NATURE OF THE DOCUMENT
Security Document

REFERENCE	DATE	VERSION
DT-FL-1310/020	15 June 2017	1.7

CERTIFICATION POLICY

CERTIFICATE FOR A SERVER

Authentication (Server & Client) / Seal and TSU

ISSUER	RECIPIENTS	CC
CERTINOMIS	PUBLIC	

Certinomis

Certinomis SA with a registered capital of 40,156 euros.

Head office: 10 avenue Charles de Gaulle

94220 Charenton Le Pont – France. Créteil TCR B 433 998 903

History of the versions

DATE	VERSION	EVOLUTION	AUTHOR
10/10/2013	1.0	Public version	Franck Leroy
28/11/2013	1.1	Incorporation of the Mozilla v2.2 policy	Franck Leroy
13/03/2014	1.2	Addition of double usage OID for holder	Franck Leroy
03/06/2014	1.3	Addition of levels of qualification	Franck Leroy
10/03/2015	1.4	Incorporation of the RGS v2.0	Franck Leroy
10/03/2016	1.5	Incorporation of EN 319 411 series	Franck Leroy
16/01/2017	1.6	Integration of DGDDI RA	Franck Leroy
15/06/2017	1.7	Update of notification breach provisions	Franck Leroy

TABLE OF CONTENTS

WARNING

The present Certification Policy is a document protected by the provisions of the Intellectual Property Code of 1 July 1992, notably by the provisions relative to intellectual and artistic property and to copyrights, as well as by all applicable international agreements. These rights are the exclusive property of Certinomis. Any entire or partial reproduction or representation (including publication and dissemination) by any means whatsoever (notably electronic, mechanical, optical, photocopy, computer records) without the prior written authorisation of Certinomis or its successors in title is strictly forbidden.

The Intellectual Property Code only authorises, in its article L. 122-5, firstly, “copies or reproductions strictly reserved for the private usage of the copyist and not intended for any collective usage” and, secondly, analyses and short quotations for the purposes of example and illustration “any representation or reproduction in whole or in part without the consent of the author or its successors in title or assigns is unlawful” (article L. 122-4 of the Intellectual Property Code).

This representation or reproduction, by any means whatsoever, would constitute an infringement sanctioned by articles L.335-2 et seq of the Intellectual property code.

The Certification Practices Declaration, owned by the Certinomis company, can be provided through licence agreements to all private or public entities wishing to use it within the framework of their own certification services.

1 INTRODUCTION

1.1 GENERAL PRESENTATION

A Public Key Infrastructure (PKI) is a set of technical, human, documentary and contractual means made available to users in order to ensure, by means of asymmetric cryptography systems, a secure environment for their electronic exchanges.

The set-up of a PKI, required for security and confidence, allows for a range of added value services for electronic transactions (for example: e-mail, commercial transactions, electronic procedures, local data protection, etc.).

Their purpose is to ensure:

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

The Certification Policy defined in the present document is intended for use by companies, associations, ministries, administrative or governmental entities and consortia of all kinds, as well as individuals. The people consulting and using this document can obtain additional implementation details from the issuer CA.

The Certification Policy covers the management and usage of certificates, based on their classes, that contain the public keys used for the purposes of the verification, authentication, integrity and concordance of the keys. For example, the certificates provided via the present policy could be used to verify the identities of correspondents exchanging e-mail or allow for remote access to an information system, to verify the identities of individuals or other legal persons (under private law or public law), or to preserve the integrity of one's servers, software programs and documents.

The Certification Policy also covers the management and usage of certificates containing the public keys that are used for confidentiality functions. The certificates provided by the present policy serve to ensure the secrecy of information considered by its owner to be private or sensitive, within certain applications such as e-mail or Web-based communications. The certificates are not used to protect classified information.

The delivery of a public key certificate pursuant to the present policy does not mean that the customer or beneficiary is authorised in any way to carry out commercial or other transactions in the name of the organisation using the CA.

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

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

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

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

1.2 DOCUMENT IDENTIFICATION

Designation of the Object Identification Numbers (OID) for this policy:

EASY CA			
OID		*Level of qualification*	
SSL Server:	1.2.250.1.86.2.3.1.20.1	RGS 1 star,	EN 319 411-1 OVCP
Client Server :	1.2.250.1.86.2.3.1.23.1	RGS 1 star,	EN 319 411-1 LCP
Server Stamp:	1.2.250.1.86.2.3.1.22.1	RGS 1 star,	EN 319 411-1 LCP

STANDARD CA			
OID		*Level of qualification*	
Server Stamp:	1.2.250.1.86.2.3.2.22.1	RGS 1 star,	EN 319 411-1 LCP

PRIME CA			
OID		*Level of qualification*	
SSL Server:	1.2.250.1.86.2.3.3.20.1	RGS 2 stars,	EN 319 411-2 QCP-w
Client Server :	1.2.250.1.86.2.3.3.23.1	RGS 2 stars,	EN 319 411-2 QCP-l-qscd, AATL
Server Stamp:	1.2.250.1.86.2.3.3.22.1	RGS 2 stars,	EN 319 411-2 QCP-l
Time-stamp unit :	1.2.250.1.86.2.3.3.24.1	RGS 1 star,	EN 319 411-2 QCP-l-qscd, AATL

1.3 DEFINITIONS AND ACRONYMS

1.3.1 Acronyms

The following acronyms are used in the present CP:

- CA Certification Authority
- RA Registration Authority
- PMA Policy Management Authority
- TSA Time-Stamping Authority
- DN Distinguished Name
- CPS Certification Practices Statement
- ETSI European Telecommunications Standards Institute
- PKI Public Key Infrastructure (key management infrastructure).
- ARL Authority Revocation List
- CRL Certificate Revocation List
- CAG Certification Agent
- OID Object Identifier
- CP Certification Policy
- TSP Trust Service Provider
- SCO Server Certificate Officer
- RSA Rivest Shamir Adelman

- PS Publication Service
- ISS Information Systems Security
- URL Uniform Resource Locator

1.3.2 Definitions

Certification Authority (CA):

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

Registration authority (RA): Cf. chapter 1.3.1.

Policy Management Authority (PMA):

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

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

Certificate:

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

Subject:

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

Beneficiary:

Natural person identified by the RA, who is responsible for the certificates delivered to him. The beneficiary can be the holder or SCO.

Holder:

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

System or application (also known as the Server):

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

Certification Policy (CP):

Set of rules identified by a name (OID) that defines the requirements with which a CA must comply when setting up and providing its services, and that indicates a certificate's applicability to a specific

community and/or to a class of applications having common security requirements. If necessary, a CP can also identify the obligations and requirements weighing on the other participants, notably the beneficiaries and users of certificates.

Certification Practices Statement (CPS):

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

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

1.4 ENTITIES INVOLVED IN THE PKI

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

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

- Certification authority,
- Registration authority,
- Beneficiaries of the Certification Authority (holder or server certificate officer),
- Subject of the certificate provided by the Certification Authority,
- Third party users.

1.4.1 Certification authorities

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

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

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

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

Registration authority (RA) - This function verifies the identification information of a certificate's future subject, possibly including other specific attributes, before sending the corresponding request to the appropriate PKI function, on the basis of the services rendered and of the PKI organisation (cf.

below). When necessary, the RA also looks after re-verifying information about the certificate's subject, when the certificate of the latter is being renewed.

Certificate generation function - This function generates (creation of the format, electronic signature with the CA's private key) the certificates on the basis of the information provided by the registration authority and of the holder's public key provided either by the beneficiary, or by the function that generates the beneficiary's secret elements, if the latter is managing the certificate's key pair.

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

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

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

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

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

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

Server Certificate Pfficer (SCO) - The natural person responsible for the server certificate, notably for the usage of this certificate and of the corresponding key pair, on behalf of the entity to which the IT server identified in this certificate is attached.

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

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

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

Within the framework of its operational functions, the requirements incumbent upon the CA as the manager of the overall PKI are the following:

- Being a legal entity according to French law.
- Having a contractual / hierarchical / regulatory relationship with the entity for which it is providing the management of the certificates for this entity's beneficiaries.
- Making all of the services declared in its CP available to the application promoters of the administration's dematerialized exchanges, to the beneficiaries, to the users of the certificates that are using its certificates.
- Ensuring that the CP's requirements and the CPS procedures are applied by each of the PKI's components, and compliant with the applicable standards.

Certinomis SA with a registered capital of 40,156€
Head office: 10 avenue Charles de Gaulle
94220 Charenton. Créteil TCR B 433 998 903

- Performing a risk analysis that will make it possible to determine the security objectives that will serve to cover the business line risks of the overall PKI and the corresponding technical and non-technical measures that will have to be implemented. It prepares the CPS on the basis of this analysis.
- Implementing the various identified functions in its CP that at least correspond with the present CP's functions, notably in terms of the generation of certificates, delivery to the beneficiary, management of revocations and information on the status of certificates.
- Undertaking whatever is necessary in order to comply with the commitments defined in the CP, notably in terms of reliability, quality and security.
- Generating, and renewing when necessary, its key pairs and the corresponding certificates (signing of certificates, of the CRL), or having the certificates renewed if the CA is attached to a hierarchically superior CA. Disseminating its CA certificates to the beneficiaries and users of the certificates.

1.4.2 Registration authority

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

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

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

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

- the acknowledgment and verification of the information regarding the future subject and its attachments entity, and the preparation of the corresponding registration file;
- if relevant, the acknowledgment and verification of the information regarding the future CAG and his attachments entity, and the preparation of the corresponding registration file;
- the acknowledgement and verification of the information regarding the future SCO and of the IT server, and of their attachment entity, and the preparation of the corresponding registration file;
- the preparation and transmission of the certificate request to the appropriate PKI function according to the latter's organisation and the available services;
- the archiving of the elements from the registration file (or dispatch to the component in charge of archiving);
- the retention and protection, in full confidentiality and integrity, of the beneficiary's authentication personal data or, if relevant, that of the CAG, including during exchanges of such data with the other PKI functions (it notably complies with the legislation relative to the protection of personal data).

Only the Certinomis RA is able to validate an Internet domain name (FQDN) with a view to issuing a publicly recognised SSL/TLS server certificate in the root authority program of the Internet browser editors (notably those that are members of the CABForum http://www.cabforum.org/forum.html). This validation function may not under any circumstances be delegated to a third party.

1.4.3 Server certificate officers

As part of the present CP, a SCO is a natural person who is in charge of the usage of the certificate for the IT server identified in this certificate and the private key corresponding with this certificate, on behalf of the entity that is also identified in this certificate. The SCO has a contractual / hierarchical / regulatory link with this entity.

The SCO complies with the conditions incumbent upon him, as defined in the present CP.

It should be noted that as the certificate is attached to the IT server and not to the SCO, the latter can change during the term of the certificate's validity: SCO's departure from the entity, change of assignment and responsibility within the entity, etc.

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

1.4.4 Certificate users

The certificate's user can be:

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

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

1.4.5 Other participants

1.4.5.1 PKI components

The functional breakdown of the PKI is described in the CPS

1.4.5.2 Certification agent

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

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

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

As part of an organisation, a CAG may be appointed in order to perform the actions needed for the issuing of a certificate in the place of customers.

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

The CAG must:

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

The CAG can designate an input operator. This operator is in charge of entering the data collected within the organisation represented by the CAG. By contract, he undertakes to maintain the strictest confidentiality regarding the data of which he may learn while performing this task.

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

The entity must inform the CA, beforehand if possible but at least as quickly as possible, of the departure of a CAG from his functions while assigning a successor.

1.5 USE OF THE CERTIFICATES

1.5.1 Applicable usage domains

1.5.1.1 Key pairs and issued certificates

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

SSL Server authentication
Usage of the server certificate
System or application that uses an identified entity's certificate for the purposes of: • establishing a secure session between a server and a person.

Client / server authentication
Usage of the server certificate
System or application that uses an identified entity's certificate: • in order to establish a secure session between two servers

Seal Server
Usage of the server certificate
System or application that uses an identified entity's certificate: • in order for an IT server to place a stamp on data, and verification of this stamp by a person. • in order for an IT server to place a stamp on data, and verification of this stamp by another IT server.

Time-stamping unit
Usage of the server certificate
System or application that uses an identified entity's certificate: • in order for an IT server to place a time-stamp token on data, and verification of

this time-stamp by a person.
- in order for an IT server to place a time-stamp token on data, and verification of this time-stamp by another IT server.

1.5.1.2 Key pairs and certificates of the CA and components

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

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

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

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

1.5.2 Forbidden usage domains

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

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

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

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

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

In the absence of a prior and written authorisation signed by a Certinomis legal representative, no one is authorised to use the private key associated with a certificate in order to sign another certificate or a CRL in the capacity of a CA.

1.6 MANAGEMENT OF THE CP

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

1.6.1 Entity managing the CP

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

1.6.2 Contact point

Certinomis general manager

10 avenue Charles de Gaulle

94220 Charenton Le Pont

Telephone: (33) (0)1.56.29.70.02
Fax: (33) (0)1. 56.29.72.67
E-mail: politiquecertification@certinomis.com

1.6.3 Entity determining the compliance of a CPS with this CP

The Certinomis Management determines the CPS's compliance with the present certification policy, either directly or indirectly by calling on independent experts specialising in the field of security and PKIs.

1.6.4 CPS compliance approval procedures

The CA is the guarantor of the CPS's application with the Certification Policy.

The CA is in charge of managing (updates, revisions) the CPS. Any request for an update of the CPS follows the established approval process. Every new CPS version is published without delay, in compliance with the requirements of paragraph 2.2.

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

2 RESPONSIBILITIES REGARDING THE PROVISION OF INFORMATION HAVING TO BE PUBLISHED

2.1 ENTITIES IN CHARGE OF PROVIDING INFORMATION

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

The CA's CRL can be accessed via the Internet through 2 access points:

- HTTP on the crl.igc-g3.certinomis.com server
- HTTP on the www.certinomis.fr server

The CA's OCSP can be accessed via the Internet through this access point:

- OCSP on the crl.igc-g3.certinomis.com server

The exact links are indicated in the "distribution point of the certificate revocation list" extension of each certificate issued by the CA.

The CRLs can also be directly downloaded from the public Web server:
www.certinomis.fr in the heading "Documents and links / Our revocation lists".

2.2 INFORMATION HAVING TO BE PUBLISHED

The Certification Policy, the public elements of the CPS, the CA certificates, the certificate application forms, the contracts and general terms in accordance with which the certificates are issued, are either available on the CA's website at the following addresshttp://www.certinomis.fr, or provided as part of the commercial negotiations.

A copy can also be obtained by e-mail.

As they provide, amongst other things, details of the means implemented in order to ensure the protection of the CA's installations, the procedures are not published for security reasons related to the "need to know".

However, if necessary, the CA can provide the complete list of procedures at the request of an authorised institution (PMA, master CA, other CA for cross-certification…), for the verification, audit or control processes included in the present declaration for that purpose, as well as within the framework of complying with the law.

If the CPS contains information relating to the CA's security or information that it considers to be confidential, there will be no publication. By means of a formal request, it is possible to obtain a summary or excerpts from the CPS in electronic format.

Moreover, given the complexity of reading a CP for holders or certificate users who are not specialists in this domain, the CA also publishes the general usage terms on its website http://www.certinomis.fr, under the heading: "Documents and links / Our general usage terms".

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

2.3 PUBLICATION TIMEFRAMES AND FREQUENCIES

The publication timeframes and frequencies depend on the information in question:

For information related to the PKI (new version of the CP, forms, etc.), the information is published whenever necessary in order to ensure, at all times, consistency between the published information and the CA's actual commitments, means and procedures.

For the CA's certificates, they are disseminated prior to any issuing of certificates and/or of corresponding CRLs within an interval of 24 hours.

The publication website is available 24 hours a day; 7/7.

For information on the status of certificates, the Certificate Revocation Lists will be updated within a maximum of 24 hours. After the update, the CRL is published within a maximum of 30 minutes.

2.4 PUBLISHED INFORMATION ACCESS CONTROL

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

Access for modification to the publication systems for the information on the status of certificates (addition, cancellation, modification of published information) is strictly limited to the authorised internal functions of the PKI, by means of strong access control (authentication by certificate on a medium).

Access for modification to the publication systems for other information is strictly limited to the authorised internal functions of the PKI, at least by means of password-type access control on the basis of a password management policy.

Certinomis SA with a registered capital of 40,156€
Head office: 10 avenue Charles de Gaulle
94220 Charenton. Créteil TCR B 433 998 903

3 IDENTIFICATION AND AUTHENTICATION

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

3.1 NAMING

3.1.1 Types of names

The employed names are compliant with the specifications of the [X.500] standard.

In each certificate compliant with the [X.509] standard, the issuing CA (issuer) and the holder (subject) are identified by means of a “Distinguished Name” (DN) of the [X.501] type.

Chapter 7.2.2 "Constraints on the names" of the [PROFILES] document sets forth rules on this subject.

3.1.2 Necessary usage of explicit names

The content of the Subject name and Issuer fields must be explicitly linked with the authenticated entity.

General
Explicit names
The distinguished name must contain the combination of the first name, family name and, optionally, initials. It can also contain a function or an organisational role. In case of another type of identified entity, the distinguished name must reflect its authenticated legal name. A distinguished name must necessarily contain the following fields: • the country (C) field; • the organisationName (O) field; • the organizationUnitName (OU) field; • the organizationIdentifier (OrgID) field; • the commonName (CN) field; • the givenName et surname (GN/SN) field; • the serialNumber (SNU) field.

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

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

In case of a dispute regarding a name in a filing of documents not under its control, the CA must ensure that, in the contract associated with this filing, there is a procedure for settling disputes with regard to names.

Every delegated CA is required to monitor and apply the naming policy of its master CA, if requested to do so.

3.1.3 Pseudonymisation of the identities

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

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

3.1.4 Rules for interpreting the various types of names

The [PROFILES] document provides rules in this regard.

3.1.5 Uniqueness of the names

The distinguished names are unique for all of a CA's identified entities. As such, the DN contains a specific field (serialNumber) consisting of numbers separated by a dash, in order to guarantee the unique nature of the distinguished name.

Chapter 7.2.2 "Constraints on the names" of the [PROFILES] document sets forth rules on this subject.

3.1.6 Identification, authentication and roles of registered trademarks

The right to use a name that is a trademark or service mark or any other distinctive sign (trade name, firm name, corporate name) within the meaning of articles L. 711-1 et seq of the Intellectual Property Code (codified by law n°92-957 of 1 July 1992 and its subsequent modifications) belongs to the legitimate holder of this trademark or service mark, or of this distinctive sign, or possibly to its licensees or assignees.

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

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method for proving possession of the private key

When the CA does not generate server keys, it verifies that the requester is truly in possession of the private key associated with the public key noted in its certificate. This verification can be performed on the basis of a certificate request packet using the PKCS#10 standard for verification of the proof of possession.

3.2.2 Validation of an institution's identity

The RA verifies the identification of the organisation, its legal representative and all persons directly or indirectly designated by the latter in order to represent it relative to the CA or RA. The legal representative and these persons, who will be identified while giving the scope of their mandate, are the certification agents.

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

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

The CA or RA archives all relevant information regarding this registration.

The CPS indicates the documents to be provided and the registration procedures implemented by the RA, in agreement with the CA.

Below is a summary of the procedures:

General
Verification of an organisation's identity
The RA checks that the request contains the following elements: • An issue authorisation signed and dated within the last 3 months, by a legal representative of the entity or by the certification agent, identifying the future beneficiary to whom the certificate must be delivered, • A certificate request signed and dated within the last 3 months, by the future beneficiary, • The general usage terms signed by the future beneficiary. • EITHER for a company registered in the French trade and companies register o a K-Bis extract, provided by the court clerk. o any document certifying the capacity of the signatory of the certificate application • OR for a French institution listed in the SIRENE directory o a SIRENE directory statement justifying your registration number o a copy of the articles of association / general meeting minutes, or any other currently valid document bearing the signatures of the institution's representatives o ELECTED REPRESENTATIVES: a copy of the minutes / discussions appointing the Mayor, Chairman, etc. This copy will have to bear your institution's stamp and the indication "certified true copy of the original". o APPOINTED REPRESENTATIVES: copy of the official journal or gazette that certifies this appointment (please highlight the line in question, if the page contains a great deal of text). For companies registered with the French trade and companies register, the RA can, if relevant, obtain a K-bis extract, provided by the court clerk. The RA retains the elements received for registration of the beneficiary, examines the submitted elements and documents with reasonable care, and verifies whether or not they appear to be compliant and valid.

3.2.3 Validation of the beneficiary's identity

This certificate must always contain the name of the identified entity and, possibly, all additional information needed to unambiguously identify its owner.

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

The CPS indicates the documents to be provided and the registration procedures implemented by the RA, in agreement with the CA.

3.2.3.1 Registration of an individual

The identification of the future holder (natural person) representing an entity requires firstly the identification of this entity, and secondly the identification of the natural person.

The entity's identification is carried out according to the provisions of article 3.2.2.

EASY CA and STANDARD CA
Verification of the identity of individuals acting on behalf of an organisation
The RA verifies the photocopy of at least one of the beneficiary's currently valid identity documents or professional card provided by an Administrative Authority, bearing a photo (national ID card, passport or residence permit). The RA retains the elements received for registration of the beneficiary, examines the submitted elements and documents with reasonable care, and verifies whether or not they appear to be compliant and valid.

PRIME CA
Verification of the identity of individuals acting on behalf of an organisation
The RA verifies the photocopy of at least one of the beneficiary's currently valid identity documents or professional card provided by an Administrative Authority, bearing a photo (national ID card, passport or residence permit). The RA retains the elements received for registration of the beneficiary, examines the submitted elements and documents with reasonable care, and verifies whether or not they appear to be compliant and valid. The distribution by the RA can be carried out directly to the beneficiary or to the certification agent. • If this involves the beneficiary, before the distribution, the RA uses a face-to-face meeting, i.e. in the presence of the beneficiary, to verify an original official identity document of the beneficiary that is currently valid, and that includes his photo and signature. • If this involves the certification agent, before the distribution, the RA uses a face-to-face meeting, i.e. in the presence of the certification agent, to verify an original official identity document of the certification agent that is currently valid, and that includes his photo and signature. The agent will then look after personally distributing to the beneficiary / beneficiaries the elements that have been provided to him.

3.2.3.2 Registration of a Certification Agent

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

- Usage of the CAG file as a reference for the identification data of the entity of all of the beneficiaries presented by the CAG.
- Possibly, supply of a certificate to the CAG so that it can sign the registration files of the beneficiaries of the entity that it represents, and then submit them in electronic form.

The identification of the future CAG representing an entity requires firstly the identification of this entity, and secondly the identification of the natural person.

The entity's identification is carried out according to the provisions of article 3.2.2.

EASY CA and STANDARD CA
Verification of the identity of the agents

The RA checks that the request contains the following elements:

- A mandate designating the CAG, signed and dated within the last 3 months, from the entity's legal representative. This mandate must be signed by the CAG for acceptance, containing:
  - A commitment from the CAG to the CA, that he will correctly and independently perform the verifications of the files of the requesters,
  - A commitment of the CAG to inform the RA of his departure from the entity,
- A currently valid official identity document for the CAG, that includes an identity photograph (notably national identity card, passport or residence card), that is provided to the RA that retains a copy.

The RA verifies the photocopy of at least one of the CAG's currently valid identity documents bearing a photo and signature, preceded by the indication "certified true copy of the original".

The RA retains the elements received for registration of the beneficiary, examines the submitted elements and documents with reasonable care, and verifies whether or not they appear to be compliant and valid.

PRIME CA
Verification of the identity of the agents

The RA checks that the request contains the following elements:

- A mandate designating the CAG, signed and dated within the last 3 months, from the entity's legal representative. This mandate must be signed by the CAG for acceptance, containing:
  - A commitment from the CAG to the CA, that he will correctly and independently perform the verifications of the files of the requesters,
  - A commitment of the CAG to inform the RA of his departure from the entity,
- A currently valid official identity document for the CAG, that includes an identity photograph (notably national identity card, passport or residence card), that is provided to the RA that retains a copy.

The RA verifies the photocopy of at least one of the CAG's currently valid identity documents bearing a photo and signature, preceded by the indication "certified true copy of the original".

The RA retains the elements received for registration of the beneficiary, examines the submitted elements and documents with reasonable care, and verifies whether or not they appear to be compliant and valid.

The distribution by the RA is carried out directly to the CAG.

The RA uses a face-to-face meeting, i.e. in the presence of the CAG, to verify an original official identity document of the CAG that is currently valid, and that includes his photo and signature. The CAG will then look after personally distributing to the requester the elements that have been provided to him.

3.2.3.3 Registration of a system or application

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

The identification of the entity and of the system manager is carried out according to the provisions of article 3.2.3.1 and, if the entity appoints a CAG, according to article 3.2.3.2.

The RA verifies that the requester is authorised to receive certificates for the system or application. The person or organisation that submits a request must provide proof of its right to use the system or

application that will be mentioned in the certificate. In particular in case of a Web server, it must provide proof that the domain name belongs to it.

EASY CA and STANDARD CA
Verification of the system's identity
The RA checks that the request contains the following elements: • An issue authorisation signed and dated within the last 3 months, by a legal representative of the entity or by the certification agent, identifying the future SCO as being authorised to be the SCO for the IT server for which the server certificate is to be delivered. • A certificate application signed and dated within the last 3 months, by the future beneficiary SCO and including the identity of the server concerned by this acceptance request. • The general usage terms signed by the future SCO. • Proof of the entity's possession of the domain name corresponding with the server's FQDN for server authentication certificate applications. The RA retains the elements received for registration of the system, examines the submitted elements and documents with reasonable care, and verifies whether or not they appear to be compliant and valid.

PRIME CA
Verification of the system's identity
The RA checks that the request contains the following elements: • An issue authorisation signed and dated within the last 3 months, by a legal representative of the entity or by the certification agent, identifying the future SCO as being authorised to be the SCO for the IT server for which the server certificate is to be delivered. • A certificate application signed and dated within the last 3 months, by the future beneficiary SCO and including the identity of the server concerned by this acceptance request. • The general usage terms signed by the future SCO. • Proof of the entity's possession of the domain name corresponding with the server's FQDN for server authentication certificate applications. The RA retains the elements received for registration of the system, examines the submitted elements and documents with reasonable care, and verifies whether or not they appear to be compliant and valid. The distribution by the RA can be carried out directly to the SCO or to the CAG. • If this involves the SACO/SSCO, before the distribution, the RA uses a face-to-face meeting, i.e. in the presence of the SACO/SSCO, to verify an original official identity document of the SACO/SSCO that is currently valid, and that includes his photo and signature. • If this involves the CAG, before the distribution, the RA uses a face-to-face meeting, i.e. in the presence of the CAG, to verify an original official identity document of the CAG that is currently valid, and that includes his photo and signature. The CAG will then personally be responsible for distributing to the SCO the elements that have been provided to him.

3.2.3.4 Registration of a new SCO for a previously issued server certificate

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

The identification of the new SCO (natural person) representing an entity requires the identification of the natural person and the verification of his authorisation as representative for the entity to which the server is attached, and as the SCO for the server in question.

To this end, a new server certificate will have to be requested in order to prepare a request relative to the new SCO (cf. § Registration of a system or application).

3.2.4 Unverified information

The certificate issued pursuant to the present CP include no unverified information.

3.2.5 Validation of the requester's authority

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

3.2.6 Interoperability criteria

No interoperability with other CAs is anticipated.

3.3 IDENTIFICATION AND VALIDATION OF A KEY RENEWAL REQUEST

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

3.3.1 Identification and validation for a current renewal

At the time of the first renewal, verification of the subject's identity is optional. If no change is made to the identified identities, the list of documents to be provided is reduced.

At the time of the next renewal, the RA receiving the request identifies the subject according to the same procedure as for the initial registration.

The CPS lists the renewal provisions.

3.3.2 Identification and validation for a renewal after revocation

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

3.4 IDENTIFICATION AND VALIDATION OF A REVOCATION REQUEST

A revocation request can be submitted on the Certinomis website, by the certificate's beneficiary or agent. For the request to be authorised, the user must be identified via the following elements:

- Type of requester (beneficiary or agent)
- Certificate e-mail address
- Name of the certificate's holder

- Self-revocation code
- Captcha code[2]

The revocation request can be submitted by telephone. For the request to be authorised, the user must be identified by a series of 4 questions / answers beforehand provided to Certinomis.

A revocation request can also be submitted by letter or fax. It must then be signed by the requester, and the service in charge of managing revocations verifies the requester's identity (verification of the handwritten signature relative to a previously registered signature) and this person's authority relative to the certificate that is to be revoked.

The CPS specifies the modalities of revocation.

[2] See the definition at: http://fr.wikipedia.org/wiki/Captcha

4 OPERATIONAL REQUIREMENTS ON THE LIFECYCLE OF CERTIFICATES

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

4.1 CERTIFICATE REQUEST

4.1.1 Origin of a certificate request

On its website, the CA publishes all of the procedures and requirements regarding a certificate request. Electronic identification applicants must follow and comply with the published procedures.

A certificate can be requested by a legal representative of the entity or by a CAG duly mandated for this entity, with in all cases the future beneficiary's prior consent.

4.1.2 Process and responsibilities for submitting a certificate request

The certificate request must include the following information:

The electronic identification request sent to the RA must at least contain the requester's surname, first name and e-mail address. In the case of an organisation, the request must also contain the information that will serve to identify the physical residence as well as the organisation's corporate name. In the case of a system or application, the request must also contain the name of the system or application.

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

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

In case of an organisation, for each request, there must also be an authorisation and a customer contract, both signed by an identified certification agent. This contract must mention the beneficiary's information obligations amongst its obligations.

4.2 PROCESSING OF A CERTIFICATE REQUEST

4.2.1 Performance of the identification and request validation processes

A certificate request in no way obliges the CA to issue a digital certificate.

The issuing of a certificate by a CA indicates that it has definitively and completely approved the certificate request according to the procedures described in the CPS.

The RA then retains a trace of the submitted identity documentation: in the form of a photocopy signed both by the future beneficiary and by the RA, or the CAG if relevant, with the signatures preceded by the indication "certified true copy of the original".

4.2.2 Request acceptance or rejection

Upon receiving a certificate request, the CA:

- ensures that the request has been properly taken into account by a RA that it has recognised, and that the said RA has processed the request and provided an attributable trace of his opinion;
- generates and signs the certificate.

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

4.2.3 Certificate preparation timeframe

After validation of the certificate request, the certificate is issued as quickly as possible.

4.3 DELIVERY OF THE CERTIFICATE

4.3.1 Actions of the CA regarding the delivery of the certificate

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

- The holder (or server) is created in the CA system, and a unique number is assigned to it.
- The beneficiary is sent an e-mail containing his self-revocation code.

When the CA does not generate keys for servers, it automatically signs certificates that will contain the public key of the CSR provided during registration.

- The beneficiary generates the server keys and sends the CSR to the PKI.
- The PKI generates the certificate.

For software certificates, when the CA generates the keys:

- The CD-R is inserted into the customisation tool.
- The PKI generates keys and certificates.
- The PKI generates an activation code for the certificates.
- The customisation tool burns the keys and certificates onto a CD-R.

Or

- The activation code selected by the user is sent to the PKI.
- The PKI generates keys and certificates protected by the activation code (pkcs12).

For hardware certificates, the RA will generate the keys in the beneficiary device:

- The cryptographic device is inserted into the customisation tool.
- The device generates its keys and sends the CSR to the PKI.
- The PKI generates the certificates and the customisation tool inserts them into the device.
- The PKI generates an activation and release code.
- The customisation tool accordingly modifies the device's codes.

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

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

EASY CA
Delivery of the certificate
This certificate is delivered by mail, when the certificate is stored on a CD-R. Otherwise, the certificate is sent to the server certificate officer by e-mail.

STANDARD CA
Delivery of the certificate
This certificate is delivered by mail, when the certificate is stored on a CD-R. Otherwise, the certificate is sent to the server certificate officer by e-mail.

PRIME CA
Delivery of the certificate
When the certificate is provided in the beneficiary device, it is delivered to the beneficiary by hand (face-to-face) by an agent of La Poste (on site or in an office of the company). This certificate can also be delivered by the Certification Agent, who must deliver it to the beneficiary face-to-face. In this case the certificates are first provided to the CAG face-to-face in a sealed envelope by an agent of La Poste. When the certificate is maintained and managed by the CA device, there is no certificate delivery. The beneficiary is notified of the availability of his certificate by email. Each face-to-face meeting with an agent of La Poste requires a delivery notice, dated and signed by the agent of La Poste verifying the beneficiary's identity. This notice is returned to the CA for processing and archiving. If the CAG ensures the face-to-face delivery he undertakes to obtain a signature on a delivery notice and either to retain it, or to return it to Certinomis. The certificate delivery may also be validated by the beneficiary on the CA website by using an activation code provided with the certificate.

When the CA generate activation codes, the certificate cannot be used without having this code (PIN or password depending on the type of cryptographic device). It is sent directly to the beneficiary's address, by secure mail.

4.4 ACCEPTANCE OF THE CERTIFICATE

4.4.1 Certificate acceptance procedure

When the certificate has been made available to the beneficiary, the fact that the latter retrieves it implies acceptance of the certificate under the commercial, legal and technical conditions defined by the CA. The certificate's first usage also implies tacit acceptance.

Once the certificate is retrieved, the beneficiary must verify the certificate's contents. The beneficiary has 15 days in which to inform the CA of its refusal (by telephone, e-mail or ordinary mail).

By accepting a certificate, the beneficiary formally recognises his acceptance of the contractual usage terms and conditions and, more generally, of all elements published in the present CA Certification Policy.

4.4.2 Publication of the certificate

The CA does not publish the newly issued certificates.

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

The CA prints cover letters in order to indicate the certificate's delivery.

- Notification to the beneficiary.
- Notification to the delivery office.
- If relevant, notification to the certification agent.

The RA synchronizes the status of the delivery requests, with the CA's production report.

The RA filters the requests such as to provide a follow-up of returns of the delivery notices.

4.5 USES OF THE KEY PAIR AND OF THE CERTIFICATE

4.5.1 Usage of the private key and certificate by the beneficiary

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

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

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

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

Cf. previous chapter and chapter 1.4.

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

4.6 CERTIFICATE RENEWAL

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

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

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

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

4.7.1 Possible causes for changing a key pair

The key pairs must be periodically renewed in order to minimise the possibility of cryptographic attacks. As such, the key pairs of the servers and the corresponding certificates are renewed at least every three years and every year for time-stamp units.

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

4.7.2 Origin of a new certificate request

The triggering of the provision of a new certificate to the beneficiary can be automatic or on the customer's initiative.

The entity, if relevant by its CAG, can also initiate a request for the provision of a new certificate for a beneficiary that is attached to it.

4.7.3 Processing procedure for a new certificate request

The identification and validation of a new certificate provision request are described in chapter 3.3 above.

For the CA's actions, cf. chapter 4.3.1.

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

Cf. chapter 4.3.2.

4.7.5 New certificate acceptance initiative

Cf. chapter 4.4.1.

4.7.6 Publication of the new certificate

Cf. chapter 4.4.2.

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

Cf. chapter 4.4.3.

4.8 CERTIFICATE MODIFICATION

Note -In compliance with [RFC3647], the modification of a certificate corresponds with modifications of information with no change to the public key (cf. chapter 4.7) and other that only a modification of the validity dates (cf. Chapter 4.6).

The present CP does not authorise certificate modifications.

4.9 REVOCATION AND SUSPENSION OF CERTIFICATES

4.9.1 Possible causes of a revocation

4.9.1.1 Certificates of the beneficiaries

The following circumstances can result in the revocation of a beneficiary's certificate:

- the subject-related information in the certificate no longer complies with the identity or usage anticipated in the certificate (for example, change of entity of the holder of the certificate), before the certificate's normal expiry;
- the beneficiary has not complied with the certificate's usage application provisions;
- the beneficiary and/or, if relevant, the CAG / the entity has not respected their obligations resulting from the CA's CP;
- an error (intentional or not) has been uncovered in the beneficiary's registration file.
- the beneficiary's private key is suspected to have been compromised, is compromised, lost or stolen,
- the beneficiary or an authorised entity (the entity's legal representative or CAG, for example) requests the certificate's revocation (notably in case of destruction or alteration of the holder's private key and/or of its medium);
- the death of the beneficiary or the cessation of activities of the beneficiary's entity (for an organisation's certificate).

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

Should the customer or beneficiary learn of the suspected or established compromise of the private key, they are obliged to immediately verify the revocation of the associated certificate, and to request it as quickly as possible if it has not already been revoked.

Should the customer or beneficiary learn of any modification of the information contained in the certificate, they are obliged to immediately verify its revocation, and to request it as quickly as possible if it has not already been revoked.

In addition to the certificate revocation cases mentioned above, the CA can revoke the beneficiary's certificate when it learns of information that would serve to indicate that the beneficiary's situation has undergone modifications that have not been indicated to it, or should it have serious suspicions with regard to the compromise of the beneficiary's private key. More generally, at its discretion, the CA can revoke an identified entity's certificate when the customer no longer complies with the obligations contained in the present certification policy and in all of the contractual documents, as well as in any applicable law and regulation.

4.9.1.2 Certificates of a PKI component

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

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

4.9.2 Origin of a revocation request

4.9.2.1 Certificates of the beneficiaries

Only the following can request a certificate's revocation:

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

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

4.9.2.2 Certificates of a PKI component

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

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

4.9.3 Processing procedure for a revocation request

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

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

4.9.3.1 Revocation of one of the beneficiary's certificates

The CA ensures that all of the procedures and requirements regarding a certificate's revocation are contained in the CPS or in another public document.

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

The revocation request must contain identification information on the certificate that is to be revoked. The request can also contain a detailed description of the revocation causes, and possibly the reasons behind such causes. The revocation procedure is described in detail on the www.certinomis.fr site.

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

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

4.9.3.2 Revocation of a certificate of a PKI component

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

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

The contact point identified on the site: http://www.ssi.gouv.fr is immediately informed in the event of revocation of one of certificates of the certification chain.

4.9.4 Timeframe granted to the beneficiary to formulate the revocation request

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

4.9.5 Timeframe for the CA to process a revocation request

4.9.5.1 Revocation of one of the beneficiary's certificates

Given its nature, a revocation request is treated as an emergency.

The function managing revocations is available 24-by-7.

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

Every certificate revocation request is processed within less than 24 hours, beginning with the receipt of the authenticated revocation request and ending with the users being provided with information on the revocation.

4.9.5.2 Revocation of a certificate of a PKI component

The certificate of a PKI component is revoked immediately upon the detection of an event described in the possible revocation causes for this type of certificate. The certificate's revocation takes effect when the certificate's serial number is added to the revocation list of the CA that had issued the certificate.

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

4.9.6 Revocation verification requirements applicable to the certificate users

Before any use of certificates, notably when the said certificates result in legal effects, the third party user must absolutely verify, with Certinomis, the validity of the certificates upon which he plans to rely, by consulting the most recent valid Certificate Revocation Lists and by verifying the certificate's intrinsic validity, most notably its signature, and the validity of the issuer's certificate.

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

4.9.7 CRL preparation frequency

The publication frequency of the CRLs is 24 hours.

4.9.8 Maximum timeframe for the publication of a CRL

The CRL is published within a maximum of 30 minutes.

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

A supplementary publication following the OCSP protocol is available.

4.9.10 Requirements of the online verification of certificate revocations by certificate users

Cf. chapter 4.9.6 and 4.9.9 above.

4.9.11 Other available information means regarding revocations

No other means are available.

4.9.12 Specific requirements in case of compromise of the private key

In case of the recognised or suspected compromise of a CA's signature private key, the CA immediately so informs all of the PMAs that accredit it.

Should the customer or beneficiary learn of the suspected or established compromise of the private key, this entails an obligation to immediately verify the revocation of the associated certificate, and to request it as quickly as possible if it has not already been revoked.

The revocation procedure for a CA is carried out via a key ceremony operation, described in detail in the CPS.

4.9.13 Possible causes of a suspension

The present CP does not authorise certificate suspensions.

4.9.14 Origin of a suspension request

Not applicable.

4.9.15 Processing procedure for a suspension request

Not applicable.

4.9.16 Limits to a certificate's suspension period

Not applicable.

4.10 CERTIFICATE STATUS INFORMATION FUNCTION

4.10.1 Operational characteristics

The CA provides certificate users with information that will allow them to verify and validate, prior to its usage, the status of a certificate and of the entire corresponding certification chain (up to and including the Root CA), which means the ability to also verify the signatures of the chain's certificates, the signatures guaranteeing the origin and integrity of the CRLs / ARLs and the status of the Root CA's certificate.

These CRLs / ARLs are CRLs in V2 format, published on a web server accessible using the HTTP(s) protocol.

4.10.2 Availability of the function

The certificate status information function is available 24-by-7.

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

4.10.3 Optional systems

No optional system is available.

4.11 END OF THE RELATIONS BETWEEN THE BENEFICIARY AND THE CA

Should the contractual / hierarchical / regulatory relations end between the CA and the beneficiary before the end of the certificate's validity, for one reason or another, the certificate is revoked.

4.12 KEY ESCROW AND RECOVERY

Beneficiary private signing keys are not escrowed.

Beneficiary private signing keys may be generated and maintained by the CA device for a remote usage by the beneficiary.

Beneficiary private encryption/decryption keys may be escrowed by the CA when explicitly requested by the beneficiary in the certificate application file.

4.12.1 Policy and practices for the recovery of escrowed keys

Encryption keys may be recovered by holders among all their encryption keys that are in the recovery period. It will be required that the user authenticates to the RA website with a valid authentication certificate.

Then after a successful authentication, escrowed encryption keys will be available for download.

At the setup of the recovery system, a list of granted operators and the number of required operators in order to recover a key, will have to be defined.

The 'k' operators that will participate among the 'n' that are granted, will have to authenticate to the recovery system and the last one will be able to download the escrowed encryption key.

This recovery with operators may be done by request from a holder, or for internal use of the RA, or by a legally authorized third party.

The recovery period setup in the recovery system doesn't takes into account the validity period to the certificate: if the recovery period is 6 years and the certificate validity is 3 years, the encryption key may be recovered even if the certificate is expired or revoked.

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

Not applicable.

5 NON-TECHNICAL SECURITY MEASURES

5.1 PHYSICAL SECURITY MEASURES

The technical rooms accommodating the certification means, and notably the signature private key, are heavily protected. They are in an access controlled area, protected against all current risks (fire, flood...).

The protection level of the technical rooms is a crucial part of guaranteeing the security of the certification means and the operation of these means.

The CPS stipulates the physical security conditions and the rules applicable to and within the technical rooms, particularly regarding the following subjects:

- Location, construction and physical access
- Electrical system and air conditioning system
- Water damage
- Fire prevention and protection
- Warehousing of media
- Scrapping and destruction of hardware
- Backup outside of the rooms

5.1.1 Geographical location and construction of the sites

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

The construction of the site complies with the applicable rules and standards and, if relevant, specific requirements relative to risks such as earthquakes or explosions (proximity of an area accommodating factories or warehouses for chemical products,...).

5.1.2 Physical access

To avoid any loss, damage or compromise of the PKI's resources and the interruption of the CA's services, access to the rooms accommodating the PKI's various components is controlled.

Access is strictly limited only to persons authorised to enter these rooms, and the traceability of all accesses is assured. Outside of business hours, the security is strengthened by the implementation of physical and software intrusion detection means.

To ensure the availability of the systems, access to the machines is limited only to those persons authorised to perform operations requiring physical access to the machines.

Note -The machines include all servers, cryptographic units, workstations and active elements of the network used for the implementation of these functions.

5.1.3 Power supply and air conditioning

The characteristics of the electrical power supply and air conditioning equipment comply with the usage conditions for the PKI equipment as determined by the equipment suppliers.

They also make it possible to comply with the requirements of the present CP, and with the commitments assumed by the CA in its CPS in terms of the availability of its functions, notably the functions managing revocations and the information on the status of certificates.

5.1.4 Vulnerability to water damage

The means for protecting against water damage make it possible to comply with the requirements of the present CP, and with the commitments assumed by the CA in its CPS in terms of the availability of its functions, notably the functions managing revocations and the information on the status of certificates.

5.1.5 Fire prevention and protection

The fire prevention and firefighting means make it possible to comply with the requirements of the present CP, and with the commitments assumed by the CA in its CPS in terms of the availability of its functions, notably the functions managing revocations and the information on the status of certificates.

5.1.6 Safekeeping of media

As part of the risk analysis, the various information elements involved in the PKI's activities have been identified and their security needs have been defined (in terms of confidentiality, integrity and availability).

The media (paper, hard disk, diskette, CE, etc.) corresponding with these information elements are processed and retained in compliance with these security needs.

5.1.7 Media taken out of service

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

The destruction and reinitialisation procedures and means are compliant with the various confidentiality levels.

5.1.8 Off-site backups

As a supplement to the on-site backup, the PKI components carry out off-site backups of their applications and information. These backups are organised such as to ensure that the PKI can resume its functions after an incident as quickly as possible, in compliance with the requirements of the present CP and of the CA's commitment in its CPS in terms of availability, most notably for the functions managing revocations and information on the status of certificates (cf. chapters 4.9.5.1 and 4.10.2).

The off-site information backups comply with the same requirements of the present CP with regard to the protection of the confidentiality and integrity of the said information.

The PKI components in charge of the functions managing revocations and information on the status of certificates implement off-site backups that will allow for a quick recovery of these functions after the occurrence of a disaster or of events that seriously and lastingly affect the performance of these services (destruction of the site, etc.).

5.2 PROCEDURAL SECURITY MEASURES

5.2.1 Trust roles

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

Security manager - The security manager is in charge 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 in charge of analysing the event logs in order to detect any incident, anomaly, attempted compromise, etc.

Application manager - Within the component to which he is attached, the application manager is in charge 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 of the functions provided by this application and the corresponding performances.

System engineer - He is in charge 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, on the basis of 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.

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

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

5.2.2 Number of persons required per task

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

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

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

5.2.3 Identification and authentication for each role

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

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

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

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

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

- is assigned directly to a person;

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

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

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

5.2.4 Roles requiring a separation of duties

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

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

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

The duties associated with each role are described in the CPS corresponding with this CP.

5.3 SECURITY MEASURES RELATIVE TO THE PERSONNEL

5.3.1 Required qualifications, skills and authorisations

The CA manager ensures that all personnel members performing tasks relative to the operation of a CA, whether they report directly to the CA or to the RA:

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

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

5.3.2 Background verification procedures

All background verifications are carried out in compliance with the CA's security-related policy.

The employee swears to the accuracy of all information provided during the hiring phase.

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

5.3.3 Requirements regarded to initial training

The CA ensures that all personnel members performing tasks involved in the operation of a CA or RA have received complete training regarding:

- the operating principles and security mechanisms of the CA or RA.

The CA's personnel members undergo a training programme in order to correctly perform their functions. It relates:

- to the various applications and versions of applications to which they may have access as part of their functions within the CA system;
- to all of the tasks that they will have to perform within the framework of the PKI;
- to the hardware and operating systems that form the CA's operational environment;
- to the CA's backup plan after a disaster and the activity continuation procedures.

Before taking up their positions, they are provided with orientation regarding the applicable security rules.

Identical obligations are incumbent upon the RA and its personnel members..

5.3.4 Continuing training requirements and frequency

The requirements described in section 5.3.3 are kept up-to-date in order to reflect the changes made to the CA's system.

Vocational training courses are provided in keeping with the needs, and the CA reviews its requirements at least once each year.

On a regular basis, the CA's personnel takes part in security training sessions.

Identical obligations are incumbent upon the RA and its personnel members..

5.3.5 Rotation frequency and sequence between the various duties

No particular requirement.

5.3.6 Penalties in case of unauthorised actions

If a person has actually performed or is suspected of having performed an unauthorised action while carrying out his tasks relative to the operation of a CA or RA, the CA can interrupt his system access.

Moreover, if the facts are confirmed, it can take all appropriate disciplinary measures.

5.3.7 Requirements relative to the personnel of external service providers

The CA ensures that the personnel of co-contracting companies can access its premises in compliance with the terms of article 5.1.1.

The requirements relative to the personnel of co-contracting companies are identical with the ones relative to employees, particularly the ones listed in articles 5.3, 5.3.2 and 5.3.6.

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

5.3.8 Documentation provided to the personnel

The CA provides the CA and RA personnel members with the Certification Policies that it accepts, as well as any law, policy or contract that applies to the positions that they occupy.

All CA personnel members have access to supplementary manuals relating to their responsibilities. These manuals relate to all of the applicable procedures.

Identical obligations are incumbent upon the RA and its personnel members.

5.4 AUDIT DATA ESTABLISHMENT PROCEDURES

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

The resulting files, in paper or electronic format, provide for the traceability and accountability of the operations undertaken.

5.4.1 Types of events to be logged

In the verification registers, the CA and RA record all events relating to system security, notably:

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

All registers and logs, whether electronic or paper, contain the event's date and time as obtained from a sufficiently reliable time source, and indicate the entity in question.

Using electronic or paper means, the CA collects and collates security-related information that is not produced by the CA's system, notably:

- physical access logs;
- maintenance and changes to the system configuration;
- changes involving the personnel;
- registers regarding the destruction of media containing keys, activation data or personal information on the beneficiaries.

The CPS stipulates the types of information that must be logged.

To facilitate the decision-making process, all agreements and correspondence relating to the CA's services are collected and collated using electronic or manual means, and grouped in a single location.

5.4.2 Processing frequency for event logs

The CA and RA ensure that these logs are reviewed at least every week on the basis of a summary in which the significant elements are identified, analysed and explained. The summary brings to light any anomalies and identified falsifications.

Moreover, the various events of the functions that interact with one another (registration authority and generation function, revocation management function and certificate status information function, etc.) are recorded in a single log, which serves to guarantee the concordance between dependent events while also contributing to the identification of any anomaly.

5.4.3 Retention period for events logs

The CA and RA retain (while making them available upon request) the logs for at least one month, and then archive them in compliance with the instructions contained in article 5.5.

5.4.4 Protection of the events logs

The system for the electronic logs directly affecting certification operations include protective mechanisms against unauthorised attempts to modify or delete the logs.

The verification information obtained by manual means is also protected against unauthorised modification or destruction attempts.

The system for dating events complies with the requirements of chapter 6.8.

5.4.5 Backup procedure for events logs

The logs and their summaries are backed up, or copied (photocopy or digitization) if on paper.

5.4.6 Collection system for event logs

In the CPS, the CA indicates which systems it uses to collect verification data.

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

When an event is logged by the verification data collection system, there is no requirement to so inform the person, organisation, system or application behind it.

5.4.8 Evaluation of vulnerabilities

Events that occur within the verification process are logged, partly in order to verify the system's vulnerable points. The RA and CA ensure that an evaluation of these vulnerable points is performed, reviewed and revised, after an examination of these events.

5.5 DATA ARCHIVING

5.5.1 Types of data to be archived

The CA also undertake provisions with regard to archiving. This archiving serves to ensure the continued existence of the logs established by the various PKI components.

It also provides for the retention of paper elements linked to certification operations, as well as their availability when necessary.

The following data are archived:

- software programs (executables) and configuration files for IT hardware;
- the CPs;
- the CPSs;
- general conditions of use;

- the contractual agreements with other CAs;
- the certificates and CRLs as issued or published;
- the receipts or notifications (for informational purposes);
- the signed commitments of the CAGs;
- the proofs of identity of the beneficiaries and, if relevant, of the entity to which they are attached;
- the proof of identity of the application services (for example who is FQDN);
- the events logs of the various PKI entities.

5.5.2 Retention period of the archives

The electronic signature certificates, as well as the CRLs produced by the CA, are retained for at least five (5) years after expiry of the keys.

Information related to the management of the lifecycle of certificates, in particular all information related to the registration, will be retained for five (5) years after the expiry of the keys.

In addition to the above-mentioned paper data present in the registration files, for example, the following will also be retained in paper and/or electronic format, for a period of five (5) years after their expiry or the end of their validity:

- all versions and revisions of the applicable CPSs by the CA or a PKI component
- all agreements signed by Certinomis with other CAs and PKI components

5.5.3 Protection of the archives

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

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

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

5.5.4 Backup procedure for the archives

The protection level of the backups is equivalent with the protection level of the archives.

5.5.5 Data time-stamping requirements

Cf. chapter 5.4.4 for the dating of events logs.

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

5.5.6 Archive collection system

Whether internal or external, the archive collection system complies with the protection requirements for the archives in question.

5.5.7 Archive recovery and verification procedures

The archives (paper and electronic) can be recovered within less than 2 business days, bearing in mind that only the CA can access all of the archives (as opposed to an entity operating a PKI component that can only recover and consult the archives for the component in question).

5.6 CHANGE OF THE CA'S KEY

The CA cannot generate a certificate having an ending date that is after the expiry date of the CA's corresponding certificate.

To this end, the validity period of this CA certificate is after that of the certificates that it signs.

In view of this certificate's validity ending date, its renewal is requested within an interval that is at least equal with the lifespan of the certificates signed by the corresponding private key.

Once a new CA key pair has been generated, only the new private key is used to sign certificates.

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

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

5.7 RECOVERY AFTER COMPROMISE AND DISASTER

5.7.1 Procedure for forwarding and handling incidents and compromising

Every PKI components implements procedures and means to forward and handle incidents and compromising, in particular through training and awareness of the operators and through the analysis of the different events logs. These procedures and means allow to mitigate the damages due to security breaches and malfunctions.

In case of a major incident, such as leak, theft, suspicion of compromise or compromise of the CA private key, the triggering event is the observation of this incident in the PKI component, which informs immediately the CA.

The case of a major incident is necessarily handled when detected, and when needed the publication of the revocation status of the certificate is made in the buffest urgency, by every possible and available means (press, web site, notice…).

The CA also notifies directly and within a maximum of 24H delay the point of contact identified on the web site http://ssi.gouv.fr (in the contact section) and any person from the "Bureau Qualifications et Agréments" with whom the CA is in contact.

If one of the algorithms, or associated parameters, used by the CA or by the beneficiaries becomes weak during the remaining usage period, then the CA:

- Notifies all the beneficiaries and the third parties that use certificates with whom the CA made agreements or other forms of relations. In addition, this information is made available to other certificates users.
- Revoke any concerned certificates.

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

The only critical activity that the CA keeps in operation is the handling and publication of certificate revocations.

The CA prepares procedures intended to ensure the continuation of the activities and, in these procedures, describes the anticipated steps in case of corruption or loss of IT resources, software or necessary data. When the CA is not responsible for filing documents, it nevertheless ensures that the contract signed with the custodian calls for the latter to set up procedures intended to safeguard the data.

The CA anticipates a backup and recovery plan for its activities (BCP/BRP).

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

Should a member of the PKI component learn of the suspected or established compromise of the private key, this entails an obligation to immediately verify the revocation of the associated certificate, and to request it as quickly as possible if it has not already been revoked.

In case of compromise of a CA's electronic signature key, and before redefining a certificate within the PKI, the CA revokes its public key.

If a CA's electronic signature certificate has to be revoked, the CA as quickly as possible informs:

- the PMAs that accredit it;
- all RAs; and
- all the beneficiaries, agents and customers;

The CA also:

- publishes the certificate's serial number in the appropriate CRL;
- revokes all certificates signed using the revoked electronic signature certificate.

After having corrected the problems leading to the revocation, the CA can:

- produce a new signature key pair and publish the certificates associated with it; and
- issue new certificates for all entities.

Should it be necessary to revoke the electronic signature certificate of any other entity, the CA will follow the directives contained in article 4.9.

5.7.4 Business continuity capacities after a disaster

Within an anti-disaster plan, the CA defines the measures to be undertaken in order to re-establish a secure installation in case of a natural catastrophe or any other type of disaster. The CA ensures that all contracts possibly signed with partners stipulate that an anti-disaster plan must be implemented and documented by the custodian.

5.8 END-OF-LIFE OF THE PKI

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

The CA shall take the necessary measures to cover any costs involved in complying with these minimum requirements in the event that the CA were to be bankrupt or for other reasons were to be unable to cover these costs by itself, this, in so far as is possible, based on the constraints of the applicable legislation in cases of bankruptcy.

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

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

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

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

- Puts in place procedures aimed at ensuring a constant service in particular in regard to archiving (notably, archiving the holders' certificates and the information relating to the certificates);
- Ensures the continuity of the revocation (acknowledgement of a request for revocation and publication of the CRLs), in accordance with the availability requirements for its functions as defined in the CP.
- In so far as the changes envisaged may have repercussions on commitments vis-à-vis the beneficiaries or users of certificates, the CA informs them thereof as soon as possible within 1 month;
- The CA shall forward to the contact point identified on the http://www.ssi.gouv.fr site, the principles of the plan of action implementing the technical and organisational resources designed to face up to a cessation of activity or to organise the transfer of activity. It shall in particular present in it the systems put in place in respect of archiving (keys and information relating to the certificates) in order to carry out this function or to have it carried out throughout the period initially provided for in its CP. The CA, in accordance with the different components of the PKI in question, shall forward the procedures for the changes implemented to the ANSSI. The CA shall measure the impact and list the consequences of this event (legal, economic, functional, technical, communicational, etc.). It shall present a plan of action designed to remove, or reduce the risk for the applications and any difficulties for beneficiaries and users of certificates;
- The CA shall keep the ANSSI informed of any obstacle or additional delay encountered in the implementation of the process.

5.8.2 Cessation of activity affecting the CA

Cessation of activity may be total or partial (for example: cessation of activity for a given family of certificates only). Partial cessation of activity is progressive such that only the obligations referred to below need to be executed by the CA, or a third party entity that resumes activities, during the expiry of the last certificate issued by it.

In the event of total cessation of activity, the CA or, if this is impossible, any entity which replaces it as a result of a law, a regulation, a legal decision or an agreement previously reached with such entity, will revoke the certificates and publish the CRLs in accordance with the commitments made in the CP.

The CA carries out the following actions:

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

During the cessation of the service, the CA shall:

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

Certinomis SA with a registered capital of 40,156€
Head office: 10 avenue Charles de Gaulle
94220 Charenton. Créteil TCR B 433 998 903

6 TECHNICAL SECURITY MEASURES

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

6.1 GENERATION AND INSTALLATION OF KEY PAIRS

6.1.1 Generation of key pairs

The principle of the separation of keys is applied to all keys used within the framework of the CA's technical system. The separation of keys means that a key pair can only be used for a given cryptographic function, namely:

- one key pair dedicated to signature creation and verification;
- one key pair dedicated to confidentiality.

The CA produces its own electronic signature key pair by means of a cryptographic algorithm, and according to a procedure that involves several roles.

6.1.1.1 CA keys

The generation of the CA's signature keys is performed within a secure environment (cf. chapter 5).

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

The generation of the CA's signature keys is performed under perfectly controlled circumstances, by personnel members within trust roles (cf. Chapter 5.2.1), within the framework of "key ceremonies". These ceremonies are performed according to pre-defined scripts.

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

These secret shares are generated using a diagram with a Shamir threshold (n parts amongst m are necessary and sufficient to reconstitute the secret). This secret makes it possible to launch the secure loading, into a new cryptographic module, of the CA private key(s) backed up during the key ceremony.

After their generation, the secret shares are provided to previously designated bearers of secret shares, authorised to occupy this trust role by the CA. In whatever form (paper, magnetic medium or confined within a smart card or a USB key), a single bearer cannot hold more than one secret share from a given CA at any one time. Each secret share is implemented by its bearer.

The key ceremonies are carried out under the control of at least two persons who have trust roles, and in the presence of several witnesses, including at least one impartial witness from outside of the CA.

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

6.1.1.2 Server keys generated by the CA

When the key pairs of the servers are generated by the CA:

- either directly in the cryptographic device intended for the SCO, and are compliant with the requirements of chapter 12 below in terms of the security level in question,
- or, in the CA's cryptographic module without the CA retaining a copy.

6.1.1.3 Server keys generated on the server level

When the key pair is generated on the server level, this generation must be performed in a device that meets the requirements of chapter 12 below in terms of the security level in question. The CA makes sure of this with the SCO, through a contractual commitment of the server manager relative to the CA.

The key pairs are generated by the server officer, who provides the public key to the Authority for certification.

6.1.2 Transmission of the private key to the beneficiary

When the key pair is generated on the CA level, the private key is sent to the SCO securely, in order to ensure confidentiality and integrity.

EASY CA
Transmission of the private key
The private key is sent to the SCO within a PKCS#12 file, protected by an activation code. When the CA does not generate the activation code, the PKCS#12 file is e-mailed directly to the SCO. Otherwise the PKCS#12 file is stored on a memory device that is sent by mail.

STANDARD CA
Transmission of the private key
When the server's keys are generated within the cryptographic hardware device under the control of the Registration Authority, the latter sends the device by mail to the SCO.

PRIME CA
Transmission of the private key
When the server's keys are generated within the cryptographic hardware device under the control of the Registration Authority, the latter sends the device by mail to the SCO.

6.1.3 Transmission of the public key to the CA

When the server's public key is sent to a component of the CA, it must provided in the form of a query (PKCS10) that certifies the possession of the corresponding private key. Transmission via a https request site provides for end-to-end integrity. This public key is then sent to the PKI that verifies its integrity.

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

The CA's verification public key is disseminated in the form of a digital certificate that can be downloaded from the CA's website.

6.1.5 Sizes of the keys

The CA and holder keys must comply with the characteristic requirements (sizes, algorithms, etc.) listed in the [PROFILES] document.

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

The key pair generation method must use parameters that comply with the international security standards specific to the algorithm in question.

The following choices will be adopted by Certinomis:

- the public exponent will be 65537;
- the choice of the first p and q can be random or strong, subject to applying the recommendations applicable to the document mentioned in the reference.

6.1.7 Key usage objectives

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

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

The usage of a CA private key and of its associated certificate is strictly limited to the signing of certificates, CRLs / ARLs (cf. chapter 1.4.1.2 and 7.1.2).

The usage of the private key and of the associated issued certificate is strictly limited to the service defined in chapters 1.4.1.1, 4.5 and 7.2.2.

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

The beneficiary must protect his private keys so that they are not disclosed. It is up to him to ensure that maintenance is performed on the workstation that is used; in particular relative to the system's stability, and the absence of viruses, worms and Trojan horses. He must also select hardware and software that offers efficient security to ensure the protection and usage of his private keys in compliance with the provisions of the present chapter 6.

6.2.1 Security standards and measures for cryptographic modules

6.2.1.1 The CA's cryptographic modules

The cryptographic modules used by the CA for the generation and implementation of its signature keys, as well as, if relevant, for the generation of the keys for future certificates, are cryptographic modules that at least meet the requirements of chapter 11 below with regard to the security level in question.

The hardware cryptographic module used for the generation and implementation of the keys of the Authorities is evaluated by the Common Criteria as being on level EAL 4+, and qualified on the enhanced level by the ANSSI.

6.2.1.2 Cryptographic devices for servers

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

When a cryptographic device is provided by the CA:

- Morpho IDeal Citiz (Morpho ypsID S3 Identity Card), CC EAL5+, SSCD, Qr.

Otherwise the CA ensures, with the server officer, that the system implemented by the server is compliant, through a clear and explicit contractual commitment from the SCO to the CA.

6.2.2 Verification of the private key by several persons

This chapter relates to the verification of the CA's private key for export / import out of / into a cryptographic module. The key pair's generation is covered in chapter 6.1.1.1, the private key's activation in chapter 6.2.8 and its destruction in chapter 6.2.10.

Several persons verify the production operations for the CA's keys. The data used for their creation are shared by several people. The secret for the generation or regeneration of the CA's key is shared between three (3) people.

6.2.3 Escrowing of the private key

Only private keys related to certificates with encryption usage may be escrowed, in accordance with the key escrow and recovery requirements defined in clause 4.12.

6.2.4 Backup copy of the private key

An identified entity can make backup copies of its own electronic signature or confidentiality keys under its sole, exclusive and entire responsibility. If relevant, the backed up keys must be saved in an encrypted form, as well as logically or physically protected against any unlawful access. The protective measures applied to the backed up key must be at least on the same level as those taken for the original key.

6.2.5 Archiving of the private key

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

The private keys of the issued certificates are not archived in any way, neither by the CA nor by any of the PKI components.

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

6.2.6.1 Private keys of the Authorities

For the CA private keys, every transfer is made in encrypted form, in compliance with the requirements of chapter 6.2.4.

6.2.6.2 Private keys of the servers

When the SCO requests a cryptographic device, the key pairs are generated under the Registration Authority's control, directly within the server's hardware device.

6.2.7 Primary key storage in a cryptographic module

The locking procedure and the procedure for placing secrets under control are specified as shown below:

- The CA's private keys are generated in the cryptographic module while using fixed or random data introduced from the exterior; they are then retained in encrypted form, while only being in plain language when needed for their usage.
- The private keys of identified modules are, whenever possible, generated by a local means. Should it be necessary for the recovery service to introduce a key pair from the exterior, it will be introduced in encrypted form and unencrypted locally, within the cryptographic resource itself, if one exists. The private keys of the identified entities are retained in encrypted form, whenever possible, while only being in plain language when needed for their usage.

6.2.8 Private key activation method

6.2.8.1 CA private keys

The activation method for the CA private keys within a cryptographic module responds to the requirements defined in chapter 11 in terms of the security level in question.

The activation of the CA private keys in the cryptographic module is controlled by means of activation data (cf. chapter 6.4), and involves at least two persons in trust roles (for example, security manager and operator).

The activation is indicated on the level of the CPS.

6.2.8.2 Private keys of the servers

When the SCO request a cryptographic device, the key pairs are activated with the use of an activation code having at least 4 characters.

In the case of software keys, if the CA generates the activation code, the key pairs are activated via a PKCS12 password with at least 12 characters.

6.2.9 Private key deactivation method

6.2.9.1 CA private keys

The deactivation of CA private keys in a cryptographic module is automatic as soon as the module's environment changes: stoppage or disconnection of the module, disconnection of the operator, etc.

A CA private key can also be deactivated after a certain period of inactivity. These deactivation conditions respond to the requirements defined in chapter 11 in terms of the security level in question.

The deactivation is indicated on the level of the CPS.

6.2.9.2 Private keys of the servers

The deactivation method is that of the server cryptographic device.

6.2.10 Destruction method for private keys

6.2.10.1 CA private keys

When the CA destroys its private key, it re-initialises the cryptographic module; this implies a complete rewrite of all types of memory in the cryptographic module. It also destroys all of the generation secrets that had been shared.

To destroy the private key, all copies of the private keys must be overwritten, whatever their medium. When the re-initialisation is not be possible after a hardware breakdown, the latter is destroyed. This destruction is tracked by means of a destruction report.

The destruction procedures for private keys are described in the CPS.

6.2.10.2 Private keys of the beneficiaries

Once the private keys have been provided to the beneficiary, their destruction is his responsibility.

In case of pre-delivery scrapping, the certificates are revoked, the medium is destroyed, and this destruction is the subject of a report archived in the beneficiary's file.

6.2.11 Cryptographic module security evaluation level

The CA's cryptographic resource is evaluated on level EAL 4+, according to the Common Criteria and qualified as being on a strengthened level.

The cryptographic devices of the beneficiaries are evaluated on the level corresponding with their intended use, as stipulated in chapter 12 below. Refer to chapter 6.2.1.2.

6.3 OTHER ASPECTS OF THE MANAGEMENT OF KEY PAIRS

6.3.1 Archiving of public keys

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

6.3.2 Lifespan of the key pairs and certificates

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

The lifespan of the keys is defined in the [PROFILES] document, chapter 5.3

General
Lifespan of the certificates
The usage of CA keys (4096 bits) in order to issue certificates is limited to ten (10) years. The maximum lifespan of a certificate issued by the CA is three (3) years and four (4) years for time-stamped units.

6.4 ACTIVATION DATA

6.4.1 Generation and installation of activation data

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

The generation and installation of a PKI cryptographic module's activation data is performed during this module's initialisation and customisation phase. These activation data are known only to the managers identified by name as part of the roles assigned to them (cf. chapter 5.2.1).

6.4.1.2 Generation and installation of activation data corresponding with the private key of the server

If the CA generates the server's key pairs, the key pairs are activated via a PKCS12 password with at least 12 characters.

When the SCO installs the PKCS12, changing the password is recommended.

If the SCO retains the PKCS12 for archiving, this archiving is under his sole responsibility.

When the SCO request a cryptographic device, the key pairs are activated with the use of an activation code having at least 4 characters.

6.4.2 Activation data protection

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

The activation data generated by the CA for the PKI's cryptographic modules are protected in terms of integrity and confidentiality, until their delivery to the recipient. This recipient is then responsible for ensuring their confidentiality, integrity and availability.

6.4.2.2 Protection of activation data corresponding with the private keys of the servers

If the CA generates the activation data, these activation data are not retained by the CA, they will be recalculated whenever necessary by a derivation function on the basis of the medium used.

The activation data are never printed in plain language, a secure envelope ensures confidentiality until delivery to the beneficiaries.

Once the activation data have been printed, the CA can no longer request that they be re-printed.

6.4.3 Other aspects related to activation data

The present CP includes no specific requirement on this subject.

6.5 SECURITY MEASURES FOR IT SYSTEMS

6.5.1 Technical security requirements specific to IT systems

The PKI systems made available to the CA offer the following functions, depending on the role assigned to the operator:

- access control to the PKI services;
- rigorous distinction of the tasks;
- usage of cryptography to ensure the security of communications;
- protection against IT viruses, including worms and Trojan horses;
- audit functions, ensuring accountability and knowledge of the nature of the completed actions;
- archiving of the PKI histories and verification logs;
- verification of the security-related events;
- management of post-error recovery.

These functions can be provided by the operating system, or by a combination of functions offered by the operating system, the PKI system and the physical protection mechanisms.

The interface between the PKI and the CA must also be secured in order to avoid any alteration or intrusion during the data transmission between the two.

The CA undertakes to bring its practices into compliance with the ANSSI documents relative to the protection of the RA's application workstation and the CA workstation.

6.5.2 IT systems security evaluation level

The minimum level of available security assurance is defined in the CPS.

6.6 SECURITY MEASURES FOR THE SYSTEMS DURING THEIR LIFECYCLE

6.6.1 Security measures linked to the development of the systems

The set-up of a system in order to implement the PKI components is documented and respected insofar as possible in keeping with the modelling and implementation standards. The configuration of the system and components, as well as any modification and upgrade, are documented and verified.

6.6.2 Measures related to security management

The CA applies a configuration management method in order to install the cryptographic core of the CA and to ensure its maintenance. When run for the first time, the CA program provides a method that will allow the CA or any other formally authorised person to check if the program installed on the system:

- comes from the company that developed it;
- was not modified before being installed;
- properly corresponds with the desired version.

The CA or any formally authorised person provides for a mechanism that will make it possible to periodically verify the integrity of the software programs.

The CA or any formally authorised person also implements mechanisms and/or policies that will provide for control and surveillance of the PKI system's configuration.

Every development is documented and appears in the internal operating procedures, and is compliant with the maintenance outline for the compliance assurance, in the case of evaluated products.

6.6.3 Security evaluation level of the systems lifecycle

The present CP includes no specific requirement on this subject.

6.7 NETWORK SECURITY MEASURES

The PKI systems are protected against attacks coming from any network, particularly open networks. Such protection is provided by the installation of security gateways configured such as to only allow the usage of protocols and commands that are needed for the proper operation of the PKI.

The CA defines the protocols and orders in the CPS.

6.8 TIME-STAMPING / DATING SYSTEM

In the CPS, the CA indicates the technical provisions that will provide for the time-stamping of the events related to the activity of the PKI components.

Certinomis SA with a registered capital of 40,156€
Head office: 10 avenue Charles de Gaulle
94220 Charenton. Créteil TCR B 433 998 903

7 PROFILES OF THE CERTIFICATES, OCSP AND OF THE CRLS

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

The exact format of the CA certificates is provided in the [PROFILES] document, chapter 2.1.

The exact format of the issued certificates is provided in the [PROFILES] document, chapter 2.3.

The exact format of the issued CRLs is provided in the [PROFILES] document, chapter 3.

Certinomis SA with a registered capital of 40,156€
Head office: 10 avenue Charles de Gaulle
94220 Charenton. Créteil TCR B 433 998 903

8 COMPLIANCE AUDIT AND OTHER EVALUATIONS

The present chapter only relates to the audits and evaluations of the CA's responsibility in order to ensure the proper operation of its PKI.

8.1 FREQUENCY AND/OR CIRCUMSTANCES OF THE EVALUATIONS

Before the first commissioning of a component of its PKI or after any significant modification within a component, the CA performs a compliance check of this component.

On a regular basis, i.e. once every two years, the CA also performs a compliance check of its overall PKI.

Internal controls are performed in order to ensure the PKI's proper operation between 2 compliance audits.

8.2 IDENTITIES / QUALIFICATIONS OF THE EVALUATORS

The CA assigns a component's verification to the team of auditors with competence in IT system security, and in the activity domain of the components undergoing the verification.

8.3 RELATIONS BETWEEN EVALUATORS AND THE EVALUATED ENTITIES

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

8.4 TOPICS COVERED BY THE EVALUATIONS

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

8.5 ACTIONS TAKEN AFTER THE CONCLUSIONS OF THE EVALUATIONS

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

- "success",
- "failure",
- "to be confirmed".

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

- In case of failure, and depending on the scope of the non-compliances, the audit team provides the CA with recommendations that can include cessation (temporary or definitive) of the activity, revocation of the component's certificate, revocation of all certificates issued since the last positive control, etc. The CA decides on the measure to be applied, that must be in compliance with its internal security policies.

- In case of a “To be confirmed” result, the CA provides the component with an opinion that indicates the timeframe for resolving the non-compliances. A “Confirmation” control will then serve to verify that all of the critical points have been resolved.
- In case of success, the CA provides the evaluated component with confirmation of its compliance with the requirements of the present CP and the associated CPS.

8.6 COMMUNICATION OF THE RESULTS

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

9 OTHER BUSINESS LINE AND LEGAL ISSUES

9.1 RATES

9.1.1 Rates for the delivery or renewal of certificates

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

9.1.2 Rates for accessing the certificates

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

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

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

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

9.1.4 Rates for other services

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

9.1.5 Reimbursement policy

No particular requirement.

9.2 FINANCIAL LIABILITY

9.2.1 Insurance coverage

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

9.2.2 Other resources

No particular requirement.

9.2.3 Coverage and guarantee regarding the user entities

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

9.3 CONFIDENTIALITY OF PERSONAL DATA

9.3.1 Perimeter of the confidential information

The following information is considered to be confidential:

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

9.3.2 Information outside of the perimeter of confidential information

No particular requirement.

9.3.3 Responsibilities in terms of the protection of confidential information

The CA applies security procedures in order to guarantee the confidentiality of the information characterized as such in §9.3.1, in particular with regard to the definitive wiping or destruction of the media used for their storage. During any data exchange, the integrity is guaranteed by a means suited to the type of information (encryption, signature, secure envelope...).

The CA can also make the registration files of the beneficiaries available to third parties within the framework of legal proceedings. These files are also accessible to the beneficiary and to the CAG in compliance with §9.4.1.

9.4 PROTECTION OF PERSONAL DATA

9.4.1 Personal data protection policy

Law n°78-17 of 6 January 1978 relative to information technology, files and freedoms, amended by law n° 2004-801 of 6 August 2004 relative to the protection of natural persons regarding the processing of personal data, applies to all documents held or transmitted by the CA or by one of the PKI components (CNIL site http://www.cnil.fr).

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

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

The CA rigorously complies with all applicable legal requirements and, on its website, explains the concrete provisions for the application of the law, notably in the “legal information” and “access right” headings.

The Certification Policy complies with the fundamental principles relative to the protection of personal data as ratified by law, in European directive 2002/58/EC and in any other international agreement that has come into force.

9.4.2 Information of a personal nature

All data gathered and held by the CA or a RA with regard to a natural or legal person (for example: registration procedure, revocation, other recorded events, correspondence exchanged between the beneficiary and the CA or RA, etc.) are considered to be confidential and cannot be disclosed without the beneficiary’s prior consent.

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

The Certificate Revocation Lists only contain the registration numbers and revocation dates of the certificates. The causes for revocation of the certificates are to remain strictly confidential.

9.4.3 Information of a non-personal nature

No particular requirement.

9.4.4 Responsibility in terms of the protection of personal data

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

9.4.5 Notification and consent to use personal data

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

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

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

9.4.7 Other circumstances for the disclosure of personal information

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

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

9.5 INTELLECTUAL AND INDUSTRIAL PROPERTY RIGHTS

All intellectual property rights held by Certinomis are protected by law, regulations and other applicable international agreements. Civil and criminal liability can result from non-compliance with them. For example, in compliance with law n°98-536 of 1 July 1998 (Official Journal of 2 July 1998, p.10075) and European directive 96/6/EC of 11 March 1996, the databases produced by Certinomis are protected. The text of the law can be consulted on the following site: http://www.legifrance.gouv.fr

9.6 CONTRACTUAL INTERPRETATIONS AND GUARANTEES

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

The various PKI components must:

- protect their private keys and the integrity and confidentiality of their possible activation data;
- only use their public and private keys for the purposes for which they were issued, and with the appropriate means;
- implement multi-factor authentication mechanisms for accounts able to issue certificates directly.
- implement technical means and employ the human resources needed for the realisation of the services to which they have committed;
- document their internal operating procedures;
- adhere to and apply the terms of this CP;
- accept the results and consequences of a compliance check, and in particular, remedy any non-compliances that could be identified; and
- comply with the agreements that bind them with the other entities comprising the PKI.

9.6.1 Certification authorities

The CA is responsible relative to its customers, beneficiaries, certification agents and third party users, for the operations relative to the certification services carried out by any of the PKI components. It guarantees the existing link between an identified entity and a key pair.

The CA sees to it that the RAs acting in its name comply with all relevant provisions of the present Certification Policy, with regard to the operation of the RAs.

The CA sees to it that the certification agents are aware of and have approved the obligations and responsibilities assumed within the framework of their functions.

The CA and the CA's manager comply with all requirements of the present Certification Policy and of the associated CPS. The CA and the CA's personnel must respect the rights of customers, beneficiaries and third party users of certificates in terms of the applicable laws and regulations.

The CA informs the third party users of the revocation of the certificate of a beneficiary or PKI component by transmitting, as quickly as possible, the certificate's revocation to the PKI that is in charge of publishing the Certificate Revocation Lists;

The CA is responsible for transmitting information to the PKI for its customers, certification agents and beneficiaries, relative to the procedures to be followed as part of the lifecycle of the certificates; this notably involves the issue, revocation and withdrawal of certificates.

The CA validates the generation of certificates, sends the information concerning the revocation of certificates and provides the users with the necessary information regarding the renewal of certificates.

The personnel members of the CA and of the RAs must comply with all of the relevant requirements of the present Certification Policy and of the associated CPS. They must respect the rights of customers, beneficiaries and third party users of certificates relative to the laws and regulations in force, and must inform the CA of any problem identified with regard to the availability of the site www.certinomis.fr.

The personnel members of the CA and of the RAs to whom roles are assigned relative to the PKI (CA manager, CA security manager...) must be personally responsible for their actions. The expression "*personally responsible*" means that it can be proven that a person has carried out a given action.

9.6.2 Registration service

A RA complies with all requirements of the present Certification Policy and of the associated CPS. Moreover, a RA:

- looks after certificate requests;
- verifies the personal identification data and the data contained in the certificate;
- provides the CA with the certificate generation, revocation and renewal requests that it has carried out favourably;
- provides the CA with an attributable trace of the validity of this verification;
- in full confidentiality, sends the physical media or activation codes to the beneficiaries; and
- retains and protects, in full confidentiality and integrity, all personal data and identification data collected during the registration procedures.

The RA submits to any technical control and quality audits relative to the procedures that may be requested by the CA or the PMAs that accredit it.

9.6.2.1 Obligations of the certification agent

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

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

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

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

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

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

9.6.3 Beneficiary of certificates

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

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

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

If the beneficiary is an organisation, it must prepare and ensure compliance with a security policy for the IT stations that are used in order to implement the certificates.

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

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

9.6.4 Certificate users

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

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

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

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

9.6.5 Other participants

9.6.5.1 Obligations of the third party user

Before any usage of certificates, notably when the said certificates create legal effect, the third party user must necessarily behave in a reasonable manner: verifying with Certinomis relative to the validity of the certificate upon which he intends to rely, consulting the most recent appropriate Certificate Revocation Lists, while also verifying their expiry date and intrinsic validity, in particular the signature, as well as the certificate's validity on the trust itinerary. Should this obligation not be met,

the third party user assumes all risks for any actions not compliant with the present policy's requirements, with Certinomis not guaranteeing the legal value of the certificates that it has issued and that could have been revoked or that might no longer be valid.

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

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

A third party user must only use the certificates in compliance with the trust itinerary validation procedure, a procedure that is set out in the X.509 and PKIX standards, and determined by the ISO/IEC 9594-8 recommendation.

9.7 GUARANTEE LIMIT

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

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

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

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

9.8 LIMIT OF LIABILITY

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

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

9.9 COMPENSATION

No particular requirement.

9.10 DURATION AND EARLY END OF THE VALIDITY OF THE CP

9.10.1 Duration of validity

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

9.10.2 Early end of the validity

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

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

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

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

No particular requirement.

9.11 INDIVIDUAL NOTIFICATIONS AND COMMUNICATIONS BETWEEN PARTICIPANTS

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

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

9.12 AMENDMENTS TO THE CP

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

9.12.1 Amendment procedures

The CA must verify that any project to modify its CP remains compliant with the requirements of the RGS type CP and with any possible supplementary RGS documents. In case of a significant change, the CA will call for a technical assessment in order to verify its impact.

9.12.2 Mechanism and information period for amendments

9.12.2.1 Advance notice timeframes

- The CA manager provides the beneficiaries and third party users with thirty (30) days of advance notice before undertaking any change of the present policy that, according to the assessment of the policy manager, will have a major impact on them.
- The CA manager provides the beneficiaries and third party users with fifteen (15) days of advance notice before undertaking any change of the present policy that, according to the assessment of the policy manager, will have a minor impact on them.

- The CA manager provides the beneficiaries and third party users with advance notice of seven (7) days relative to a change of the present policy that results in a situation beyond the control of the policy manager, provided that this change has an impact on them.
- The CA manager can modify the present policy without notice to the beneficiaries and third party users when, according to the assessment of the policy manager, these modifications have no impact on them.

9.12.2.2 Dissemination form for the notices

Should a notice be necessary, the CA manager so informs the customers and beneficiaries of the modifications made to the policy, by disseminating the change on the policy manager's website, and by e-mail.

When the opinion is intended for beneficiaries and customers, the notice is disseminated by e-mail if the changes result in a major impact, and disseminated on the website of the CA and of the present policy's manager in all other cases.

9.12.2.3 Period for commentaries

People wishing to express themselves regarding the modifications must submit their comments to the policy manager within timeframes that are less than half the length of the timeframes for notifications indicated in article 9.12.2.1.

9.12.2.4 Processing of comments

No particular requirement.

9.12.3 Circumstances in which the OID must be changed

If, based on the policy manager's assessment, a policy change has a major impact on a significant number of customers, beneficiaries and/or third party users, the policy manager shall establish a new policy with a new object identifier (OID).

9.13 PROVISIONS REGARDING THE RESOLUTION OF CONFLICTS

In case of dispute related to the interpretation, formation or performance of the present policy, and in the absence of an amicable agreement or settlement, the parties confirm the formal and exclusive competence of the Paris courts, notwithstanding multiple defendants, summary order, and activation of guarantees or protective measures.

9.14 COMPETENT JURISDICTIONS

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

9.15 COMPLIANCE WITH LEGISLATION AND REGULATIONS

The legislative and regulatory texts applicable to the present CP are notably the ones listed in chapter 10 below.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Overall agreement

No particular requirement.

9.16.2 Transfer of activities

Cf. chapter 5.8.

9.16.3 Consequences of an invalid clause

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

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

9.16.4 Application and waiver

Any notification having to be provided pursuant to the present policy will be considered to have been provided if it is sent by recorded delivery letter or by fax sent to the declared residence as indicated at the start of the services contract, and will be considered to have been received seven (7) days after the date of the postmark in the event of a recorded delivery letter and one (1) day after the sending date in the event of a fax.

9.16.5 Force majeure

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

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

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

Total or partial strike, lockout, riot, civil disturbance, insurrection, civil or foreign war, nuclear risk, embargo, confiscation, capture or destruction by any public authority, bad weather, epidemic, blockage of transportation or procurement means for any reason whatsoever, earthquake, fire, storm, flooding, water damage, government or legal restrictions, legal or regulatory modifications to the marketing forms, computer breakdown, blockage of electronic communications, including

telecommunication networks, any major scientific discovery that calls into question all or part of the principles of asymmetric cryptography, any consequence of a technological development, that is not anticipated by the CA, and that calls into question the norms and standards of its profession, as well as any case that is independent of the desire of the parties but that would prevent the normal performance of the present contract.

9.17 OTHER PROVISIONS

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

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

The infringement of trademarks or service marks, drawings and models, distinctive signs, copyright (for example: software programs, webpages, databases, original texts, etc.) is sanctioned by articles L. 716-1 et seq of the Intellectual Property Code.

10 APPENDIX 1: REFERENCED DOCUMENTS

10.1 REGULATIONS

Reference	Document
[CNIL]	*Law n° 78-17 of 6 January 1978 relative to information technology, files and freedoms, modified by n° 2004-801 of 6 August 2004*
[DIRSIG]	*Directive 1999/93/EC of the European Parliament and Council of 13 December 1999, on a community framework for electronic signatures.*
[LCEN]	*Law n° 2004-575 of 21 June 2004 on confidence in the digital economy, notably its article 31 regarding the declaration of the provision of cryptology and its article 33 that stipulates the liability regime for electronic certification service providers that provide qualified electronic certificates.*
[ORDER]	*Order n° 2005-1516 of 8 December 2005 relative to electronic exchanges between users and the administrative authorities and between the administrative authorities*
[PSCO_QUALIF]	*Note d'application, Règlement eIDAS : critères d'évaluation de la conformité des prestataires de services de confiance qualifiés, référence XXXX/ANSSI/XXX du XX/XX/XX.*
[QPSCe]	*Decree of 26 July 2004 relative to the recognition of the qualification of electronic certification service providers and to the accreditation of the institutions performing their assessment*
[DécretRGS]	*Decree in application of articles 9, 10 and 12 of order n° 2005-1516 of 8 December 2005.*
[SIG]	*Decree n°2001-272 of 30 March 2001 in application of article 1316-4 of the Civil Code and relative to electronic signatures.*

10.2 TECHNICAL DOCUMENTS

Reference	Document
[RGS]	*Référentiel Général de Sécurité – version 1.0*
[PROFILS]	*Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques DT-FL-1310-002-PC-PROFILS*
[RGS_A1]	*RGS – Fonction de sécurité « xxxx » - Version 3.0.*
[RGS_A4]	*RGS – Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 3.0.*
[CWA14167-1]	*CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1*
[CWA14167-2]	*CWA 14167-2 (2003-10) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP). This PP has been certified EAL4+.*
[CWA14167-3]	*CWA 14167-3 (2003-10) Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)*
[CWA14167-4]	*CWA 14167-4 (2003-10) Cryptographic Module for CSP Signing Operations – Protection Profile (CMCSO-PP). This PP has been certified EAL4+.*

[CWA14169]	*CWA 14169 (2002-04) Secure Signature Creation Devices (SSCD). This PP has been certified EAL4+.*
[EN_CP]	*EN 319 411-1 V1.1.1 (février 2016) Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*
[EN_QCP]	*EN 319 411-2 V2.1.1 (février 2016) olicy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*
[ETSI_SigPol]	*ETSI TR 102 272 - ASN.1 format for signature policies V1.1.1 (December 2003)* *ETSI TR 102 038 - XML format for signature policies V1.1.1 (April 2002)*
[PROG_ACCRED]	*COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – version published at www.cofrac.fr*
[RFC2560]	*IETF - Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol, RFC 2560 - June 1999*
[RFC3647]	*IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - November 2003*
[X.509]	*Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version March 2000 (completed by technical corrections n° 1 of October 2001, n° 2 of April 2002 and n° 3 of April 2004)*
[PP_HORO]	*DCSSI - Profil de Protection - Systèmes d'horodatage EAL3+ DCSSI PP 2008/07*
[972-1]	*DCSSI - Guide Technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter – N° 972-1/SGDN/DCSSI du 17/07/2003*

Certinomis SA with a registered capital of 40,156€
Head office: 10 avenue Charles de Gaulle
94220 Charenton. Créteil TCR B 433 998 903

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

11.1 REQUIREMENTS REGARDING THE SECURITY OBJECTIVES

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

- if the key pairs of the issued certificates are generated by this module, guaranteeing that these generations are carried out exclusively by authorised users and guaranteeing the cryptographic sturdiness of the generated key pairs;
- if the key pairs of the issued certificates are generated by this module, ensuring the confidentiality of the private keys and the integrity of the private and public keys when they are under the responsibility of the CA and during their transfer to the beneficiary's cryptographic device, and ensuring their secure destruction after this transfer;
- ensuring the confidentiality and integrity of the CA's signature private keys throughout their lifecycle, and ensuring their secure destruction at their end-of-life;
- being able to identify and authenticate its users;
- limiting access to its services according to the user and role assigned to the latter;
- ability to carry out a series of tests in order to verify that it is running correctly and filling out a report if an error is detected;
- making it possible to create a secure electronic signature in order to sign the certificates generated by the CA, that does not reveal the CA's private keys and that cannot be falsified with knowing these private keys;
- creating audit records for each modification relating to security;
- if a backup and restoration function for the CA's private keys is offered, 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 detects attempted physical alterations and fills in a report when an attempted alteration is detected.

11.2 QUALIFICATION REQUIREMENTS

The cryptographic module used by the CA is the subject of a qualification, on a strengthened level according to the process described in the [RGS], and is compliant with the requirements of chapter 11.1 above.

12 APPENDIX 3: REQUIREMENTS OF THE CRYPTOGRAPHIC DEVICE

12.1 REQUIREMENTS REGARDING THE SECURITY OBJECTIVES

Used by the beneficiary in order to store and implement its private key and, if relevant, to generate its key pair, the cryptographic device must meet the following security requirements:

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

Besides, organizational, procedural or technical security measures must be organized to:

- 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;
- making it possible to guarantee the public key's authenticity and integrity when exported outside of the device.

Confidentiality
Security goals
The protection means of the beneficiary secret elements shall complies to these additional requirements: • ensures the decryption function of symmetric keys for files or messages is only for the legitimate beneficiary and protect the private key against any use by third party; • ensures the authenticity and integrity of symmetric keys for files or messages, when deciphered and exported outside of the device for uses by the data decryption software. • When applicable, ensures confidentiality, authenticity and integrity of the private key when exported outside of the device for uses by key escrow or key archiving functions.

Seal
Security goals
The protection means of the beneficiary secret elements shall complies to these additional requirements: • Ensures that the electronic seal generation function is only used by the legitimate server and the protection of the private key against any uses by third parties.

Server Authentication
Security goals
The protection means of the beneficiary secret elements shall complies to these additional requirements: • ensures the authentication function and the decryption function of session symmetric keys are only used by the legitimate server and protect the private key against any use by third party; • ensures the authenticity and integrity of session symmetric keys when deciphered and exported outside of the device for uses by the data decryption software.

12.2 QUALIFICATION REQUIREMENTS

EASY CA
Certification of the systems
When the cryptographic device is provided by the CA, the latter is qualified at the enhanced level, according to the process described in the [RGS], and is compliant with the requirements of chapter 12.1 above. Otherwise it is recommended to use a device that is qualified to the elementary level.

EASY STANDARD
Certification of the systems
When the cryptographic device is provided by the CA, the latter is qualified at the enhanced level, according to the process described in the [RGS], and is compliant with the requirements of chapter 12.1 above. Otherwise it is recommended to use a device that is qualified to the standard level.
Certification of the systems for AATL
When the cryptographic device is not provided by the CA, the latter shall be qualified as a minimum to FIPS 140-2 Level 2 or CWA 14169 (SSCD) and comply with the requirements of chapter 12.1 above. It is recommended to use a device that is qualified to the enhanced level.

PRIME CA
Certification of the systems
When the CA provides the cryptographic device, the latter is qualified at the enhanced level, in accordance with the process described in the [RGS], and is compliant with the requirements of chapter 12.1 above. Otherwise, if the CA does not provide the cryptographic device, it is recommended to use a device qualified at the enhanced level.
Certification of the systems for AATL
When the cryptographic device is not provided by the CA, the latter shall be qualified as a minimum to FIPS 140-2 Level 2 or CWA 14169 (SSCD) and comply with the requirements of chapter 12.1 above. It is recommended to use a device that is qualified to the enhanced level.
Certification of the time-stamping units
When the CA does not provide the cryptographic device, it must comply with the requirements of [PSCO_QUALIF] clause 5.3.5.