Certigna

Certification Policy
CERTIGNA IDENTITY CA

OID :	1.2.250.1.177.2.3.1
Version :	1.9
Date :	02/26/19
Authors :	J. Allemandou
Classification :	Public

CERTIGNA is the trademark of DHIMYOTIS for the certification services

CONTENTS

DOCUMENT HISTORY **8**

1. INTRODUCTION **9**

1.1. General presentation 9
1.2. Document identification 9
1.3. Definitions and abbreviations 10
1.3.1. Abbreviations 10
1.3.2. Definitions 11
1.4. Entities involved in PKI 13
1.4.1. Certification authority 13
1.4.2. Registration authority 14
1.4.3. Subjects 14
1.4.4. Certificate users 15
1.4.5. Other participants 15
1.5. Use of the certificates 16
1.5.1. Applicable usage domains 16
1.5.2. Forbidden usage domains 17
1.6. Management of the CP 17
1.6.1. Entity managing the CP 17
1.6.2. Contact point 17
1.6.3. Entity determining the compliance of the CPS with the CP 17
1.6.4. CPS compliance approval procedures 17

2. RESPONSIBILITIES REGARDING THE PROVISION OF INFORMATION HAVING TO BE PUBLISHED **18**

2.1. Entity in charge of providing information 18
2.2. Information having to be published 18
2.2.1. Publication of documentation 18
2.2.2. Publication of CRL 19
2.2.3. Publication of ARL 19
2.3. Report a malicious or dangerous certificate 19
2.4. Publication timeframes and frequencies 19
2.4.1. Publication of documentation 19
2.4.2. Publication of CA certificates 19
2.4.3. Publication of CRL 19
2.4.4. Publication of ARL 19
2.5. Published information access control 20

3. IDENTIFICATION AND AUTHENTICATION **21**

3.1. Naming 21
3.1.1. Types of names 21
3.1.2. Necessary usage of explicit names 21
3.1.3. Anonymisation or pseudonymisation 21

3.1.4. Rules for interpreting the various types of names *21*
3.1.5. Uniqueness of the names *21*
3.1.6. Identification, authentication and roles of registered trademarks *21*
3.2. INITIAL IDENTITY VALIDATION 22
3.2.1. Method for proving possession of the private key *22*
3.2.2. Validation of an entity's identity *22*
3.2.3. Validation of an individual's identity *22*
3.2.4. Unverified informations *27*
3.2.5. Validation of the requester's authority *27*
3.3. IDENTIFICATION AND VALIDATION OF A KEY RENEWAL REQUEST 28
3.3.1. Identification and validation of a current renewal *28*
3.3.2. Identification and validation of a renewal after revocation *28*
3.4. IDENTIFICATION AND VALIDATION OF A REVOCATION REQUEST 28

4. OPERATIONAL REQUIREMENTS ON THE LIFECYCLE OF CERTIFICATES 29

4.1. CERTIFICATE REQUEST 29
4.1.1. Origin of a certificate request *29*
4.1.2. Process and responibilities for submitting a certificate request *29*
4.2. PROCESSING OF A CERTIFICATE REQUEST 29
4.2.1. Performance of the identification and request validation processes *29*
4.2.2. Request acceptance or rejection *30*
4.2.3. Certificate preparation timeframe *30*
4.3. DELIVERY OF THE CERTIFICATE 30
4.3.1. Actions of the CA regarding the delivery of the certificate *30*
4.3.2. Notification by the CA of the certificate's delivery to the Subject *30*
4.4. ACCEPTANCE OF THE CERTIFICATE 30
4.4.1. Certificate acceptance procedure *30*
4.4.2. Publication of the certificate *31*
4.4.3. CA notification to the other entities of the delivery of the certificate *31*
4.5. USES OF THE KEY PAIR AND OF THE CERTIFICATE 31
4.5.1. Usage of the private key and certificate by the Subject *31*
4.5.2. Usage of the public key and certificate by the certificate user *31*
4.6. CERTIFICATE RENEWAL 31
4.7. DELIVERY OF A NEW CERTIFICATE AFTER CHANGE OF THE KEY PAIR 32
4.7.1. Possible causes for changing a key pair *32*
4.7.2. Origin of a new certificate request *32*
4.8. CERTIFICATE MODIFICATION 32
4.9. REVOCATION AND SUSPENSION OF CERTIFICATES 32
4.9.1. Possible causes for a certificate's revocation *32*
4.9.2. Origin of a revocation request *33*
4.9.3. Processing procedure for a revocation request *34*
4.9.4. Timeframe granted to the Subject to formulate the revocation request *35*
4.9.5. Timeframe for the CA to process a revocation request *35*
4.9.6. Revocation verification requirements applicable to the certificate users *35*
4.9.7. CRL preparation frequency *35*
4.9.8. Maximum timeframe for the publication of a CRL *36*

4.9.9. Availability of an online system for verifying the revocation and status of certificates *36*
4.9.10. Other available information means regarding revocations *36*
4.9.11. Specific requirements in case of compromise of the private key *36*
4.9.12. Suspension of certificate *36*
4.10. CERTIFICATE STATUS SERVICE 36
4.10.1. Operational characteristics *36*
4.10.2. Availability of the function *37*
4.11. END OF THE RELATIONS BETWEEN THE SUBJECT AND THE CA 37
4.12. KEY ESCROW AND RECOVERY 37
4.12.1. Recovery policy for key escrow *37*
4.12.2. Identification and validation of a recovery request *38*

5. NON-TECHNICAL SECURITY MEASURES 39

5.1. PHYSICAL SECURITY MEASURES 39
5.1.1. Geographical location and construction of the sites *39*
5.1.2. Physical access *39*
5.1.3. Power supply and air conditioning *39*
5.1.4. Vulnerability to water damage *39*
5.1.5. Fire prevention and protection *39*
5.1.6. Safekeeping of media *39*
5.1.7. Disposal of media *40*
5.1.8. Off-site backups *40*
5.2. PROCEDURAL SECURITY MEASURES 40
5.2.1. Trusted roles *40*
5.2.2. Number of persons required per task *41*
5.2.3. Identification et authentication for each role *41*
5.2.4. Role requiring a separation of duties *41*
5.3. SECURITY MEASURES RELATIVE TO THE PERSONNEL 41
5.3.1. Required qualifications, skills and authorizations *41*
5.3.2. Background verification procedures *42*
5.3.3. Initial training requirements *42*
5.3.4. Continuity training requirements and frequency *42*
5.3.5. Rotation frequency and sequence between the various duties *42*
5.3.6. Penalties in case of unauthorised actions *42*
5.3.7. Requirements relative to the personnel of external providers *42*
5.3.8. Documentation provided to the personnel *42*
5.4. AUDIT LOGGING PROCEDURES 43
5.4.1. Types of events to log *43*
5.4.2. Processing frequency for event logs *44*
5.4.3. Retention period for event logs *44*
5.4.4. Protection of event logs *44*
5.4.5. Backup procedure of event logs *44*
5.4.6. Collection system for event logs *44*
5.4.7. Notification of an event to the person responsible for this event *44*
5.4.8. Evaluation of vulnerabilities *45*
5.5. RECORDS ARCHIVAL 45

5.5.1. Types of records to be archived ... *45*
5.5.2. Retention period of the archives ... *45*
5.5.3. Protection of archives ... *46*
5.5.4. Backup procedure of archives ... *46*
5.5.5. Data timestamping requirements ... *46*
5.5.6. Collection system of archives ... *46*
5.5.7. Archive recovery and verification procedures ... *46*
5.6. CHANGE OF THE CA KEY ... 46
5.6.1. CA key ... *46*
5.6.2. Keys of the other components ... *47*
5.7. COMPROMISE AND DISASTER RECOVERY ... 47
5.7.1. Procedure for reporting and processing incidents and compromising ... *47*
5.7.2. Recovery procedure in case of corruption of IT resources ... *47*
5.7.3. Recovery procedure in case of compromise of a component's private key ... *48*
5.7.4. Business continuity capacities after a disaster ... *48*
5.8. END-OF-LIFE OF THE PKI ... 48

6. TECHNICAL SECURITY MEASURES ... 50

6.1. GENERATION AND INSTALLATION OF KEY PAIRS ... 50
6.1.1. Generation of key pairs ... *50*
6.1.2. Transmission of the private key to the Subject ... *51*
6.1.3. Transmission of the public key to the CA ... *51*
6.1.4. Transmission of the CA's public key to the certificate users ... *51*
6.1.5. Size of the keys ... *51*
6.1.6. Verification of the generation and quality of the parameters of the key pairs ... *51*
6.1.7. Key usage objectives ... *52*
6.2. SECURITY MEASURES FOR THE PROTECTION OF PRIVATE KEYS AND FOR CRYPTOGRAPHIC MODULES ... 52
6.2.1. Security standards and measures for cryptographic modules ... *52*
6.2.2. Control of the private key by several persons ... *52*
6.2.3. Private key escrow ... *53*
6.2.4. Backup copy of the private key ... *53*
6.2.5. Private key archival ... *53*
6.2.6. Transfer of the private key with the cryptographic module ... *53*
6.2.7. Private key storage in the cryptogaphic module ... *53*
6.2.8. Private key activation method ... *54*
6.2.9. Private key desactivation method ... *54*
6.2.10. Private keys destruction method ... *54*
6.2.11. Cryptographic module security evaluation level ... *55*
6.3. OTHER ASPECTS OF THE MANAGEMENT OF KEY PAIRS ... 55
6.3.1. Public key archival ... *55*
6.3.2. Lifespan of the key pairs and certificates ... *55*
6.4. ACTIVATION DATA ... 55
6.4.1. Generation and installation of activation data ... *55*
6.4.2. Activation data protection ... *55*
6.4.3. Other aspects related to activation data ... *56*
6.5. SECURITY MEASURES FOR IT SYSTEMS ... 56
6.5.1. Technical security requirements specific to IT systems ... *56*

6.5.2. IT systems security evaluation level ... *56*
6.6. SECURITY MEASURES FOR THE SYSTEMS DURING THEIR LIFECYCLE ... 56
6.6.1. Security measures linked to the development of the systems ... *56*
6.6.2. Measures related to security management ... *57*
6.6.3. Security evaluation level of the systems lifecycle ... *57*
6.7. NETWORK SECURITY MEASURES ... 57
6.8. TIMESTAMPING/DATING SYSTEM ... 57

7. PROFILES OF THE CERTIFICATES AND THE CRL ... 58

7.1. TRUSTED HIERARCHY ... 58
7.2. PROFILES OF ROOT AUTHORITIES CERTIFICATES ... 58
7.3. PROFILE OF THE INTERMEDIATE CA CERTIFICATE ... 59
7.3.1. Basic fields ... *59*
7.3.2. Extensions ... *59*
7.4. PROFILE OF THE SUBJECT CERTIFICATE ... 60
*7.4.1. Encipherment * [Individual]* ... *60*
*7.4.2. Encipherment * [Company] [Administrative authority]* ... *61*
*7.4.3. Authentication and signature * [Individual]* ... *62*
*7.4.4. Authentication and signature * [Company] [Administrative authority]* ... *63*
7.5. PROFILE OF LCR ... 64
7.5.1. Basic fields ... *64*
7.5.2. Extensions ... *64*
7.6. PROCESSING CERTIFICATES EXTENSIONS BY APPLICATIONS ... 64
7.6.1. Criticality ... *64*
7.6.2. Extension description ... *65*

8. COMPLIANCE AUDIT AND OTHER EVALUATIONS ... 66

8.1. FREQUENCY AND/OR CIRCUMSTANCES OF THE EVALUATIONS ... 66
8.2. IDENTITIES/QUALIFICATIONS OF THE EVALUATORS ... 66
8.3. RELATIONS BETWEEN EVALUATORS AND THE EVALUATED ENTITIES ... 66
8.4. TOPICS COVERED BY THE EVALUATIONS ... 66
8.5. ACTIONS TAKEN AFTER THE CONCLUSIONS OF THE EVALUATIONS ... 66
8.6. COMMUNICATION OF THE RESULTS ... 67

9. OTHER BUSINESS LINE AND LEGAL ISSUES ... 68

9.1. RATES ... 68
9.1.1. Rates for the delevery or renewal of certificates ... *68*
9.1.2. Rates for accessing the certificates ... *68*
9.1.3. Tates for accessing information on the status and revocation of certificates ... *68*
9.1.4. Rates for other services ... *68*
9.1.5. Reimbursement policy ... *68*
9.2. FINANCIAL LIABILITY ... 68
9.2.1. Insurance coverage ... *68*
9.2.2. Other ressources ... *68*
9.2.3. Coverage and guarantee regarding the user entities ... *68*
9.3. CONFIDENTIALITY OF PERSONAL DATA ... 68
9.3.1. Protection of personal data ... *68*
9.3.2. Information outside of the perimeter of confidential information ... *69*

9.3.3. Responsibilities in terms of the protection of confidential information *69*
9.4. PROTECTION OF PERSONNEL DATA 69
9.4.1. Personal data protection policy *69*
9.4.2. Personal identifiable information *70*
9.4.3. Information of non-personal nature *70*
9.4.4. Responsabilities in terms of the protection of personal data *70*
9.4.5. Notification et consent to use personal data *70*
9.4.6. Conditions for the disclosure of personal information to legal or administrative authorities *70*
9.4.7. Other circumstances for the disclosure of personal information *70*
9.5. INTELLECTUAL AND INDUSTRIAL PROPERTY RIGHTS 70
9.6. CONTRACTUAL INTERPRETATIONS AND GUARANTEES 71
9.6.1. Certification authorities *71*
9.6.2. Registration authority *71*
9.6.3. Subject *72*
9.6.4. Certificate user *72*
9.6.5. Other participants *72*
9.7. GUARANTEE LIMIT 72
9.8. LIMIT OF LIABILITY 72
9.9. COMPENSATION 73
9.10. DURATION AND EARLY END OF VALIDITY OF THE CP 73
9.10.1. Duration of validity *73*
9.10.2. Early end of validity *73*
9.10.3. Effects of the end of validity and clauses remaining in effect *73*
9.11. INDIVIDUAL NOTIFICATIONS AND COMMUNICATIONS BETWEEN PARTICIPANTS 73
9.12. AMENDMENTS TO THE CP 74
9.12.1. Amendment procedures *74*
9.12.2. Mechanism and information period for amendments *74*
9.12.3. Circumstances in which the OID must be changed *74*
9.13. DISPUTE RESOLUTION PROCEDURE 74
9.14. COMPETENT JURISDICTIONS 74
9.15. COMPLIANCE WITH LEGISLATION AND REGULATIONS 75
9.16. MISCELLANEOUS PROVISIONS 75
9.16.1. Overall agreement *75*
9.16.2. Transfer of activites *75*
9.16.3. Consequences of an invalid clause *75*
9.16.4. Application and waiver *75*
9.16.5. Force majeure *75*
9.17. OTHER PROVISIONS 75

10. APPENDIX 1: SECURITY REQUIREMENTS FOR THE CA'S CRYPTOGRAPHIC MODULE 76

10.1. SECURITY OBJECTIVES REQUIREMENTS 76
10.2. QUALIFICATION REQUIREMENTS 76

11. ANNEXE 2: SECURITY REQUIREMENTS FOR THE DEVISE USED BY THE SUBJECT 77

11.1. SECURITY OBJECTIVES REQUIREMENTS 77
11.2. QUALIFICATION REQUIREMENTS 77

DOCUMENT HISTORY

Date	Version	Authors	Document change
03/05/15	1.0	Y. LEPLARD	Création
04/28/15	1.1	R. DELVAL	OCSP Response archiving
10/19/15	1.2	R. DELVAL	Addition of Authentication and signature certificates
02/16/16	1.3	R. DELVAL	Changing the calculation of the "serialNumber" field in DN
08/01/16	1.4	J. ALLEMANDOU	Precisions about E-mail address verification (cf. 3.2)
10/25/16	1.5	J. ALLEMANDOU	Addition of “msEFS” extension inside encirpherment certificates
12/16/16	1.6	J. ALLEMANDOU	Revision of the graphique chart et precisions about: - The level of conformity with ESTI specifications (cf. 1.1), - The semantic of the DN « serialNumber » field (cf. 3.1.5), - The withdrawal of « Certifié conforme » (cf. 3.2.3), - The terms of a current renewal (cf. 3.3.1), - The terms of acceptance of the certificate (cf. 4.4.1), - The role of Registration officier (cf. 5.2.1), - The minimum delay for archival (cf. 5.5.2), - The activation data transmission (cf. 6.4.1), - The CA certificates issued by two root CA (cf. 7), - The qualification requirement of the device (Cf. 11.2).
09/01/17	1.7	J. ALLEMANDOU	Addition of « ExpiredCertsOnCRL » extension (7.3.2)
01/25/18	1.8	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 possible causes for revocation (Cf. 4.9.1), - The physical access (cf. 5.1.2), - The diagram of the CA hierarchy (cf. 7), - The maximum longer of serial number (cf. 7), - The qualification of CA cryptographic module (cf. 10.2).
02/26/19	1.9	J. ALLEMANDOU	Precisions about: - The deadline for issuing certificates (see 4.2.3), - The practices for key escrow (see 4.12), - The protection of personal data (see 9.4.1).

1. INTRODUCTION

1.1. General presentation

Dhimyotis has a Certification Authority (CA) named "Certigna Identity CA" to provide certificates to natural persons.

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

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

This CP meets the requirements of

- the CP « *Certificats électroniques de personnes* » for auhtentication and signature, and encipherment usages at level * of the « Référentiel Général de Sécurité » (RGS) developed by the National Agency for the information systems security (ANSSI);
- The eIDAS Regulation (EU) N°910/2014 at ETSI EN 319 411-1 LCP level;

1.2. Document identification

This PC can be identified by the name of the « Certigna Identity CA » and by its OID: 1.2.250.1.177.2.3.1

Usage(s)	RGS	ETSI / Level	Type	OID
Encipherment	*	EN 319 411-1 LCP	Individual	1.2.250.1.177.2.3.1.3.1
Encipherment	*	EN 319 411-1 LCP	Professionnal	1.2.250.1.177.2.3.1.1.1
Authentication and signature	*	EN 319 411-1 LCP	Individual	1.2.250.1.177.2.3.1.4.1
Authentication and signature	*	EN 319 411-1 LCP	Professionnal	1.2.250.1.177.2.3.1.2.1

1.3. Definitions and abbreviations

1.3.1. Abbreviations

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

AA	Administrative Authority
ANSSI	National Agency for information systems security
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).

Encipherment
- Recovery management function - Recovery and escrow function

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 natural person. It is responsible for the use of the certificate (and associated private key) and the entity for which he uses the certificate and with which it maintains a contractual, hierarchical or regulatory.

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

In the rest of the document the term "entity" is used to mean a company or an administration. The name "business" includes undertakings in the broadest sense, ie all legal persons of private law firms, associations and independent artisans and workers.

1.4.4. Certificate users

Encipherment
- An online service that uses an encryption device to encrypt data or a message to the certificate subject; - A person who transmits an encrypted message for the certificate subject.

Authentication and Signature
- An online service that uses a certificate and an authentication verification device to validate an access request made by the certificate subject in the context of an access control or to authenticate the origin of a message or data transmitted by the subject of the certificate; - An online service that uses a signature verification device to verify the electronic signature on the data or a message of the subject of the certificate; - A user recipient of a message or data and who uses a certificate and an authentication verification device to authenticate the origin. - A user who electronically sign a document or a message; - A user recipient of a message or data and who uses a certificate and a signature verification device to verify the electronic signature by the subject of the certificate on this message or data.

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

1.4.5. Other participants

CA also relies on DRA to outsource some of the functions of the RA. An operator of DRA has the power to:

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

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

The commitments of the DRA operator against CA are specified in a written agreement with the responsible entity of the operator and in the commitment letter to be signed by the latter. Both documents include state that the operator must perform impartial and scrupulous identity checks and possible future Subject attributes, and respect the parts of the CP and CPS incumbent on him.

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

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

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

The commitments of the Certification Agent in respect of the CA are specified in a written agreement with the entity responsible of the Certification Agent and in the commitment letter to be signed by the Certification Agent. Both documents specify that the Certification Agent must make impartial and scrupulous identity checks and possible future Subjects attributes, and respect the parts of the CP and CPS incumbent on him.

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

1.5. Use of the certificates

1.5.1. Applicable usage domains

Key pairs and certificates of the subjects

Encipherment
- Decrypt: using its private key, a subject decrypts the data that were transmitted through electronic exchanges, encrypted with his public key; - Encryption: using the recipient's public key, a number of individual data.

Authentication and Signature
- Authentication of subjects on remote Subjects or to other people. It may be authentication in the framework of an access control to a Subject or an application, or authentication of data's origin as part of the electronic mail. - Data electronic signature. Such electronic signature brings, besides the authenticity and integrity of signed data, the manifestation of consent of the signatory for the content of these data.

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

Key pairs and certificates of CA and of components

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

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

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

1.5.2. 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. To this end, it publishes to the Subjects, Certification Agent and potential users the Terms of use that can be found on the site https://www.certigna.fr before any request or use of a certificate.

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:

- Web Servers :
  - http://crl.certigna.fr/identityca.crl
  - http://crl.dhimyotis.com/identityca.crl
- OCSP Servers :
  - http://identityca.ocsp.certigna.fr
  - http://identityca.ocsp.dhimyotis.com

2.2. Information having to be published

The CA issues to the Subjects and certificate users:

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

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

2.2.1. 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.

2.4.3. Publication of CRL

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

2.4.4. Publication of ARL

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

2.5. Published information access control

Access to information published to users is free.

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

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of names

In each certificate conform wih X.509 Standard, the issuing CA (corresponding to the "issuer" field) and Subject ("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

The combination of the country, the name and the email address of the Certificate Subject uniquely identifies the Certificate Subject.

The serialNumber attribute, unique value assigned to each certificate issued by the CA and present in the DN, also ensures the uniqueness of the DN. This field is made up from a unique random number generated by the CA and begin with a letter which indicates certificate’s usage(s):

- “I” for “Authentication” and “Signature”,
- "C” for “Encirpherment” only,

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

3.1.6. Identification, authentication and roles of registered trademarks

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

3.2. Initial identity validation

Registering a 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.

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 generates the key pair in a device compliant with the requirements of the chapter 11, and provides to the CA the proof of possession of the private key by signing his certificate request (Certificate signing request with the PKCS # 10 format).

3.2.2. Validation of an entity's identity

Cf. chapter 3.2.3

3.2.3. Validation of an individual's identity

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

The registration of the future Subject requires the verification of:

- the "natural person" identity **[Individual][Company][Administrative authority]**
- the "legal person" identity of the entity **[Company] [Administrative authority]**
- the attachment of the future subject with the entity **[Company] [Administrative authority]**

Registration of Subject [Individual] without Certification Agent

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

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

Official identification document of the Subject	
Subject	A photocopy of an identity official document valid of the Subject with an ID photo. *Eg.: national identity card, passport or residence permit*
Date	Piece valid at the time of registration

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

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

Registration of Subject [Company][Administrative authority] without Certification Agent

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

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

Official identification document of the Subject	
Subject	A photocopy of an identity official document valid of the Subject or a professional card issued by an administrative authority (if that authority maintaining a register of identities ensuring the link between the agent and the professional card) with an ID photo (including national identity card, passport or residence permit) or a reference to the administrative file of the agent.
Date	Piece valid at the time of registration

Official identification document of the legal representative	
Subject	A photocopy of an identity official document valid of the legal representative or a professional card issued by an administrative authority (if that authority maintaining a register of identities ensuring the link between the agent and the professional card) with an ID photo (including national identity card, passport or residence permit) or a reference to the administrative file of the agent.
Date	Piece valid at the time of registration

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

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

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

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

Registration of a Certification Agent [Company][Administrative authority]

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

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

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

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

Official identification document of the Certification Agent	
Subject	A photocopy of an identity official document valid of the Certification Agent or a professional card issued by an administrative authority (if that authority maintaining a register of identities ensuring the link between the agent and the professional card) with an ID photo (including national identity card, passport or residence permit) or a reference to the administrative file of the agent.
Date	Piece valid at the time of registration

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

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

Authentication of the Certification Agent by the RA is achieved by sending the paper file by post, accompanied by a photocopy of the identity documents of each of the signatories of the documents (legal representative, Certification Agent).

This authentication can also be done in dematerialized form if the various supporting documents are signed using an electronic signature process complying with the requirements of the level * and that the signature is verified and valid at the time of the registration. If the Certification Agent is not equipped with a certificate of level * or higher, the files can not be sent in dematerialized form. In this case, each file will be validated only after receipt of the original documents by mail.

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

Registration of a Subject via a Certification Agent [Company][Administrative authority]

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

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

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

Official identification document of the Subject	
Subject	A photocopy of an identity official document valid of the Subject or a professional card issued by an administrative authority (if that authority maintaining a register of identities ensuring the link between the agent and the professional card) with an ID photo (including national identity card, passport or residence permit) or a reference to the administrative file of the agent.
Date	Piece valid at the time of registration

Authentication of the Subject by the Certification Agent is achieved by sending the paper file by post, accompanied by a photocopy of the identity documents of each of the signatories of the documents (legal representative, Certification Agent).

This authentication can also be done in dematerialized form if the various supporting documents are signed using an electronic signature process complying with the requirements of the level * and that the signature is verified and valid at the time of the registration.

During the transmission of the request forms by the Certification Agent, he must be authenticated to the RA by initials of the Certification Agent affixed to the various pages of the forms and documents, supplemented by his signature on the main pages.

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

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

At the time of the first renewal, the verification of the identity of the Subject is optional. It is left to the discretion of the CA who assumes responsibility for the validity of the information contained in the renewed certificate. At the next renewal, the RA identifies the Subject through the same procedure as for the initial registration.

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

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

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

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

The paper request must include the following:
- The first and last name of the Subject;
- The email address of the Subject;
- The identity of the Subject;
- The reason for the revocation.

If the Subject is not the subscriber:

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

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

4. OPERATIONAL REQUIREMENTS ON THE LIFECYCLE OF CERTIFICATES

4.1. Certificate request

4.1.1. Origin of a certificate request

For [Company] and [Admniistrative authority], the certificate request must come from a legal representative of the entity, a Certification Agent duly mandated for this entity, with prior consent of the future Subject.

4.1.2. Process and responibilities for submitting a certificate request

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

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

4.2. Processing of a certificate request

4.2.1. Performance of the identification and request validation processes

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

- Validation of the Subject's identity;
- Validation of the identity of the entity;
- Validation of the identity of the signatory of the request (Subject, legal representative);
- Validation of the files and the consistency of evidence presented;
- Assurance that the future Subject is informed of the applicable requirements to the use of the certificate.

The identity of the future Subject and the legal representative is approved if the supporting documents provided are valid at the date of receipt.

In the case of a request with a DRA operator, he forwards the files to the RA after performing the above operations. The RA then ensures that the request corresponds to the mandate of the DRA operator.

In the case of request with a Certification Agent, he forwards the files to the RA after performing some of the above operations (validating the identity of the future Subject, validation of the files, insurance about the knowledge of Terms and Conditions). The RA then ensures that the request corresponds to the mandate of the Certification Agent.
In all cases, the registration files are archived by the RA.

4.2.2. Request acceptance or rejection

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

The justification for any refusal is made by the RA specifying the cause:
- The request files are incomplete (missing document);
- One of the documents is invalid (signature date more than 3 months, the date of validity of a document is exceeded, etc.);
- The request does not match with the mandate of the DRA operator or the Certification Agent.

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

4.2.3. Certificate preparation timeframe

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

4.3. Delivery of the certificate

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

After validation by the RA, the CA initiate the certificate generation process for the Subject.

The conditions for generating keys and certificates and security measures to meet are described in Chapters 5 and 6 below, including the separation of trusted roles.
(See section 5.2).

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

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

4.4. Acceptance of the certificate

4.4.1. Certificate acceptance procedure

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

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

its revocation.

4.4.2. Publication of the certificate

Certificates issued by the CA are not published.

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

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

4.5. Uses of the key pair and of the certificate

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

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

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

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

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

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

4.6. Certificate renewal

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

If the Subject generates his key pair, he is committed, accepting the Terms and Conditions, to generate a new key pair for each request.

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

4.7.1. Possible causes for changing a key pair

The key pairs must be periodically renewed to minimize the possibilities of cryptographic attacks. Thus, the Subjects' key pairs, and corresponding certificates are regularly renewed (see chapter 6.3.2 validity period).

Moreover, a key pair and a certificate can be renewed early, following the revocation of the Subject certificate.

4.7.2. Origin of a new certificate request

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

4.8. Certificate modification

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

4.9. Revocation and suspension of certificates

4.9.1. Possible causes for a certificate's revocation

Subject certificate

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

- The Subject information contained in its certificate is not in accordance with the identity or purpose in the certificate (eg, change in the identity), this before the normal expiry of certificate;
- The Subject did not comply with applicable Terms and Conditions of the certificate;
- The Subject, the entity, if any Certification Agent or DRA operator, has not fulfilled its obligations under this CP;
- The Subject, the legal representative of the entity to which it belongs, if any Certification Agent or DRA operator request the revocation of the certificate (especially in the case of destruction or alteration of the Subject's private key and / or its support);
- The legal representative of the entity to which it belongs notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The Subject did not comply with applicable Terms and Conditions of the certificate or the CA obtains evidence that the certificate was misused;
- The CA is made aware that a subject has violated one or more of its material obligations under the Terms and Conditions;
- The service information contained in its certificate is not in accordance with the identity or purpose in the certificate, this before the normal expiry of certificate;
- The Subject, the entity, if any Certification Agent or DRA operator, has not fulfilled its obligations under the CP or the CPS;

- The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- The CA signing the certificates is revoked (which results in the revocation of all valid certificates signed by the corresponding private key);
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.
- The die of the Subject or the cessation of activity of the entity attached to the Subject;
- An error (intentional or not) was detected in the registration files;
- The Subject's private key is suspected of being compromised, is compromised, lost or stolen (or possibly the activation data associated with the private key);
- For technical reasons (failure to send the certificate ...).

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

Certificate of a component of the PKI

The following circumstances may cause the revocation of a certificate of a component of the PKI:
- Suspicion of compromise, compromise, loss or theft of the private key;
- Feature change the PKI decision following the detection of non-compliance of the procedures applied within the component with those announced in this CP (eg, following an audit qualification or negative Compliance);
- Cessation of activity of the entity operating the component.

4.9.2. Origin of a revocation request

Subject certificate

Individuals or entities may request revocation of a Subject certificate are:
- The Subject;
- A legal representative of the entity to which is attached the Subject;
- If appriopriate, a Certification Agent;
- The CA;
- The RA or DRA operators.

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

Certificate of a component of the PKI

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

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

4.9.3. Processing procedure for a revocation request

Subject certificate

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

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

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

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

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

Certificate of a component of the PKI

In case the CA decides to revoke the intermediate CA certificate (following the compromise of the private key of the CA), the latter informed by email all Subjects that their certificates are

no longer valid because one of the certificates in the certificate chain is no longer valid. This information will also be relayed directly from the entities and where appropriate their Certification Agent.

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

4.9.4. Timeframe granted to the Subject to formulate the revocation request

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

4.9.5. Timeframe for the CA to process a revocation request

Subject certificate

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

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

The maximum downtime per interruption (failure or maintenance) of the revocation management function is 1 hour.

The maximum total duration of downtime per month for the revocation management function is 4 hours.

Certificate of a component of the PKI

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

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

4.9.6. Revocation verification requirements applicable to the certificate users

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

4.9.7. CRL preparation frequency

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

4.9.8. Maximum timeframe for the publication of a CRL

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

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

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

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

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

4.9.10. Other available information means regarding revocations

Not applicable.

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

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

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

4.9.12. Suspension of certificate

The certificates issued by the CA can not be suspended.

4.10. Certificate status service

4.10.1. Operational characteristics

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

The information based on the status of certificates makes available to certificates users a free consultation mechanism CRL/ARL. These CRL/ARL are in CRL V2 format published on the

publication website (available with the HTTP protocol).

4.10.2. 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.

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

4.11. End of the relations between the Subject and the CA

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

4.12. Key escrow and recovery

The escrow of CA private keys is prohibited.

Encipherment
Private keys of the subjects are escrowed.

4.12.1. Recovery policy for key escrow

Escrow request

Encipherment
The escrow of the certificate and the key pair are automatically made for a period of ten (10) years from the date of issuance of the certificate. The Subject may, at the time of the order, ask to change the retention period or do not to benefit from the escrow.

Processing an escrow request

Encipherment
The certificate of encipherment and the associated private key are the subject of a escrow allowing their recovery in case of loss. The duration of the escrow is ten (10) years from the date of issue of the certificate unless explicitly requested by the Subject when requesting the certificate. Each escrowed private key is uniquely identified and unequivocally by the serial number of the corresponding certificate.

Origin of a escrow request

Encipherment
In addition to the subjects and entities authorized by law to access private keys escrowed by a CA, the only legal representative of the entity or explicitly designated person (by name or by position) by the legal representative of the entity may request the recovery of a private key of a given subject.

4.12.2. Identification and validation of a recovery request

Encipherment
The identity of the subject for a recovery must be validated, except in special cases of the entities authorized by law, by the RA following the same requirements as the initial validation of the identity of a certificate applicant (Cf. chapter 3.2). The request for recovery must include at least the reason for the recovery of the private key and the information to identify the private key to recover. The RA ensures that the applicant is one of the persons entitled to seek recovery of the relevant key.

Processing a recovery request

Encipherment
Following the identification and validation of the request for recovery, a RA operator shall provide the private key to the applicant, with equivalent safety to the delivery of the private key when generating for the certificate subject The pieces of the recovery request are archived by the RA.

Destruction of key escrowed

Encipherment
At the end of the retention period of an escrowed key, all copies of that key held by CA are reliably destroyed.

Availability of escrow and recover functions

Encipherment
The recovery management function is available during business hours. In all cases, the maximum period for processing a request for recovery is 72 hours. This delay means between the receipt of the authenticated request for recovery and the provision of the private key to the applicant.

5. Non-technical security measures

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

5.1. Physical security measures

5.1.1. Geographical location and construction of the sites

These informations are specified in the CPS.

5.1.2. Physical access

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

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

5.1.3. Power supply and air conditioning

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

5.1.4. Vulnerability to water damage

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

5.1.5. Fire prevention and protection

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

5.1.6. Safekeeping of media

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

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

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

5.1.7. Disposal of media

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

5.1.8. Off-site backups

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

5.2. Procedural security measures

5.2.1. Trusted roles

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

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

The different roles are defined in the description of functions specific to any entity operating a component of the PKI on the principles of separation of duties and least privilege. These roles determine the sensitivity of the functions, depending on responsibilities and access levels, background checks and employee training and awareness.
Measures are in place to prevent equipment, information, media and software relating to CA services are removed from the site without permission.

5.2.2. Number of persons required per task

For reasons of availability, each task must be performed by at least two people.
At a minimum, each task is assigned to two different people:

- System administrator ;
- Operator.

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

5.2.3. Identification et authentication for each role

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

5.2.4. Role requiring a separation of duties

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

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

5.3. Security measures relative to the personnel

5.3.1. Required qualifications, skills and authorizations

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

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

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

5.3.2. Background verification procedures

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

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

5.3.3. Initial training requirements

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

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

5.3.4. Continuity training requirements and frequency

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

5.3.5. Rotation frequency and sequence between the various duties

Not applicable.

5.3.6. Penalties in case of unauthorised actions

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

5.3.7. Requirements relative to the personnel of external providers

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

5.3.8. Documentation provided to the personnel

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

5.4. Audit logging procedures

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

5.4.1. Types of events to log

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

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

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

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

Encipherment
- The escrow of a Subject private key; - The reception of a recovery request; - The validation/reject of a recovery request; - The recovery of a private key; - The provision of a recovered private key to the recovery requester.

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

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

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

5.4.2. Processing frequency for event logs

Cf. chapter 5.4.8

5.4.3. Retention period for event logs

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

5.4.4. Protection of event logs

Only members dedicated CA can process these files.

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

5.4.5. Backup procedure of event logs

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

5.4.6. Collection system for event logs

Details are given in the CPS.

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

Not applicable.

5.4.8. Evaluation of vulnerabilities

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

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

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

5.5. Records archival

5.5.1. Types of records 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.

Encipherment
The private key recovery requests d'une clé privée are archived by CA until 't' = 't_0' + 10 years, with 't_0' is the achiving date of the certificate request associated to the recovered private key.

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

5.5.5. Data timestamping requirements

The data are dated according to Chapter 6.8.

5.5.6. Collection system of archives

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

5.5.7. Archive recovery and verification procedures

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

Data about contractors can be retrieved on their request.

5.6. Change of the CA key

5.6.1. CA key

The CA can not generate a certificate for which the end date is later than the expiration date

of the certificate corresponding to the CA. For this, the validity period of the CA certificate must be higher than the certificate that it signs. Knowing the date of expiry of the certificate, renewal must be requested within a delay at least equal to the lifespan of the certificates signed by the corresponding private key.

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

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

5.6.2. Keys of the other components

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

5.7. Compromise and disaster recovery

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

5.7.1. Procedure for reporting and processing incidents and compromising

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

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

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

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

5.7.2. Recovery procedure in case of corruption of IT resources

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

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

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

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

Similarly, all valid 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.

5.7.4. Business continuity capacities after a disaster

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

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

5.8. End-of-life of the PKI

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

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

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

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

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

- It ensures the continuity of the archive service, especially certificates and registration records;
- It ensures the continuity of the revocation service, in accordance with the availability

requirements for its functions under this CP;
- It informs 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.

Cessation of activity affecting the CA

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

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

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

6. Technical security measures

6.1. Generation and installation of key pairs

6.1.1. Generation of key pairs

CA key

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

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

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

The ceremony took place following a predefined script:
- It takes place under the control of at least one person with a trusted role within the PKI and in the presence of several witnesses;
- Witnesses testify in an objective and factual manner, the order of the key ceremony in relation to previously defined script.

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

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

Keys generated by the Subject

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

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

Keys of the Subjects generated by the CA

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

6.1.2. Transmission of the private key to the Subject

In the case where the private key is generated by the CA, the athentication of the Subject is achieved by the RA in compliance with chapter 3.2.3 requirements and previously the key pair transmission. After request validation and Certificate subject authentication, the key pair is transmised to the Subject through the send of the device compliant with chapter 11 by secured mail. Activation data of the device are not transmited in this mail.

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

6.1.3. Transmission of the public key to the CA

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

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

The issuance of public key of the CA, which allows all those who need to validate a certificate issued by the CA under the CP, is made by means ensuring integrity and authentication of the public key.
The public key of CA is broadcast in a certificate signed by the Certigna Root CA. The public key of the Certigna Root CA is distributed in a self-signed certificate.

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

6.1.5. Size of the keys

CA key

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

Subject key

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

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

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

CA key

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

Subject key

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

6.1.7. Key usage objectives

CA key

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

Subject key

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

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

6.2.1. Security standards and measures for cryptographic modules

Cryptographic modules of CA

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

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

Devices for protecting Subject's private key

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

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

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

6.2.2. Control of the private key by several persons

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

least equal to 2).

6.2.3. Private key escrow

CA key

The CA private keys are never escrowed.

Subject key

Encipherment
Subject private keys are escrowed.

6.2.4. Backup copy of the private key

CA key

The private key of the CA is saved:

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

Subject key

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

6.2.5. Private key archival

CA key

The private key of the CA is never archived.

Subject key

Encipherment
Escrowed private keys are backuped complying security requirements for key escrow.

6.2.6. Transfer of the private key with the cryptographic module

For reminder, the Subjects private keys are generated under the responsibility of the operator of RA, DRA, Certification Agent or Subject.

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

6.2.7. Private key storage in the cryptogaphic module

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

6.2.8. Private key activation method

CA key

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

Subject key

Activation of key pairs is controlled by activation data (cf. chapter 6.4) which are used by the device.

6.2.9. Private key desactivation method

CA key

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

Subject key

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

6.2.10. Private keys destruction method

CA key

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

Subject key

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

Chiffrement
When the private key of a Subject is no longer required, the method of destroying this private key makes it possible to satisfy the requirements defined in chapter 11 for the security level considered. At the end of the period of validity of a certificate, the transition to a new private key can be done by the Subject: - by retaining the old and the new private key, so that the Subject continues to access the previously encrypted data with its old private key, - by transcoding the old private key to the new one, in which case the old key need not be retained.

6.2.11. Cryptographic module security evaluation level

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

6.3. Other aspects of 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

The key pairs and certificates of Subjects covered have a term of 5 years maximum for [Individual] and 3 years maximum for [Company][Administrative authority] depending on the policy purchased.

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

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

6.4. Activation data

6.4.1. Generation and installation of activation data

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

Generation and installation of activation data of the cryptographic module of the CA are performed during the initialization and customization phase of the module (see chapter 6.1.1). The activation data match the PIN of the administration smart cards for the cryptographic module.

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

In the case where the key pair is generated by the CA, activation data are transmitted by SMS (or by e-mail in case of problem) and are after modified by the Subject from the Customer space.

6.4.2. Activation data protection

Protection of activation data corresponding to the CA private key

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

Protection of activation data corresponding to the subject private key

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

6.4.3. Other aspects related to activation data

Not applicable.

6.5. Security measures for IT systems

6.5.1. Technical security requirements specific to IT systems

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

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

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

6.5.2. IT systems security evaluation level

Not applicable.

6.6. Security measures for the systems during their lifecycle

6.6.1. Security measures linked to the development of the systems

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

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

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

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

6.6.2. Measures related to security management

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

6.6.3. Security evaluation level of the systems lifecycle

Not applicable.

6.7. Network security measures

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

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

6.8. Timestamping/dating system

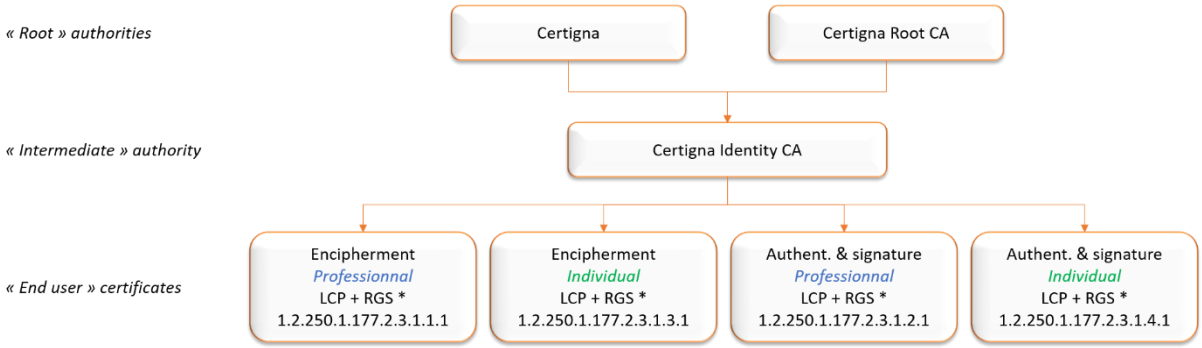
To ensure synchronization between different dating of events, the various components of the PKI synchronize their clocks with respect to a reliable source of UTC.

7. Profiles of the certificates and the CRL

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

7.1. Trusted hierarchy

The trusted hierarchy is composed with following certificates and authorities:



7.2. Profiles of Root Authorities certificates

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

7.3. Profile of the intermediate CA certificate

7.3.1. Basic fields

Fields	Signed by « Certigna »	Signed by « Certigna Root CA »
Version	V3	
Serial Number	41 12 0D 20 00 2E 4B 6F 9F 47 D3 55 73 E7 8A 77	59 44 CB 2D BE 6A DE A5 13 4E 9A 32 19 41 0C AE
Signature	Identifier of CA signing algorithm SHA-256 RSA 4096	
Subject Public Key Info	RSA 4096 bits	
Validity	Dates and times of activation and expiry of the certificate	
Issuer DN	CN = Certigna O = Dhimyotis C = FR	CN = Certigna Root CA OU = 0002 48146308100036 O = Dhimyotis C = FR
Subject DN	CN = Certigna Identity Plus CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR	

7.3.2. Extensions

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

7.4. Profile of the Subject certificate

7.4.1. Encipherment * [Individual]

Fields	Description
Version	V3
Serial Number	Unique serial number output from a CSPRNG (Cryptographically secure pseudorandom number generator) / Between 128 and 160 bits
Signature	ID of the CA signing algorithm / SHA-256 RSA 4096
SubjectPublicKeyInfo	RSA 2048
Validity	Dates and times of activation and expiry of the certificate [Maximum 5 years]
Issuer DN	CN = Certigna Identity CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR
Subject DN	CN = <Firstname> < SURNAME > **CHIF** GN= <Firstname> SN= <SURNAME> C = Country of the competent authority to which the entity is officially registered SN= Serie of characters with a random value for uniqueness

Extensions	Crit.	Description
Authority Key Identifier	No	ID of the public key of CA
Subject Key Identifier	No	ID of the public key of Subject
SubjectAlternativeName	No	Nom RFC822=Subject E-mail address
Key Usage	**Yes**	keyEncipherment
Extended Key Usage	No	Email Protection / msEFS
Certificate Policies	No	**OID=**1.2.250.1.177.2.3.1.3.1 **CPS**= https://www.certigna.fr/autorites/
CRL Distribution Points	No	**URL**=http://crl.certigna.fr/identityca.crl **URL**=http://crl.dhimyotis.com/identityca.crl
Authority Information Access	No	**caIssuers**=http://autorite.certigna.fr/identityca.der **caIssuers**=http://autorite.dhimyotis.com/identityca.der **URL**=http://identityca.ocsp.certigna.fr **URL**=http://identityca.ocsp.dhimyotis.com
Basic Constraints	No	**cA** = FALSE

7.4.2. Encipherment * [Company] [Administrative authority]

Fields	Description
Version	V3
Serial Number	Unique serial number output from a CSPRNG (Cryptographically secure pseudorandom number generator) / Between 128 and 160 bits
Signature	ID of the CA signing algorithm / SHA-256 RSA 4096
SubjectPublicKeyInfo	RSA 2048
Validity	Dates and times of activation and expiry of the certificate [Maximum 3 years]
Issuer DN	CN = Certigna Identity CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR
Subject DN	CN = <Firstname> < SURNAME > **CHIF** GN= <Firstname> SN= <SURNAME> OU = ICD + identifier of the entity of the subject registered in accordance with the laws and regulations OI = Information on the proof of identity of the entity O = Name of the entity linked to the Subject C = Country of the competent authority to which the entity is officially registered SN= Serie of characters with a random value for uniqueness

Extensions	Crit.	Description
Authority Key Identifier	No	ID of the public key of CA
Subject Key Identifier	No	ID of the public key of Subject
SubjectAlternativeName	No	Nom RFC822=Subject E-mail address
Key Usage	**Yes**	keyEncipherment
Extended Key Usage	No	Email Protection / msEFS
Certificate Policies	No	**OID=**1.2.250.1.177.2.3.1.1.1 **CPS**= https://www.certigna.fr/autorites/
CRL Distribution Points	No	**URL**=http://crl.certigna.fr/identityca.crl **URL**=http://crl.dhimyotis.com/identityca.crl
Authority Information Access	No	**caIssuers**=http://autorite.certigna.fr/identityca.der **caIssuers**=http://autorite.dhimyotis.com/identityca.der **URL**=http://identityca.ocsp.certigna.fr **URL**=http://identityca.ocsp.dhimyotis.com
Basic Constraints	No	**cA** = FALSE

7.4.3. Authentication and signature * [Individual]

Fields	Description
Version	V3
Serial Number	Unique serial number output from a CSPRNG (Cryptographically secure pseudorandom number generator) / Between 128 and 160 bits
Signature	ID of the CA signing algorithm / SHA-256 RSA 4096
SubjectPublicKeyInfo	RSA 2048
Validity	Dates and times of activation and expiry of the certificate [Maximum 5 years]
Issuer DN	CN = Certigna Identity CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR
Subject DN	CN = <Firstname> < SURNAME > **ID** GN= <Firstname> SN= <SURNAME> C = Country of the competent authority to which the entity is officially registered SN= Serie of characters with a random value for uniqueness

Extensions	Crit.	Description
Authority Key Identifier	No	ID of the public key of CA
Subject Key Identifier	No	ID of the public key of Subject
SubjectAlternativeName	No	Nom RFC822=Subject E-mail address
Key Usage	**Yes**	Digital signature / Non repudiation
Extended Key Usage	No	Client Auth / Email Protection
Certificate Policies	No	**OID=**1.2.250.1.177.2.2.1.4.1 **CPS**= https://www.certigna.fr/autorites/
CRL Distribution Points	No	**URL**=http://crl.certigna.fr/identityca.crl **URL**=http://crl.dhimyotis.com/identityca.crl
Authority Information Access	No	**caIssuers**=http://autorite.certigna.fr/identityca.der **caIssuers**=http://autorite.dhimyotis.com/identityca.der **URL**=http://identityca.ocsp.certigna.fr **URL**=http://identityca.ocsp.dhimyotis.com
Basic Constraints	No	**cA** = FALSE

7.4.4. Authentication and signature * [Company] [Administrative authority]

Fields	Description
Version	V3
Serial Number	Unique serial number output from a CSPRNG (Cryptographically secure pseudorandom number generator) / Between 128 and 160 bits
Signature	ID of the CA signing algorithm / SHA-256 RSA 4096
SubjectPublicKeyInfo	RSA 2048
Validity	Dates and times of activation and expiry of the certificate [Maximum 3 years]
Issuer DN	CN = Certigna Identity CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR
Subject DN	CN = <Firstname> < SURNAME > **ID** GN= <Firstname> SN= <SURNAME> OU = ICD + identifier of the entity of the subject registered in accordance with the laws and regulations OI = Information on the proof of identity of the entity O = Name of the entity linked to the Subject C = Country of the competent authority to which the entity is officially registered SN= Serie of characters with a random value for uniqueness

Extensions	Crit.	Description
Authority Key Identifier	No	ID of the public key of CA
Subject Key Identifier	No	ID of the public key of Subject
SubjectAlternativeName	No	Nom RFC822=Subject E-mail address
Key Usage	**Yes**	Digital signature / Non repudiation
Extended Key Usage	No	Client Auth / Email Protection
Certificate Policies	No	**OID=**1.2.250.1.177.2.3.1.2.1 **CPS**= https://www.certigna.fr/autorites/
CRL Distribution Points	No	**URL**=http://crl.certigna.fr/identityca.crl **URL**=http://crl.dhimyotis.com/identityca.crl
Authority Information Access	No	**caIssuers**=http://autorite.certigna.fr/identityca.der **caIssuers**=http://autorite.dhimyotis.com/identityca.der **URL**=http://identityca.ocsp.certigna.fr **URL**=http://identityca.ocsp.dhimyotis.com
Basic Constraints	No	**cA** = FALSE

7.5. Profile of LCR

7.5.1. Basic fields

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

7.5.2. Extensions

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

7.6. Processing certificates extensions by applications

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

7.6.1. Criticality

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

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

- If the extension is not compliant with what the application wants to do, the certificate is rejected.

7.6.2. Extension description

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

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

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

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

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

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

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

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

8. Compliance audit and other evaluations

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

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

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

8.1. Frequency and/or circumstances of the evaluations

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

This control is conducted every 3 years by the CA. Qualification audits are perfomed every year.

8.2. Identities/qualifications of the evaluators

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

8.3. Relations between evaluators and the evaluated entities

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

8.4. Topics covered by the evaluations

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

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.

9.4. Protection of personnel data

9.4.1. Personal data protection policy

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

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

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

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

DHIMYOTIS, Service du DPO,
20 Allée de Râperie, 59 650 Villeneuve d'Ascq, France

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

9.4.2. 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.

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. Subject

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

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

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

9.6.4. 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.
- Check that the certificate issued by CA is referenced at the level of security and for the required trusted service by the application.

9.6.5. Other participants

Not applicable.

9.7. Guarantee limit

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

9.8. 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 of RGS and additional documents to the latter.

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

9.12.2. 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.

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.

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

11.1. Security objectives requirements

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

- If the Subject key pair is generated by the device, guaranteeing that this generation is implemented exclusively by authorized users and guaranteeing the cryptographic sturdiness of the generated key pair;
- Detecting defects during the initialisation, customisation and operation phases, and ensuring secure techniques for the destruction of the private key in case of re-generation of the private key;
- Guaranteeing the private key's confidentiality and integrity;
- Ensuring the correspondence between the private key and the public key;
- Generating a security function which cannot be falsified without knowing the private key;
- Ensuring the public key's authenticity and integrity when exported oustide of the device;
- Ensuring for the legitimate subject only, the security function, and protecting the private key against any usage by third parties.

Encipherment
The private key protection device must also meet the following requirements: - Ensure the decryption function, symmetric key file or message, to the lawful subject only and protect the private key against unauthorized use by third parties; - Allow to ensure the authenticity and integrity of the symmetric key file or message, once deciphered, at its export from the device to the data decryption application; - If necessary, help to ensure the confidentiality, authenticity and integrity of the private key in its export outside of the device, to an escrow or archiving private keys function.

11.2. Qualification requirements

*** Level**
The Key pair protection device provided by CA or used by the subject is: - Qualified at least at the « Elementary » level by the ANSSI.