditions
Date	Signed less than 3 months ago
Signature	Signed by a legal representative to mandate the future Certificate Manager Signed by the future Certificate Manager to accept this role and the Terms and conditions

Official identification document of the Certificate Manager	
Subject	A photocopy of a valid identification element of the Certificate Manager, recognized by the Member State in which is deposited the certificate request. It can be an identification, a business card issued by an administrative authority (if that authority maintaining a register of identities ensuring the link between the agent and the business card), or a reference to administrative record of the agent. This item will be valid and be genuine or assumed we must assume that there as an authoritative source. The existence of the alleged identity is known from an authoritative source and CA must assume that the person is who they claim to be.
Date	Piece valid at the time of registration

Official identification document of the Certification Agent	
Subject	A photocopy of a valid identification element of the Certification Agent, recognized by the Member State in which is deposited the certificate request. It can be an identification, a business card issued by an administrative authority (if that authority maintaining a register of identities ensuring the link between the agent and the business card), or a reference to administrative record of the agent. This item will be valid and be genuine or assumed we must assume that there as an authoritative source. The existence of the alleged identity is known from an authoritative source and CA must assume that the person is who they claim to be.
Date	Piece valid at the time of registration

The files are sent by mail to the RA for conservation, and possibly electronically signed with the certificate of the Certification Agent.
The Certificate Manager is informed that personal identity information can be used as authentication data during a possible revocation request.

Registration of a new Certificate Manager via a Certification Agent to a previously issued certificate

In case of change of Certificate Manager to a valid server certificate, the new Certificate Manager must be registered to the RA for the replacement of the old Certificate Manager.The registration files filed with a Certification Agent must include at least:

New Certificate Manager Registration form	
Subject	Designation of a Certification Agent of the entity and its contact informations
	Designation of the future Certificate Manager and its contact informations
	Designation of applicable Terms and conditions
Date	Signed less than 3 months ago
Signature	Signed by a Certification Agent to mandate the future Certificate Manager Signed by the future Certificate Manager to accept this role and the Terms and conditions

Official identification document of the Certificate Manager	
Subject	A photocopy of a valid identification element of the Certificate Manager, recognized by the Member State in which is deposited the certificate request. It can be an identification, a business card issued by an administrative authority (if that authority maintaining a register of identities ensuring the link between the agent and the business card), or a reference to administrative record of the agent. This item will be valid and be genuine or assumed we must assume that there as an authoritative source. The existence of the alleged identity is known from an authoritative source and CA must assume that the person is who they claim to be.
Date	Piece valid at the time of registration

The registration files are sent by mail to the RA for conservation, and possibly electronically signed with the certificate of the Certificate Manager.

3.2.4. Unverified informations

Not applicable.

3.2.5. Validation of the requester's 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. Validation of Domain Control

In addition to the validation of the authorization on the domain name, one of the controls below is implemented for each FQDN in order to ensure its control by the applicant and to confirm the legitimacy of the certificate request.

Constructed Email to Domain Contact

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

The random value is unique for each FQDN and remains valid no more than 30 days from its creation.

The email can be re-sent but a link with a new random value will be provided, making invalid the link sent previously.

If the constructed email is similar for multiple requested FQDNs (e.g. case of subdomains), then just one mail is sent to the domain contact containing associated links to confirm the control of each FQDN.

Agreed-Upon Change to Website

An email is sent by CERTIGNA to the applicant with an attachment containing a random value. This is a text file that the applicant must place in the "/.wellknown/pki-validation" directory of the website. An automatic control by CERTIGNA via port 80 (HTTP) or port 443 (HTTPS) makes it possible to check the presence on the website of the file and to check the random value it contains. The random value in the file does not appear in the request used for the check.

The random value is unique for each FQDN and remains valid no more than 30 days from its creation.

The email can be re-sent but a file with a new random value will be provided, making invalid the file sent previously.

If multiple FQDNs are concerned by the same request, only one mail is sent to the applicant containing the associated files. The applicant must place all files in the directory to allow the control of each FQDN.

DNS Change

An email is sent by CERTIGNA to the applicant with a DNS CNAME record to add to the website DNS configuration. This record consists of the domain name that is prefixed with a label with an underscore character (“_”) and of a random value.

The random value is unique for each FQDN and remains valid no more than 30 days from its creation.

The email can be re-sent but a record with a new random value will be provided, making invalid the record sent previously.

If multiple FQDNs are concerned by the same request, only one mail is sent to the applicant containing the associated records. The applicant must add all the records to the website DNS configuration to allow the control of each FQDN.

3.2.7. High risk status

The CA develops, maintains and implements documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements. In particular, the RA has carried out controls with databases of domain names that are suspected to be used for phishing activities and with CA's internal databases of revoked certificates for compromising reason or request of certificates which are suspected to be used for phishing activities.

3.3. Identification and validation of a key renewal request

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 validation of a current renewal

At the time of the first renewal, the verification of the identity of the Certificate Manager and the service is optional. It is left to the discretion of the CA who assumes responsibility for the validity of the information contained in the renewed certificate.

The validation of domain control by the applicant is always achieved via one of methods mentioned in chapter 3.2.6.

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

3.3.2. Identification and validation of a renewal after revocation

The verification of the Certificate Manager's identity is identical to the original request.

3.4. Identification and validation of a revocation request

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

- Mail: request completed and signed from the form of revocation of a certificate available on the website of Certigna http://www.certigna.fr;
- From the customer area of the Certigna website http://www.certigna.fr selecting the certificate to be revoked.

The mailing address of the revocation service is available on the website of Certigna http://www.certigna.fr

The paper request must include the following:

- The first and last name of the Certificate Manager;
- The email address of the Certificate Manager;
- The identity and function of the server;
- The reason for the revocation.

If the Certificate Manager is not the subscriber:

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

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

4. OPERATIONAL REQUIREMENTS ON THE LIFECYCLE OF CERTIFICATES

4.1. Certificate request

4.1.1. Origin of a certificate request

The certificate request must come from a legal representative of the entity, a Certification Agent duly mandated for this entity, with prior consent of the future Certificate Manager.

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

4.1.2. Process and responibilities for submitting a certificate request

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

The certificate application must contain the elements described in section 3.2.3.

4.2. Processing of a certificate request

4.2.1. Performance of the identification and request validation processes

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

- Validation of the server's identity (identity of the entity and function of the server);
- Validation of the identity of the entity;
- Validation of the identity of the signatory of the request (Certificate Manager, legal representative);
- Validation of the authorization to issue a certificate for the domain names requested;
- Validation of domain control;
- Validation of the files and the consistency of evidence presented;
- Assurance that the future Certificate Manager is informed of the applicable requirements to the use of the certificate.

All the operations mentioned above are carried out by the RA, but in the case of a request made via a DRA or a Certification Agent, the latter retransmits the request to the RA after making sure that the future Certificate Manager has been informed of the applicable requirements to the use of the certificate via the distribution of the Terms of Use, in addition

to their distribution operated by the CA.

The RA ensures that the request corresponds to the DRA operator's or of the Certification Agent's mandate. In all cases, the registration files are archived by the RA.

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

In compliance with the RFC 6844, controls are performed by the Registration Authority for every domain name present in "subjectAltName" extension of the certificate to issue and for which the "DNS CAA" option is enabled in associated DNS record. These controls allow to check that the CA is part of the authorities authorized to issue a certificate for these domains.
The following cases do not allow the CA to authorize the issuance of the certificate:

- The CAA DNS field is present, it contains an "issue" or "issuewild" tag and does not list Certigna as an authorized Certificate Authority;
- The CAA DNS field is present, it is designated as "critical" and the tag used is not supported by the CA (it is not an "issue" or "issuewild" tag);
- The zone is validly DNSSEC-signed and our DNS query times out.

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

4.2.2. Request acceptance or rejection

The certificate request is made, to reminder, in two separate stages:

- Sending electronic request (CSR);
- Acquisition of the request (receipt signed request files or their possibly dematerialized version).

An automatic process is implemented, when ordering a wildcard TLS/SSL certificate, to verify that the requested domain name is made up as "*.domain.tld". To consolidate this check, TLDs validated by ICANN are everyday automatically retrieved through the list on the https://publicsuffix.org website.

In addition, the verification of the domain name owner performed by the RA will in all cases lead to a rejection of the application as it is impossible to identify the owner of a domain name of type "*.tld". Applications with an invalid TLD or non-domain (E.g. *.co.uk) will therefore be systematically rejected.

CA don't issue certificates containing a new gTLD under consideration by ICANN. Prior to

issuing a Certificate containing an Internal Name with a gTLD that ICANN has announced as under consideration to make operational, the CA provides a warning to the applicant that the gTLD may soon become resolvable and that, at that time, the CA will revoke the Certificate unless the applicant promptly registers the domain name.

When a gTLD is delegated by inclusion in the IANA Root Zone Database, the Internal Name becomes a Domain Name, and at such time, a Certificate with such gTLD, which may have complied with these Requirements at the time it was issued, will be in a violation of these Requirements, unless the CA has verified the Subscriber's rights in the Domain Name. The provisions below are intended to prevent such violation from happening.

Within 30 days after ICANN has approved a new gTLD for operation, as evidenced by publication of a contract with the gTLD operator on [www.ICANN.org] the CA compare the new gTLD against the CA's records of valid certificates and ceases issuing Certificates containing a Domain Name that includes the new gTLD until after the CA has first verified the Subscriber's control over or exclusive right to use the Domain Name in accordance with Section 3.2.2.4. Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], the CA revokes each Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name.

After processing the request (control of the record, reconciliation and consistency check with the CSR), in case of rejection, the RA notifies the Certificate Manager, if applicable the operator of DRA, or the Certification Agent.

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

- The request files are incomplete (missing document);
- One of the documents is invalid (signature date more than 3 months, the date of validity of a document is exceeded, etc.);
- The request does not match with the mandate of the DRA operator or the Certification Agent;
- Electronic Request (CSR) is not consistent with the request files (information such as identity, function of the server or the name of the organization are different).

If accepted by the RA, after generation of the certificate by the CA, the RA sends a mail to The Certificate Manager to complete the certificate import.

4.2.3. Certificate preparation timeframe

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

4.3. Delivery of the certificate

4.3.1. Actions of the CA regarding the delivery of the certificate

After validation by the RA, the CA initiate the certificate generation process for the Certificate Manager.The conditions for generating keys and certificates and security

measures to meet are described in Chapters 5 and 6 below, including the separation of trusted roles (see section 5.2).

The generation and signing operations of the certificates issued by the root CA are performed in the same controlled circumstances as the generation of CA key pairs (see 6.1.1), with the presence of trusted roles authorized by the CA (at least a Security Officer, a Controller, a CA Administrator and secret bearers) and as part of "key ceremonies". The CA administrator performs the certificate generation and signing commands for the root CA in the presence of trusted roles that ensure that the practices comply with the security requirements and the defined script.

4.3.2. Notification by the CA of the certificate's delivery to the certificate manager

Complete and accurate certificate is made available to the Certificate Manager (on the customer area). The Certificate Manager authenticates on the customer area to accept the certificate or complete a paper form.

4.4. Acceptance of the certificate

4.4.1. Certificate acceptance procedure

Acceptance may be achieved in two ways:

- Either during the installation of the certificate, the Certificate Manager chooses to accept or not the certificate from the customer area. Notification of acceptance or rejection is automatically transmitted to CA.
- Either the Certificate Manager notifies the acceptance or rejection of the certificate by completing a paper form that will be sent by mail or delivered in a face to face.

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

4.4.2. Publication of the certificate

All certificates issued by the CA are not published.

4.4.3. A notification to the other entities of the delivery of the certificate

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

4.5. Uses of the key pair and of the certificate

4.5.1. Usage of the private key and certificate by the certificate manager

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

The authorised use of the ey pair and of the associated certificate is also described in the certificate itself, via the extensions relating to the key usage.

As part of the registration files, the Terms and condition are made known to the Certificate Manager or to the Certification Agent by the CA before entering in a contractual relationship. They are consulted prior to any online certificate request. They are available on the http://www.certigna.fr website. The conditions accepted by the Certificate Manager during the certificate request shall remain valid for the entire life of the certificate, or if necessary to the acceptance and signature by the Certificate Manager of new Terms and Conditions issued and made available to it by CA via http://www.certigna.fr website. Signed new Terms and Conditions must be provided by the Certificate Manager to the CA to be applicable.

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

Certificate users must strictly respect the permitted uses of certificates.
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). The Certificate Manager is committed, accepting the Terms and Conditions, to generate a new key pair for each request.

4.7. Delivery of a new certificate after change of the key pair

4.7.1. Possible causes for changing a key pair

The key pairs must be periodically renewed to minimize the possibilities of cryptographic attacks. Thus, the servers' key pairs, and corresponding certificates are renewed at least every three years (see chapter 6.3.2 validity period). Moreover, a key pair and a certificate can be renewed early, following the revocation of the application service.

4.7.2. Origin of a new certificate request

The triggering of the provision of a new certificate is initiated by the Certificate Manager (no existence of automated process). The entity, through its Certification Agent if necessary, can also be at the initiative of a new certificate request for an application service attached to it.

The generation of CSR remains under the responsibility of the Certificate Manager, the operator of RA or the operator of DRA. Import the new certificate is also carried out under the responsibility of the Certificate Manager.

4.8. Certificate modification

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

4.9. Revocation and suspension of certificates

4.9.1. Possible causes for a certificate's revocation

Server certificate

The following circumstances may cause the revocation of a server certificate:

- The Certificate Manager, the legal representative of the entity to which it belongs, if any Certification Agent or DRA operator request the revocation of the certificate (especially in the case of destruction or alteration of the server's private key and / or its support);
- The legal representative of the entity to which it belongs notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The Certificate Manager did not comply with applicable Terms and Conditions of the certificate or the CA obtains evidence that the certificate was misused;
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- The CA is made aware that a Certificate Manager has violated one or more of its material obligations under the Terms and Conditions;
- The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- The server information contained in its certificate is not in accordance with the identity or purpose in the certificate (eg, change in the identity or function of the server), this before the normal expiry of certificate;
- The Certificate Manager, the entity, if any Certification Agent or DRA operator, has not fulfilled its obligations under the CP or the CPS;
- The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- The CA signing the certificates is revoked (which results in the revocation of all valid certificates signed by the corresponding private key);
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CA within a given period of time).
- The final judgment of the server or the cessation of activity of the entity attached to the server and the Certificate Manager;

- An error (intentional or not) was detected in the registration files;
- The server's private key is suspected of being compromised, is compromised, lost or stolen (or possibly the activation data associated with the private key);
- For technical reasons (failure to send the certificate ...).

When the above circumstances occurring, and the CA has knowledge about that, the relevant certificate is revoked.

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 (eg, following an audit qualification or negative Compliance);
- Cessation of activity of the entity operating the component.

4.9.2. Origin of a revocation request

Server certificate

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

- The Certificate Manager;
- A legal representative of the entity to which is attached the server;
- If appriopriate, a Certification Agent;
- The CA;
- The RA or DRA operators.

The Certificate Manager is informed, particularly through the Terms and conditions accepted by him, persons or entities that may request a revocation of the certificate for which he is responsible.

Certificate of a component of the PKI

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. Processing procedure for a revocation request

Server certificate

The revocation request is made by the RA, a Certification Agent or the CA.
To a request made from the customer area, the user authenticates with his account and select the certificate to be revoked.
For a request by mail, the following information must be included in the certificate

revocation request (form to download on the website):
- The identity of the Certificate Manager;
- The email address of the Certificate Manager;
- The identity and function of the server;
- The reason of the revocation;

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

If the application is sent by mail, it must be signed by the subscriber (the signature is verified by the RA with that of the certificate request files).
If the request is made online, the empowerment of the person to perform this request is checked (authentication with the user account). In this case the person making the request can be:
- The Certificate Manager;
- If appriopriate, a Certification Agent;
- The CA;
- The RA or DRA operators.

The steps are:
- The applicant for revocation sends its request to the RA by mail or online;
- The RA authenticates and validates the revocation request to the requirements described in Chapter 3.4;
- The certificate serial number is registered in the CRL;
- In all cases, the Certificate Manager is notified of the revocation by email;
- The transaction is recorded in the event logs with, if necessary, sufficient information on the underlying causes that led to the revocation of the certificate;
- The CA does not publish in the CRL the causes of revocation.

Certificate of a component of the PKI

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 Certificate Managers 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. Timeframe granted to the certificate manager to formulate the revocation request

As soon as the Certificate Manager 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. Timeframe for the CA to process a revocation request

Certificate of the server

The revocation management function is available working hours for revocations online.
In all cases, the maximum period for processing revocation request is 24 hours. This delay means between the receipt of the authenticated revocation request and the provision of revocation information from users.

The maximum downtime per interruption (failure or maintenance) of the revocation management function is 2 hours on working days.

The maximum total duration of downtime per month for the revocation management function is 16 hours on working days.

Certificate of a component of the PKI

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 verification requirements applicable to the certificate users

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

4.9.7. CRL preparation frequency

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

4.9.8. Maximum timeframe for the publication of a CRL

A CRL is issued within a maximum of 30 minutes after its generation.

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

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

- http://wildca.ocsp.certigna.fr
- http://wildca.ocsp.dhimyotis.com

The OCSP responder meets the requirements of integrity, availability and deadline for the publication described in this CP. The Informations provided by OCSP responder for server

certificates are updated at maximum every 4 days, and OCSP responses are valid during 7 days. Revoked and expired certificates are maintained into CRL and OCSP responder.

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

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

4.9.10. Other available information means regarding revocations

Not applicable.

4.9.11. Specific requirements in case of compromise of the private key

The Certificates Manager 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 server certificate and private key that it is associated. Remember, this commitment is made upon acceptance of the Terms and Conditions.

4.9.12. Suspension of certificate

The certificates issued by the CA can not be suspended.

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 Certigna Root CA), ie to also check the signatures of the certificates in the chain, signatures guaranteeing the origin and integrity of the CRL/ARL and the state of the certificate of Certigna 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. Availability of the function

The information function on the status of certificates is available 24/7. This function has a maximum downtime per outage (failure or maintenance) of 4 hours (working days) and a maximum total duration of downtime per month 32 hours (working days).

If check online of the status of a certificate, the OCSP server response time to the received request is a maximum of 10 seconds. This is the time measured at the server (request received by the server response from the latter).

4.11. End of the relations between the certificate manager and the CA

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

4.12. Key escrow and recovery

The escrow of private keys is prohibited.

5. Non-technical security measures

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 measures

5.1.1. Geographical location and construction of the sites

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 supply 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. Vulnerability to water damage

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. Safekeeping of media

The informations 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 informations 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. Disposal of media

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

5.1.8. Off-site backups

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 informations.

5.2. Procedural security measures

5.2.1. Trusted roles

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

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

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

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 a 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. Security measures relative to the personnel

5.3.1. Required qualifications, skills and authorizations

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 verification 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. Initial training requirements

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

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

5.3.4. Continuity training requirements and frequency

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

5.3.5. Rotation frequency and sequence between the various duties

Not applicable.

5.3.6. Penalties in case of unauthorised 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. Requirements relative to the personnel of external providers

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 provided to the 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 to log

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 Certificate Managers).

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);
- Logs of operations carried out to process certificate requests, including those relating to “DNS CA” and “Certificate Transparency”;
- Validation / reject a certificate request;
- Certificate generation;
- Transmission certificates to Certificate Managers and, if appropriate, acceptances / explicit releases by Certificate Managers;
- 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 Certificate Managers.

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. Processing frequency for event logs

Cf. chapter 5.4.8

5.4.3. Retention period for event 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 event logs

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. Backup procedure of event logs

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. Collection system for event logs

Details are given in the CPS.

5.4.7. Notification of an event to the person responsible for this event

Not applicable.

5.4.8. Evaluation of vulnerabilities

The event logs are monitored once per working 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 2 weeks 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 month 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 to be archived

The 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 of the archives

Certificates request files

All accepted certificate registration files are archived seven years minimum 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 acceptance of the certificate by the Certificate Manager. 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 the real identity of Certificate Managers at an instant "t" on the designated server in the certificate issued by the CA in the certificate.

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

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

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

Event logs

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

5.5.3. Protection of archives

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. Backup procedure of archives

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

5.5.5. Data timestamping requirements

The data are dated according to Chapter 6.8.

5.5.6. Collection system of archives

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

5.5.7. Archive recovery and verification procedures

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. Change of the CA key

5.6.1. CA key

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

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

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

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. Procedure for reporting and processing incidents and compromising

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 Certificate Managers 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 procedure in case of corruption of IT resources

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 three years.

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

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

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

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

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

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

5.7.4. Business continuity capacities 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. End-of-life of the PKI

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.

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 Certificate Managers 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 (http://www.ssi.gouv.fr). The CA will inform him including any obstacles or additional delay encountered during the process of transfer or retirement.

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 Certificate Managers, 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 (http://www.ssi.gouv.fr) is immediately informed in case of cessation of trading of the CA.

6. Technical security measures

6.1. Generation and installation of key pairs

6.1.1. Generation of key pairs

CA key

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 one person with a trusted role within the PKI and in the presence of several witnesses;
- 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.

Keys generated by the Certificate Manager

The Certificate Manager is committed by contract, accepting the terms of use, to:
- generate the private key in a device which meets the requirements of Chapter 11.
- comply with requirements for the device he uses to generate and store the private key, if it is not provided by the RA.

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

Clés générées par l'AC

Key generation of servers takes place in a device compliant with the requirements of the chapter 11.

6.1.2. Transmission of the private key to the certificate manager

The private key is generated by the RA or the Certificate Manager and is transmitted securely.

In case where the private key is generated by the RA, the private key and/or activation data of private key are download securely by the Certificate Manager from Customer space and after the authentication of the Certificate Manager.

After the certificate issued, CA doesn't store and copy the private key.

6.1.3. Transmission of the public key to the CA

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

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

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 http://www.certigna.fr.

6.1.5. Size of the keys

CA key

- Root CA: Key pair RSA 4096 bits / Hash algorithm de hachage SHA-256 (256 bits)
- CA: Key pair RSA 4096 bits / Hash algorithm de hachage SHA-256 (256 bits)

Server's key

Key pair RSA 2048 bits / Hash algorithm de hachage SHA-256 (256 bits)

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

The parameters and signature algorithms implemented in cryptographic boxes, physical media and software are documented by CA. In the context of the use of RSA, the value of the public exponent is an odd number equal to 3 or more.

CA key

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

Server key

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

6.1.7. Key usage objectives

CA key

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

Server key

The use of the server's private key and the associated certificate is exclusively limited to the service defined at chapter 1.5.1.

6.2. Security measures for the protection of private keys and for cryptographic modules

6.2.1. Security standards and measures for cryptographic modules

Cryptographic modules of CA

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.

Devices for protecting server's private key

The device used by the CA or the Certificate Manager to protect the private key is compliant with the requirements of the chapter 11.

In the case where the CA provides the device to the Certificate Manager, directly or undirectly, CA ensure that:

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

6.2.2. Control of the private key by several persons

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

CA key

The CA private keys are never escrowed.

Server key

Private keys of servers are never escrowed.

6.2.4. Backup copy of the private key

CA key

The private key of the CA is saved:

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

Server key

Private keys of the servers are not the subject of any backup copy of the CA.

6.2.5. Private key archival

CA key

The private key of the CA is never archived.

Server key

Private server keys are archived in no case.
For private keys generated on cryptographic module, it is technically impossible to make a copy of these keys outside the HSM.

6.2.6. Transfer of the private key with the cryptographic module

For reminder, the server private keys are generated under the responsibility of the operator of RA, DRA, Certification Agent or Certificate manager.

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 in the cryptogaphic module

The CA private keys are generated and stored in a cryptographic module described in section 6.2.1 in accordance with the requirements of Section 6.2.4.

6.2.8. Private key activation method

CA key

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).

Server key

The Certificate Manager receives by phone (or in case of failure, by email) the certificate activation data (password to use the certificate) that will change at the time of acceptance of the certificate.

6.2.9. Private key deactivation method

CA key

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

The deactivation of a CA private key that must no longer be operational is performed by destructing this key in the cryptographic module. In the case where the cryptographic module is dedicated to this key, the module can then be tuned off in order to deactivate this key.

Server key

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

6.2.10. Private keys destruction method

CA key

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.

Server key

The Certificate Manager is the sole owner of the private key; it is the only one who can destroy (delete of the key or physical destruction of the device).

6.2.11. Cryptographic module security evaluation level

The level of assessment of the cryptographic module of the CA is specified in Chapter 10.
Server key pair protection devices are evaluated at a specified level in chapter 11.

6.3. Other aspects of the management of key pairs

6.3.1. Public key archival

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

6.3.2. Lifespan of the key pairs and certificates

The key pairs and certificates of servers covered have a term of 825 days maximum depending on the policy purchased.

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. Generation and installation of activation data

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.

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

The Certificate Manager defines from the customer area the data that will directly encrypt the generated key pair. This activation data is not retained by the CA.

6.4.2. Activation data protection

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.

Protection of activation data corresponding to the server private key

The Certificate Manager defines from the customer area the data that will directly encrypt the generated key pair. This activation data is not retained by the CA.

6.4.3. Other aspects related to activation data

Not applicable.

6.5. Security measures for IT systems

6.5.1. Technical security requirements specific to IT systems

A minimum level of 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. IT systems security evaluation level

Not applicable.

6.6. Security measures for the systems during their lifecycle

6.6.1. Security measures linked to the development of the systems

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. Measures related to security management

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

6.6.3. Security evaluation level of the systems lifecycle

Not applicable.

6.7. Network security measures

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. Timestamping/dating system

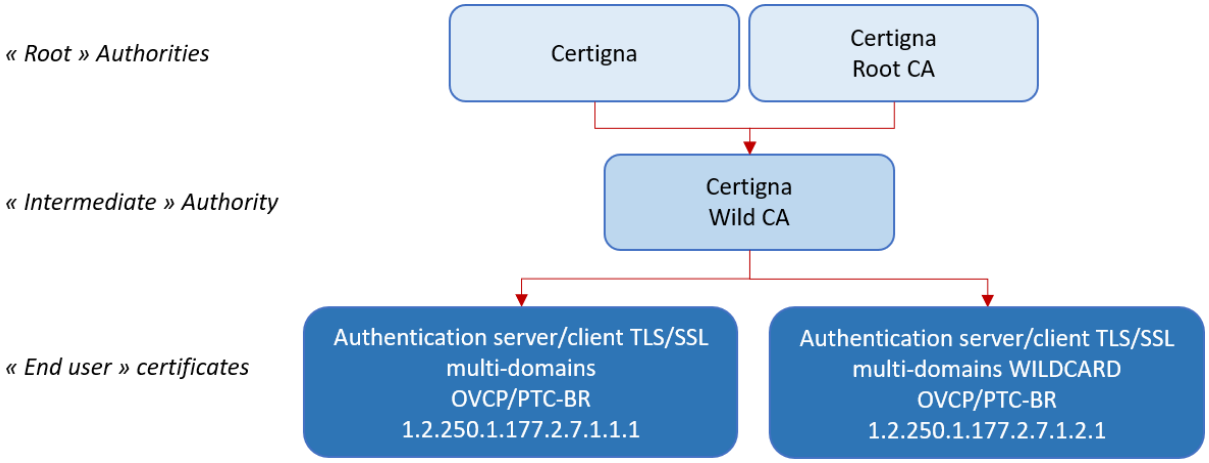
To ensure synchronization between different dating of events, the various components of the PKI synchronize their clocks with respect to a reliable source of UTC.

7. Profiles of the certificates and the CRL

The certificates and CRLs generated by the CA comply with ITU-T Recommendation X.509 v3 standard and RFC 5280.

7.1. Trusted hierarchy

The trusted hierarchy is composed with following certificates and authorities:



7.2. Profiles of Root Authorities certificates

These profiles are described by Certification Policies associated to Root Authorities and available at the following address: https://www.certigna.fr/autorites/.

7.3. Profile of the Intermediate Authority certificate

Two CA certificates have been issued for this Certification Authority: one signed by the old root CA « Certigna », other by the new root CA « Certigna Root CA ».

7.3.1. Basic fields

Field	Signed by "Certigna"	Signed by "Certigna Root CA"
Version	V3	
Serial Number	00 AB 07 8D EE DD DA C7 23 05 F5 ED 8C 50 84 F8 95	00 E3 72 E9 1B 19 B6 FC 27 E1 C4 31 8C C6 8D 09 EB
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	CN = Certigna Root CA OU = 0002 48146308100036 O = Dhimyotis C = FR
Subject DN	CN = Certigna Wild CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR	

7.3.2. Extensions

Extensions	Critical	Description
Subject Key Identifier	No	ID of the public key of CA
Authority Key Identifier	No	ID of the public key of Root CA
Certificate Policies	No	**OID=**1.2.250.1.177.2.0.1.1 **CPS**=https://www.certigna.fr/autorites/
Authority Information Access	No	**caIssuers**=http://autorite.certigna.fr/certignarootca.der **caIssuers**= http://autorite.dhimyotis.com/certignarootca.der
CRL Distribution Points	No	**URL**=http://crl.certigna.fr/certignarootca.crl **URL**=http://crl.dhimyotis.com/certignarootca.crl
Basic Constraints	**Yes**	**cA** = TRUE **PathLengthConstraint** = 0
Key Usage	**Yes**	Certificate signature CRL signature

7.4. Profile of the server certificate

7.4.1. Authentication Server/client – SSL/TLS – multi-domains

Field	Description
Version	V3
Serial Number	Unique serial number output from a CSPRNG (Cryptographically secure pseudorandom number generator) / Between 128 and 160 bits
Signature	ID of the CA signing algortihm SHA-256 RSA 4096
Subject Public Key Info	RSA 2048
Validity	Dates and times of activation and expiry of the certificate [Maximum 825 jours]
Issuer DN	CN = Certigna Wild CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR
Subject DN	CN = One FQDN of the SubjectAlternativeName Extension OU = ICD + identifier of the entity that owns the server registered in accordance with the laws and regulations OI = Information on the proof of identity of the entity O = Name of the entity that owns the server L = Locality of the entity C = Country of the competent authority to which the entity is officially registered

Extensions	Critical	Description
Authority Key Identifier	No	ID of the public key of the CA
Subject Key Identifier	No	ID of the public key of the server
Subject Alternative Name	No	FQDN of the different domains
Key Usage	**Yes**	Digital signature / Key Encipherment
Extended Key Usage	No	id-kp-serverAuth / id-kp-clientAuth
Certificate Policies	No	**OID=**1.2.250.1.177.2.7.1.1.1 **OID=**2.23.140.1.2.2 **CPS**= https://www.certigna.fr/autorites/
CRL Distribution Points	No	**URL**=http://crl.certigna.fr/wildca.crl **URL**=http://crl.dhimyotis.com/wildca.crl
Authority Information Access	No	**caIssuers**=http://autorite.certigna.fr/wildca.der **caIssuers**=http://autorite.dhimyotis.com/wildca.der **URL**=http://wildca.ocsp.certigna.fr **URL**=http://wildca.ocsp.dhimyotis.com
Basic Constraints	No	**cA** = FALSE
Certificate Transparency 1.3.6.1.4.1.11129.2.4.2	No	List of SCTs

7.4.2. Authentication Server/client – SSL/TLS – WILDCARD multi-domains

Field	Description
Version	V3
Serial Number	Unique serial number output from a CSPRNG (Cryptographically secure pseudorandom number generator) / Between 128 and 160 bits
Signature	ID of the CA signing algortihm SHA-256 RSA 4096
Subject Public Key Info	RSA 2048
Validity	Dates and times of activation and expiry of the certificate [Maximum 825 years]
Issuer DN	CN = Certigna Wild CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR
Subject DN	CN = One FQDN of the SubjectAlternativeName Extension OU = ICD + identifier of the entity that owns the server registered in accordance with the laws and regulations OI = Information on the proof of identity of the entity O = Name of the entity that owns the server L = Locality of the entity C = Country of the competent authority to which the entity is officially registered

Extensions	Critical	Description
Authority Key Identifier	No	ID of the public key of
Subject Key Identifier	No	ID of the public key of server
Subject Alternative Name	No	FQDN of the different domains with the syntax: *.<nameofthedomain>
Key Usage	**Yes**	Digital signature / Key Encipherment
Extended Key Usage	No	id-kp-serverAuth / id-kp-clientAuth
Certificate Policies	No	**OID=**1.2.250.1.177.2.7.1.2.1 **OID=**2.23.140.1.2.2 **CPS**= https://www.certigna.fr/autorites/
CRL Distribution Points	No	**URL**=http://crl.certigna.fr/wildca.crl **URL**=http://crl.dhimyotis.com/wildca.crl
Authority Information Access	No	**caIssuers**=http://autorite.certigna.fr/wildca.der **caIssuers**=http://autorite.dhimyotis.com/wildca.der **URL**=http://wildca.ocsp.certigna.fr **URL**=http://wildca.ocsp.dhimyotis.com
Basic Constraints	No	**cA** = FALSE
Certificate Transparency 1.3.6.1.4.1.11129.2.4.2	No	List of SCTs

7.4.3. OCSP Certificate

CA issues also OCSP certificates used for certificates information status function. OCSP responses conform with RFC 6960.

Field	Description	
Version	V3	
Serial Number	Unique serial number	
Signature	ID of the CA signing algortihm SHA-256 RSA 4096	
Subject Public Key Info	RSA 2048	
Validity	Dates and times of activation and expiry of the certificate	
Issuer DN	CN = Certigna Wild CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = DHIMYOTIS C = FR	
Subject DN	CN = OCSP Wild CA OU = 0002 48146308100036 O = DHIMYOTIS C = FR	
Extensions	**Critical**	**Description**
Authority Key Identifier	No	ID of the public key of
Subject Key Identifier	No	ID of the public key of server
Key Usage	No	Digital signature, Non-repudiation
Extended Key Usage	No	OCSPSigning
CRL Distribution Points	No	**URL**=http://crl.certigna.fr/wildca.crl **URL**=http://crl.dhimyotis.com/wildca.crl
Authority Information Access	No	**calssuers**=http://autorite.certigna.fr/wildca.der **calssuers**=http://autorite.dhimyotis.com/wildca.der **URL**=http:// wildca.ocsp.certigna.fr **URL**=http:// wildca.ocsp.dhimyotis.com
Ocsp No Check	No	
Basic Constraints	No	**cA** = FALSE

7.5. Profile of CRL

7.5.1. Basic fields

Champ	Description
Version	V2
Signature	ID of the CA signing algortihm SHA-256 RSA 4096
Issuer	CN = Certigna Wild CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR
This Update	Date of generation of CRL
Next Update	Date of next update of CRL (maximum: 7 days)
Revoked certificates	List of serial numbers of revoked certificates

7.5.2. Extensions

Field	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.

7.6. Pre-certificates

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

- ct.googleapis.com/rocketeer
- ct.googleapis.com/logs/xenon*20XX* (where *20XX* is the expiry year of the certificate)
- mammoth.ct.comodo.com
- yeti*20XX*.ct.digicert.com (where *20XX* is the expiry year of the certificate)

7.7. Processing certificates extensions by applications

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

7.7.1. 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.

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

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

- **Authority Information Access:** This extension identifies (with Method = OCSP) the location of OCSP server(s) providing information on the status of 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

- **Certificate Transparency:** This extension allows to control the registration of the certificate in the logs used for the “Certificate Transparency”.

8. Compliance audit and other evaluations

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 and/or circumstances of the evaluations

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 every three years by the CA.

8.2. Identities/qualifications of the evaluators

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

8.3. Relations between evaluators and the evaluated entities

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 the evaluations

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, ...).

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

The CA strictly controls the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist employed by the CA perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in

the period beginning immediately after the last sample was taken. The CA SHALL review each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and associated CPS.

8.5. Actions taken after the conclusions of the evaluations

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 the 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 line and legal issues

9.1. Rates

9.1.1. Rates for the delevery or renewal of certificates

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

9.1.2. Rates for accessing the certificates

Not applicable.

9.1.3. Tates for accessing information on the status and revocation of certificates

The access to certificate status information and revocation is free.

9.1.4. Rates 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. Reimbursement policy

Certificate commands can not be canceled once the command is being processed. Any certificate issued can not be subject to a reimbursement.

9.2. Financial liability

9.2.1. Insurance coverage

CA has purchased liability insurance policy adapted to information technologies.

9.2.2. Other ressources

Not applicable.

9.2.3. Coverage and guarantee regarding the user entities

Cf. chapter 9.9.

9.3. Confidentiality of personal data

9.3.1. Protection of personal data

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 servers;
- Activation Data associated with CA private key and of server;
- All the PKI secrets;
- Event logs of components of the PKI;
- The server registration records;
- The causes of revocation.

9.3.2. Information outside of the perimeter of confidential information

Not applicable.

9.3.3. Responsibilities in terms of the protection of confidential information

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

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 certificate managers to third parties in connection with legal proceedings. It also provides access to this information at certificate managers, certification agents and possibly DRA's operators in connection with the certificate managers.

9.4. Protection of personnel data

9.4.1. Personal data protection policy

Any collection and any use of personal data by the CA are made in strict compliance with legislation and regulations in force on the French territory, particularly in relation to the CNIL and the Article 226-13 (Ordinance No 2000-916 of 19 September 2000 Article 3 Official Journal of 22 September 2000 in force 1 January 2002) of the Penal Code. "the disclosure of secret information by a person who is depositary by state or profession or because of a function or a temporary mission, is punishable by one-year imprisonment and a fine of 15,000 Euros "

In accordance with the law n°78-17 of January 6, 1978 relating to data, files and liberties, 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 rights by sending an e-mail 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. Personal identifiable information

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 of non-personal nature

Not applicable.

9.4.4. Responsabilities in terms of the protection of personal data

Cf. legislation and regulations on French territory.

9.4.5. Notification et consent to use personal data

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

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

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 circumstances for the disclosure of personal information

Not applicable.

9.5. Intellectual and industrial 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. Contractual interpretations and guarantees

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. Certification authorities

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

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 certificate managers 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. Registration authority

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

9.6.3. Certificate manager

The Certificate manager has the duty to:

- Communicate accurate and updated informations at the request or renewal of the certificate;
- Protect the server private key under its responsibility by means appropriate to its environment;
- Protect his activation data and, where appropriate, implement them;
- Protect access to server certificates;
- Respect the conditions of use of the server private key and certificate;
- Inform Registration Authority of any changes to the information contained in the server certificate;
- Make, without delay, a request for server 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 Certificate Manager and the CA or its components is formalized by a commitment from the Certificate Manager to certify the accuracy of information and documents provided.

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

9.6.4. Certificate user

Third party users must:

- Check and maintain the use for which a certificate was issued;
- For each certificate of the certification chain, from the server 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. Other participants

Not applicable.

9.7. Guarantee limit

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

9.8. Limitations of liability

It is expressly understood that CA can not be held liable, or for any damage resulting from a fault or negligence of an acceptor and/or Certificate Manager, or injury caused by an external fact, particularly if:

- Using a certificate for an application other than the applications defined in Chapter 1.5.1 of this CP;
- Using a Certificate to secure another object that the identity of the server for which the certificate was issued;
- Using a revoked certificate;
- Using a Certificate beyond its maximum validity;
- Non-compliance by the entities concerned of the obligations defined in Sections 9.6.3 and 9.6.4 of this CP;
- External facts to issue the certificate, such as a failure of the application for which it may be used;
- Force majeure as defined by the French courts.

9.9. Indemnification

CA 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).

9.10. Duration and early end of validity of the CP

9.10.1. Duration of validity

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

9.10.2. Early end of validity

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

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

9.11. Individual notifications and communications between 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 to the CP

9.12.1. Amendment procedures

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 described at chapter 1.1.

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. A review and an update if necessary of this CP and the CPS are achieved once a year minimum.

9.12.2. Mechanism and information period for amendments

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

9.12.3. Circumstances in which the 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 (eg, increase in registration requirements of subjects, which can not 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 procedure

It is recalled that the conditions of use of the certificates issued by the CA are defined by this CP and / or the subscription contract for certification services defining the relationship between CA one hand and the Certificates managers of somewhere else.

The parties agree to attempt to resolve amicably any dispute that may occur between them, either directly or through a mediator, within 2 months of receiving mail with acknowledgment informing the dispute. Prospective mediation shall be borne equally by both parties. If necessary, the matter shall be referred to the Lille Commercial Court.

9.14. Competent jurisdictions

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

9.15. Compliance with legislation and regulations

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

9.16. Miscellaneous provisions

9.16.1. Overall agreement

This document contains all the provisions governing the PKI.

9.16.2. Transfer of activites

Cf. chapter 5.8.

9.16.3. Consequences of an invalid clause

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

In the event of a conflict between these Requirements 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. Application and waiver

Not applicable.

9.16.5. Force majeure

Are considered as force majeure those usually retained by the French courts, including the case of a compelling, insurmontable and unpredictable event.

9.17. Other provisions

Not applicable.

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 shall be:

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

11. Annexe 2: Security requirements for the devise used by the server

11.1. Security objectives requirements

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

- If the server key pair is generated by the device, guaranteeing that this generation is implemented exclusively by authorized users and guaranteeing the cryptographic sturdiness of the generated key pair;
- Ensuring the correspondence between the private key and the public key;
- the generated authentication cannot be falsified without knowing the private key;
- Detecting defects during the initialisation, customisation and operation phases, and ensuring secure techniques for the destruction of the private key in case of re-generation of the private key;
- Guaranteeing the private key's confidentiality and integrity;
- Ensuring the public key's authenticity and integrity when exported oustide of the device;
- Ensuring for the legitimate server the authentication function and the session symmetric keys encipherment function, and protecting the private key against any usage by third parties.
- Ensure the authenticity and the integrity of the session symmetric key, after encipherment, during its export from the device to the data encirpherment application.

11.2. Qualification requirements

Not applicable.