Certification Practice Statement
CERTIGNA ROOT CA

OID : 1.2.250.1.177.2.0.2
Version : 1.4
Date : 01/25/18
Authors : J. Allemandou
Classification : Public

CONTENTS

DOCUMENT HISTORY

Date	Version	Authors	Document change
10/19/15	1.0	R. DELVAL	Création
12/16/16	1.1	J. ALLEMANDOU	Revision of the graphique chart
04/17/17	1.2	J. ALLEMANDOU	Precisions about: - Version of applicable CAB/Forum BR (cf. 1.1), - RFC 5280 conformity (cf. 7), - Periodicity of CP/CPS reviews (cf. 9.12.1), - Management of conflicting requirements (cf. 9.16.3).
09/01/17	1.3	J. ALLEMANDOU	Addition of « ExpiredCertsOnCRL » extension (7.3.2)
01/25/18	1.4	J. ALLEMANDOU	Precisions about: - The Certigna email contact (cf. 1.6.2), - The form to report a certificate (cf. 2.3), - The periodicity of ARL and CRL update (cf. 2.4), - The physical access (cf. 5.1.2), - The qualification of CA cryptographic module (cf. 10.2).

1. INTRODUCTION

1.1. General presentation

Dhimyotis has a Certification Authority (CA) named "Certigna Root CA" to provide certificates to Intermediate CA.

This Certification Practice Statement (CPS) outlines the practices that CA applies in the delivery of its electronic certification services to users in accordance with its Certification Policy (CP) which it has committed to respect. The 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 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 CPS and the CP Requirements, those Requirements take precedence over this CPS.

1.2. Document identification

This CPS can be identified by the name of the « Certigna Root CA » and by its OID: 1.2.250.1.177.2.0.2. It describes the provisions implemented to meet the commitments made in the Certification Policy (CP) with the following OID: 1.2.250.1.177.2.0.1.

Usage(s)	OID
Signature of ARL and intermediate CA certificates	1.2.250.1.177.2.0.1

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
ANTS	National Agency for Secure Documents
ARL	Authority Revocation List
BCP	Business Continuity Plan
CA	Certification Authority
CAG	Certification Agent
CGU	Conditions of General Use
CNIL	National Commission for Computing and Liberties
CP	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 Subject
RSA	Rivest Shamir Adleman
SGMAP	General Secretariat for Modernisation of Public Action
SSL	Secure Sockets Layer
TA	Timestamping Authority
TLS	Transport Layer Security
TSP	Trust Service Provider
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

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 - 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.

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

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

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

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

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

1.4.3. Subjects

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

1.4.4. Certificate users

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

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

1.5. Use of the certificates

1.5.1. Applicable usage domains

Key pairs and certificates of Root CA

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

Key pairs and certificates of intermediate CA

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: CA certificates, ARL.

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

1.5.2. 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 Subjects and certificate users.

1.6. Management of the CP

1.6.1. Entity managing the CP

Dhimyotis 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 "Information security policy". The Security Committee shall ensure that the means used and described in the CPS meet these requirements as the approval process in place. A compliance check of the CPS compared to the CP is made through the internal and external audits for the CA qualification.

Any update request of the CPS also follows this process.
Any new approved version of the CPS is published without delay.

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

2.1. Entity in charge of providing information

Dhimyotis 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:

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

All publication services are hosted by the CA on several information systems to ensure a high availibility.

2.2. Information having to be published

The CA issues to the Subjects and certificate users:
- The CP;
- The Root CA certificate and valid intermediate CA certificate;
- The Certificate Revocation List (ARL / CRL);
- The CPS on specific request to Dhimyotis.

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 https://www.certigna.fr.

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

Publication of CPS

The CA issues, to the Subjects 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 Subjects and certificate users can access the CA certificates that are issued at the following addresses:
- https://www.certigna.fr/autorites,
- https://www.dhimyotis.com/autorites.

2.2.2. 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.
To ensure this availability and a quick recovery in case of disaster, several replicated sites have been implemented.
To detect and correct as soon as possible any incident occuring during the operation of one of these sites, the following measures have been deployed:
- Installation and operation of a monitoring software to monitor all the components of the technical plateform (servers, equipment, processes) and to send real-time alerts in case of detection of an incident;
- Development and implementation of scripts to automate and simplify load balancing from one site to another;
- Introduction of on-call during non-business hours;
- Subscription to a security monitoring service (24 hours a day);

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.

Access to the publishing system requires a double authentication: user session and the use of a user certificate stored in a dedicated device.

2.5. Published information access control

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 Certificate Subject.
It is built from the firstname and lastname of the subject specified in his identity document provided during the registration with the RA or the Certification Agent.

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

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

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

3.1.6. Identification, authentication and roles of registered trademarks

The CA is responsible for the uniqueness of the names used in its CA 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 Subject 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 Subject is verified through sending multiple emails that allow the Subject to access to his Certigna Customer account and certain activation data enabling him to recover and to use its certificate.

A strict control of the application files transmitted by a third person makes it possible to ensure that the latter is registred as delegated RA operator, or as a certification agent on behalf the entity to which the future CM belongs.

In both cases (request through a delegated RA or a certification agent), a control of the individual is carried out based on the transmitted informations.

3.2.1. Method for proving possession of the private key

CA ensures the detention of the private key by the Subject before certifying the public key. For this, the RA or the Subject 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).

The RA verifies beforehand the validity of the signature during the processing of the certificate requests received. This treatment is automated and therefore requires no human intervention. Any signature error, due in particular to the non-possession of the private key associated with the public key to be certified, is systematically detected and causes the rejection of the request.

3.2.2. Validation of an entity's identity

Cf. chapter 3.2.3

3.2.3. Validation of an individual's identity

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

3.2.4. 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).

3.3. 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

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

3.3.2. Identification and validation of a renewal after revocation

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

3.4. Identification and validation of a revocation request

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

The revocation request processing by the RA is detailed in the "Operational Revocation Request Procedure".

As with certificate applications, periodic audits may consider sample checks of revocation requests processed by the RA to ensure compliance with procedures.

4. 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.

4.1.2. Process and responbilities for submitting a certificate request

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

4.2. Processing of a certificate request

4.2.1. Performance of the identification and request validation processes

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

4.2.2. Request acceptance or rejection

Non-applicable.

4.2.3. Certificate preparation timeframe

The CA certificate request is established during the key ceremony; the certificate is generated within the hours following the request.

4.3. Delivery of the certificate

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

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

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

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

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

4.4. Acceptance of the certificate

4.4.1. Certificate acceptance procedure

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

4.4.2. Publication of the certificate

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

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

The representants of the different PKI components are informed of the delivery of a new CA certificate during or at the end of the key ceremony.

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

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

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 PKI automatically detects a certificate request with a public key that has already been certified. Any request for certification of a public key that has already been signed results in a failure with an explicit message at the level of the management module of the certificate requests of the RA.

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 CA key pairs, and corresponding certificates are renewed at least every twenty years (see chapter 6.3.2 validity period).

4.7.2. Origin of a new certificate request

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

4.8. Certificate modification

The modification of certificates is not recommended.

4.9. Revocation and suspension of certificates

4.9.1. Possible causes for a certificate's revocation

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 of the authority;
- 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 authority.

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

4.9.2. Origin of a revocation request

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.

The revocation mechanism is described in the "Operational revocation request procedure

4.9.3. Processing procedure for a revocation request

In case the CA decides to revoke the intermediate CA certificate (following the compromise of the private key of the CA), the latter informed by email all 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 ANSSI website (https://www.ssi.gouv.fr) is immediately informed in case of revocation of a certificate of the certificate chain.

The process is detailed in the "Cryptographic key management procedure" and in the "Component certificate management procedure".

4.9.4. Timeframe granted to the certificate manager to formulate the revocation request

As soon as 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

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

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

4.9.6. 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 is at the discretion of the user based on their availability and constraints in its implementation

4.9.7. CRL preparation frequency

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

4.9.8. Maximum timeframe for the publication of a CRL

An ARL 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

Not applicable for CA certificates.

4.9.10. Online verification requirements for certificate revocation by users of certificates

Cf. chapter 4.9.6

4.9.11. Other available information means regarding revocations

Not applicable.

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

The Certification Authority 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 Certification Authority 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.

4.9.13. Suspension of certificate

The CA certificates can not be suspended.

4.10. Certificate status service

4.10.1. Operational characteristics

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).

The publishing service activities are defined in the "Publishing Service Management Procedure".

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 2 hours and a maximum total duration of downtime per month 8 hours.

The replication of services on several information systems ensures automatic continuity of services in the event of a disaster. The CA also relies on its staff on-call during non-working hours to supervise the availability alerts for these functions.

4.11. 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. This CPS is established based on this risk analysis. The management of information security risks is described in the "IS Risk Management Procedure" and in the "IS Risk Management Form".

5.1. Physical security measures

5.1.1. Geographical location and construction of the sites

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

5.1.2. Physical access

A strict control of physical access to the components of PKI is performed, with access logging and video surveillance: the defined security perimeter around the systems hosting the PKI components is limited to people within a trusted role on this PKI.
Outside working hours, the implementation of physical and logical intrusion detection means strengthening the security of the PKI. In addition, any person (external service provider, etc.) entering in this physically secure area can not be left without the supervision of an authorized person.

Physical access to production centers is restricted through physical access control measures. The measures implemented are described in the "Safety Policy".

5.1.3. Power 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.

The production centers are equipped with inverters and generators. The measures implemented are described in the "Safety Policy".

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.

Means for the detection of water leaks are positioned in the production centers. The measures implemented are described in the "Safety Policy".

5.1.5. Fire prevention and protection

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

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

5.1.6. 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.

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

Specific measures are implemented to avoid compromise or theft of information. The assets corresponding to 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.

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

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.

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

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.

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

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.

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

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

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

5.2.2. Number of 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".

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

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.).

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

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.

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

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.

Professional skills are determined during recruitment and each year by Security Officiers.
The document "Roles, Responsibilities and Authorities", the "Personnel Management Procedure" and the "Staff Monitoring" document describe the measures implemented.

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.

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

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.

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

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.

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

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.

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

5.3.8. Documentation 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.

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

5.4. Audit logging procedures

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

5.4.1. Types of events 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 Subjects).

Specific events to different functions of the PKI are also logged:
- Events related to signing keys and CA certificates or activation data (generation, backup and recovery, revocation, destruction, disposal of media, …);
- Receiving a certificate request (initial and renewal);
- Validation / reject a certificate request;

- Certificate generation;
- Transmission certificates to Subjects and, if appropriate, acceptances / explicit releases by Subjects;
- Publish and update information related to the CA (CP / CPS, CA certificates, Terms and Conditions, etc.)
- Receipt of requests for revocation;
- Validation / reject a request for revocation;
- CRL generation and publication;
- Disposal of media containing personal information on Subscribers and Subjects.

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

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

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

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

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

The measures implemented are described in the « Logging Procedure » and the « Archive Procedure ».

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.

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

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

The "Clocks Synchronization Procedure" describes the measures implemented.

5.4.5. 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.

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

5.4.6. 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 work day to identify abnormalities related to failed attempts (access or instruction).

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

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

The measures implemented are described in the « Logging Procedure ».

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 Subject. During this period of enforceability of documents, the certificate request files can be submitted by the CA in any solicitation by the competent authorities. The files, completed by the words recorded by the RA or Certification Agents, is traceable to find at an instant "t" the real identity of Subject of the certificate issued by the CA in the certificate.

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

Certificates of Subjects and of CA and the CRL / ARL produced (respectively by the CA and Certigna 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 replication process guarantees the existence of a backup of the entire archive.

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

5.5.5. 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.

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

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.

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

5.6.2. Keys of the other components

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

5.7. Compromise and disaster recovery

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

These procedures are formalized as part of the implementation of Business Continuity Plans. In particular for the major risks identified, these plans address the immediate treatment in the case of strong constraints of service availability required by the PC. The operation of a supervisory monitor ensures that incidents are detected and taken into account in real time at both production sites.

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

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

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

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

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

Note: In the case of Certigna 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. The "Cryptographic Key Management Procedure", the "Incident Management Procedure" and the "Business Continuity Plans" describe the measures implemented.

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

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 Subjects if the proposed changes may affect the commitments and that, at least in the period of 1 month;
- It informs application managers listed in Chapter 1.4.1 the principles of the action plan for dealing with the cessation of business or to organize the transfer of activities;

- It carries information to the administrative authorities. In particular, contact of the ANSSI is warned (https://www.ssi.gouv.fr). The CA will inform him including any obstacles or additional delay encountered during the process of transfer or retirement.

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

Cessation of activity affecting the CA

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

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

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

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

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 two persons with a trusted role within the PKI and in the presence of several witnesses whom at least two are externed of the CA and are impartials;
- 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.

Key ceremony scripts and the distribution of secret shares are monitored and documented. The "Cryptographic Key Management Procedure" and the "HSM Management Procedure" describe the measures implemented.

6.1.2. 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 https://www.certigna.fr.

6.1.3. Size of the keys

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

6.1.4. 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.

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

6.1.5. Key usage objectives

The use of the private key of the CA and associated certificate is exclusively limited to signing CA certificates and ARL (cf. chapter 1.5).

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

6.2.1. Security standards and measures for cryptographic modules

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

The cryptographic modules used are BULL Trustway Proteccio. The "HSM Management Procedure" describes the measures implemented.

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

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

6.2.3. Private key escrow

The CA private keys are never escrowed.

6.2.4. Backup copy of the private 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.

6.2.5. Private key archival

The private key of the CA is never archived.

6.2.6. Transfer of the private key with the cryptographic module

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

6.2.7. Private key storage 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.

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

6.2.8. Private key activation method

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).

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

6.2.9. Private key desactivation method

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.

6.2.10. Private keys destruction method

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.

The measures implemented are described in the "Cryptographic Key Management Procedure".

6.2.11. Cryptographic module security evaluation level

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

6.3. Other aspects of the management of key pairs

6.3.1. Public key archival

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

6.3.2. Lifespan of the key pairs and certificates

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

6.4.2. Activation data protection

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

The secrets are stored in devices with limited access, in secure envelopes to detect any unauthorized opening and traced.

The "HSM Management Procedure" and the "Materiel Management Procedure" describe the measures implemented.

6.4.3. 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.

The "Safety Policy", the "Logical Access Control Policy", the "Security Charter", the "Firewall Management Procedure" describe the measures implemented.

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.

The description of the evolution context of the PKI is defined in the "Procedure for updating the technical platform".

Developments of the modules related to the exploitation of the components of the PKI are carried out in accordance with the rules and instructions enacted in the "Development Guide".

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.

The "Firewall Management Procedure", the "Monitoring Management Procedure" and the "Logical Access Control Policy" describe the measures implemented.

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.

The "Clocks Synchronization Procedure" describes the measures implemented.

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. The profiles are provided at chapter 7 of associated Certification.

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 deployment of certification services relative to means and rules mentioned in the CP and in the CPS.

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

The « Audit management procedure » and « Audit program » describe in detail the measures implemented.

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.

Internal audits are achieved by persons in the « controler » trusted role. Periodical controls are also achieved by Security Officers.

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.

For certification / qualification audits, the intervening entity is external and independent.

For internal audits, the selection of auditors and trusted roles is described in the document "Roles, Responsibilities and Authorities" and in the "Audit Management Procedure".

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, …).

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 Subjects 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

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

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

The "Classification and Information Handling Policy", the "Material Management Procedure" and the "Archive Procedure" describe the measures implemented.

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 Data Protection Act (Section 40 of the Act of 6 January 1978), Certigna PKI gives to Subjects a right for rectification of their personal data if data are inaccurate, incomplete or misleading at the time of they were collected. Certigna PKI is committed to correct as soon as it is informed that data is wrong.

Any correction of data can be requested by sending a mail to the registration authority concerned stating:
- Initial data transmitted during the certificate request;
- The corrections to perform;
- Any evidence (identity card photocopy).

The request must be dated and signed by the applicant and sent to the attention of CERTIGNA Head CNIL, 20 allée de la râperie, 59650 Villeneuve d'Ascq, FRANCE.

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 Subject to CA must not be disclosed or transferred to third parties except in the following circumstances: prior consent of the Subject, court order or other legal authorization.

9.4.6. 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.

Through this judicial requisition, the investigator is allowed to ask:
- The contact informations of the Certificates Manager (surname, first name, email address, etc.);
- The sites or e-mail addresses related to the entity concerned;
- The data relating to the certificate (s);
- Any element that may facilitate the decryption by the investigator of data encrypted by the Certificate Manager: information on the format used by the CA encryption utilities, etc.

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

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

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

9.6.2. Registration authority

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

9.6.3. 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 Subject certificate to the Certigna Root CA, verify the digital signature of the issuing CA on the certificate and check the validity of the certificate (validity date, revocation status);
- Check and respect the obligations of certificate users expressed in this CP.

9.6.4. Other participants

Not applicable.

9.7. Guarantee limit

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

9.8. Limit of liability

It is expressly understood that Dhimyotis can not be held liable, or for any damage resulting from a fault or negligence of an acceptor and/or Subject, 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 Subject 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. Compensation

Dhimyotis signed a contract of "liability insurance".

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 https://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 Certigna 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 is:
- 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.