CERTIFICATION POLICY

Certification Authority

"CertEurope eID Root"

Identification (OID): 1.2.250.1.105.22.1.0

Version: 1.0
Update: 00
Creation date: November 14, 2016
Last updated: November 14, 2016
Document status: Official
Drafted by: CertEurope
Verified by: PKI Committee
Approved by: PKI Committee

CertEurope, an Oodrive company
www.certeurope.fr
26, rue du Faubourg Poissonnière, 75010 Paris – France
Tel: +33 (0)1 45 26 72 00 / Fax: +33 (0)1 45 26 72 01

MODIFICATIONS

Date	Status	Version	Comments
11/14/2016	Official	1.0	

CONTENTS

I. Introduction

I.1. Overview

CertEurope provides the option of certifying the signature keys of Certification Authorities using its Root Certification Authority, CertEurope eID Root. This option offers:

- on one hand, the sharing of one single Root Certification Authority among different CAs
- on the other hand, a mutual recognition vector for subscription certificates issued by different subordinate Authorities.

The Certification Policy defined in this document describes the obligations of the parties involved in the service of certifying the signature keys of subordinate Authorities.

In accordance with this policy, certificates will only be issued to Certification Authorities. The issuance of a certificate on behalf of a subscribed natural person is excluded.

The Root CA CertEurope eID Root CA shall be subject to the laws and regulations in force on French Republic territory, as well as the European standards in force and international conventions signed by France, and which affect the application, development, interpretation and validity of certification policies mentioned in this document.

The Root CA CertEurope eID Root CA reserves the right to enter into cross-certification agreements with one or several third-party certification authorities.

This Certification Policy applies to the issuance and use of Certification Authority certificates.

This policy has been designed to be used in certain situations, and indicates the specific roles and responsibilities

- of the Root CA,
- of the registration authority,
- and of subordinate CAs.

This document has been created based on the French Government Certification Policy (GSS).

I.2. Document Identification

This CP is identified by the OID 1.2.250.1.105.8.1.1.0.

The Certification Policy and the Certification Practice Statement are hereinafter referred to as the “CP” and the “CPS”.

- Iso(1)
    - member-body(2)
        - fr(250)
            - type-org(1)
                - CertEurope (105)
                    - CertEurope eID Root (8)
                        - CertEurope eID Root (1) CP
                            - Major version (1)
                                - Minor version (0)

I.3. PKI Participants

The Public Key Infrastructure (PKI) is composed of a number of entities, which are described below.

I.3.1. Certification Authorities

The authority to which certification service users give their trust for the purpose of the generation and issuance of certificates is called the Certification Authority, and is listed in the CA document.

A CA is an Electronic Certification Service Provider (ECSP) that issues certificates.

This entity is responsible for certificates signed in its name and for providing the following certification services:

- **Registration service**: verifies the identification data and the authorizations of the natural person, the agent.
- **Certificate generation service**: generates and signs certificates based on the information transmitted by the registration service.
- **Publication and distribution service**: makes available to the various parties concerned the policies and practices published by the CA, the CA certificates, and all other relevant information intended for the agents, excluding information concerning the status of certificates. Subject to the CA's policy, it may also distribute valid certificates to Subordinate CAs.
- **Revocation management service**: processes revocation requests (including applicant identification and authentication) and determines the actions to be taken. The results of this process are distributed via the certificate status information service.
- **Certificate status information service**: provides information about the status of certificates (revoked, valid, etc.) to certificate users.

The Root Certification Authority is responsible for its customers, but also for any person trusting a certificate that it has issued, for the entire certification process, and therefore for the validity of the certificates it issues. As such, it enacts the Certification Policy and validates the Certification Practice Statement, which must identify the obligations of all entities participating in the CA's services.

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

In accordance with this policy, The Root CertEurope eID Root is responsible for:

- creating and signing certificates binding subordinate Authorities and their key pairs
- communicating the status of certificates by means of CRLs
- ensuring that the CP and CPS are complied with by the different components of the Root CA, and the subordinate Authorities

The certificate registration function is one of the essential functions of a PKI, and is ensured by the Registration Authority.

I.3.2. Registration Authorities

The Registration Authority is the link between the Root Certification Authority and the Subordinate Authority. In accordance with this Certification Policy, an RA is responsible for all tasks assigned to it by the CA.

The RA applies procedures for identifying the natural and legal persons responsible for the Subordinate Authority component to be certified, in compliance with the rules defined by the Certification Authority. Its aim is:

- to establish the authority of the applicant
- to distribute the certificate to the person responsible for the Subordinate Authority
- to maintain, administrate, use and protect the machines and software used to fulfill these functions.

The RA also has the task of receiving the certificate revocation requests and must process them.

The RA archives the certificate or revocation application files.

The RA functions are executed by personnel appointed and approved by the root CA responsible person; these personnel are familiar with and comply with the rules, principles and procedures formulated in the CP and CPS.

I.3.3. Certification Agent

The Certification Agent is a natural person duly identified and appointed by the applicant in order to represent them to apply for the creation of a subordinate Certification Authority certificate.

I.3.4. Certificate Bearers

The only bearers of certificates issued by the CA CertEurope eID Root are the entities to which the certificates of subordinate CAs are attached. These entities are represented by their certification agent or their legal representative.

In accordance with this Certification Policy, a subordinate Authority is a legal person that obtains a CA certificate from the services of the Root CertEurope eID.

The subordinate Authority is responsible:

- for the authenticity, accuracy and completeness of the identification data provided to the RA upon registration
- for establishing and ensuring compliance with the security policy on the computer system(s) used to implement the certificate(s) generated by the Root CA as well as the associated private key(s).
- for the protection, integrity and confidentiality of the subordinate Authority's private key, and for any activation data
- for the security of its equipment, software and networks involved in the use of its certificates, the use of its private key and its certificate, which must comply with this Certification Policy.

The subordinate Authority must communicate any information resulting in the revocation of its certificate to the Root CA, via the channels assigned to it, as defined in the CPS.

I.3.5. The certificate users

Certificate users, also known as third party users, rely on the certificates issued by the CA and/or on the digital signatures verified through the use of the certificate.

The users of the subordinate CA's certificates are defined in the CP of the subordinate CA.

I.3.6. Other participants

I.3.6.1. Certification Operator

The Certification Operator (CO) is a component of the ECSP that is responsible for the following services, as stipulated in §I.3.1:

- the certification generation service
- the publication and distribution service
- the service for delivering the activation code to the bearer
- the emergency revocation management service
- the certificate status information service
- the bearer assistance service

The CO must comply with the sections of the CA’s CP and CPS that apply to it.

I.4. Use of certificates

I.4.1. Areas of application

The different possible uses of public keys are defined and restricted by the use of a certificate extension X.509 v3 ("keyUsage" field).

The "keyUsage" field is marked as "critical".

I.4.1.1. Root CA and Subordinate CA Key pairs and Certificates

A public verification key must be used for the purposes of identification, authentication, integrity and/or non-repudiation.

The public verification key of the Root CA is the only key that can be used to verify the signature of a Subordinate CA certificate and CRLs.

The "**keyUsage**" field of the certificate is used in accordance with the profile of certificates and CRLs. This field includes the following values:

For Root CA and Subordinate CA signature key certificates:

- **Certificate signature**
- **CRL signature**

No other use of the key pair is authorized.

I.4.2. Prohibited certificate uses

Subordinate CA certificates cannot be used for anything other than the signature of certificates and of CRLs of subordinate CAs of the CA CertEurope eID Root.

I.5. CP Administration

I.5.1. Entity administering the CP

I.5.1.1. Responsible entity

The company **CERTEUROPE** is responsible for this CP.

CERTEUROPE
26 rue du Faubourg Poissonnière – 75010 Paris
FRANCE

I.5.1.2. Responsible natural person

Monsieur Stanislas de Rémur
Chairman
26 rue du Faubourg Poissonnière – 75010 Paris
FRANCE

I.5.2. Point of contact

All users of certificates issued by this CA may contact CERTEUROPE:

- By post, at the following address:

  CERTEUROPE – Autorité de Certification
  26 rue du Faubourg Poissonnière – 75010 Paris
  FRANCE

  By email, at the following address:
  info@certeurope.fr
- By telephone, at the following number: +33 1 45 26 72 00

I.5.3. Entity determining the compliance of the CPS with the CP

The compliance of the CPS with the CP is determined by CertEurope Management.

I.5.4. Procedures for approving the compliance of the CPS

The compliance of the CPS with the CP is approved by the CertEurope PKI Committee, following the approval process in place. All new versions of the CPS are published immediately.

I.6. Definitions and acronyms

CA	Certification Authority
RA	Registration Authority
FNISA	French Network and Information Security Agency
PA	Policy Authority
C	Country
ECS	European Committee for Standardization
FICISS	French Interministerial Commission for the Security of Information Systems
CN	Common Name
SF	Subscription File
DN	Distinguished Name
CPS	Certification Practice Statement
DSA	Digital Signature Algorithm
EAR	Entité d'Audit et de Référencement (French Auditing and Listing Agency)
CPS	Certification Practice Statement
ETSI	European Telecommunications Standards Institute
PKI	Public Key Infrastructure
PKI	Public Key Infrastructure
CCRL	CA Certificate Revocation List
CRL	Certificate Revocation List
LDAP	Light Directory Access Protocol
CTA	Certification Agent

MD5	Message Digest n°5
MINEFI	Ministry of the Economy, Finance and Industry
O	Organization
CO	Certification Operator
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organization Unit
CP	Certification Policy
PDS	PKI Disclosure Statement
PP	Protection Profile
ECSP	Electronic Certification Service Provider
GSS	Global Security Standard
RSA	Rivest Shamir Adelman algorithm
SGMAP	General Secretariat for the Modernization of Public Action
S/MIME	Secure/Multipurpose Internet Mail Extensions
SN	Serial Number
SSCD	Secure Signature Creation Device
SHA-1	Secure Hash Algorithm One
SHA-256	Secure Hash Algorithm Two
SP	Publication Service
ISS	Information Systems Security
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator

II. PUBLICATION RESPONSIBILITIES

II.1. Entities responsible for the provision of information

The CO is responsible for the following publication services:

- the publication and distribution service
- the certificate status information service

The CO uses a number of channels for disseminating information based on availability requirements.

The channels used are:

1) http://www.certeurope.fr/reference/certeurope_eid_root.crl
2) ldap://lcr1.certeurope.fr/cn=Certeurope%20eID%20Root,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList
3) ldap://lcr2.certeurope.fr/cn=Certeurope%20eID%20Root,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList

II.2. Mandatory publication of information

On behalf of the CertEurope eID Root CA, the CO publicly distributes:

- The current CertEurope eID Root CA Certification Policy (CP), accessible at the following URL: http://www.certeurope.fr/reference/certeurope_eid_root.pdf
- The Certificate Revocation List (CRL).
- The CertEurope eID Root CA's current certificate. This certificate is available on the CertEurope website at the URL https://www.certeurope.fr/chaine-de-confiance. The certificate's digital fingerprint is also available to guarantee integrity.

II.3. Publication timetables and frequency

The timescales and frequency of publication depend on the information concerned:

- This CP is published as soon as it is validated. It is reviewed as often as necessary.
- The CertEurope eID Root CA 's certificate is released prior to any distribution of subordinate CA certificates and/or CRLs within 24 hours.
- For certificate status information, see §IV.9 and §0.

The availability requirements for the systems that publish this information depend on the information concerned:

- For information related to the PKI (new version of the CP, forms, etc.), the systems must be available business days with a maximum period of non-availability due to service interruptions (breakdowns or maintenance) of 8 hours (business days) and a total maximum duration of non-availability per month of 32 hours (business days), except in cases of force majeure.
- For CA certificates, the systems must be available 24 hours a day, 7 days a week with a maximum period of non-availability due to service interruptions (breakdowns or maintenance) of 2 hours and a total maximum duration of non-availability per month of 8 hours, except in cases of force majeure.
- For certificate status information.

Note that a loss of integrity of information which has been made available (the presence of the information and the integrity of its content) is considered to constitute the non-availability of this information, and that the above requirements also apply to the availability of information published on these systems.

II.4. Control of access to published information

All information published for the benefit of certificate users is accessible on a read-only basis.

Write access to certificate status information publication systems (adding, deleting or modifying published information) is strictly limited to authorized internal PKI functions, with strong access control (certificate and password).

Write access to other information publication systems is strictly limited to authorized internal PKI functions, with strong access control **(**certificate and password).

III. Identification and authentication

III.1. Naming

III.1.1. Types of names

The names used comply with the specifications of the X.500 standard.

In each X509v3 certificate, the CA CertEurope eID Root CA (issuer) and the bearer (subject) are identified by a X.501 "Distinguished Name" (DN) in accordance with the requirements stipulated in the document [PROFILS].

III.1.2. Need for names to be meaningful

The names selected to designate certificate bearers are meaningful.

All characters shall be in the *printableString or UTF8String* format, i.e. using neither accents nor characters that are specific to the French language and in a manner that is compliant with the X.501 standard.

The information contained in the "Subject" field of the Certificate is explicitly described below according to the different X509v3 fields:

- in the "**CountryName**": the characters FR;
- in the "**OrganizationalName**" field:
  The full official name of the entity responsible for the subordinate CA;
- in the "**OrganizationUnitName**" field:
  This field contains the SIREN number for the entity responsible for the subordinate CA. The number is preceded by the number string "0002" and a space.
  If the OrganizationUnitName attribute is present in other instances, these entries must not begin with a 4-number string.
- in the "**CommonName**" field:
  This field contains the name of the subordinate CA.

III.1.3. Pseudonymity of bearers

Not applicable.

III.1.4. Rules for interpreting various name forms

Not applicable.

III.1.5. Uniqueness of names

The uniqueness of a subordinate CA certificate is based on the uniqueness of its serial number within the Root CA's domain. However, different names must be unique within the CA CertEurope eID Root CA. The uniqueness of names is obtained following the rules described in §III.1.2 of this chapter.

The RA guarantees the uniqueness of names used for the certificates of subordinate CAs.

III.1.6. Identification, authentication and the role of trademarks

The right to use a name that is a trademark, business name or service mark or other distinctive mark (trade name, logo, company name) as defined in Articles L.711-1 et seq of the Intellectual Property Code (codified by law no. 92-957 of July 1, 1992 and subsequent amendments) belongs to the rightful owner of that trademark, business name, service mark or other distinctive mark, or its licensees or assignees.

The RA restricts its verifications on the right to use a name to the verification of the information contained in the identification documents, any mandates, the K-bis and the SIRENE notice.

CertEurope disclaims all liability for unauthorized use by customers and subscribers of trademarks, well-known brands and distinctive symbols, as well as domain names.

III.2. Initial identity validation

III.2.1. Method for proving the possession of the private key

Key pairs of subordinate CAs are generated under the control of the CO.

III.2.2. Validation of the identity of an organization

See §III.2.3.

III.2.3. Validation of the identity of a subordinate CA bearer

The RA verifies the identification of the organization, its legal representative and all persons appointed by the latter, directly or indirectly, to represent it before the CA CertEurope eID Root CA or the RA.

The identity of the person behind the CA certificate request is validated by the RA, during a face-to-face meeting with the certification agent.

The CA or RA must archive all relevant information relating to the registration.

III.2.4. Non-verified bearer information

Not applicable.

III.2.5. Validation of the authority of the applicant

For any requests for a subordinate CA certificate made on the basis of belonging to an organization, said request must be confirmed in writing by the legal representative of the organization in question.
In the case of a certification agent, the RA ensures the powers of the latter.
The content of the request for a subordinate CA certificate is described in chapter §IV.1.2.

III.2.6. Criteria for CA inter-operation

Not applicable.

III.3. Identification and validation for re-key requests

III.3.1. Identification and validation for the re-key of a current certificate

Not applicable.

III.3.2. Identification and validation for a re-key following a revocation

Following the permanent revocation of a certificate, a subordinate CA certificate may not be renewed.

III.4. Identification and validation of a revocation request

A request for revocation may only be presented by an authorized entity and is authenticated by the RA or the CA CertEurope eID Root CA.

In the event of a subordinate CA certificate having to be revoked, the responsible person from the subordinate CA must inform the CA CertEurope eID Root as soon as possible.

IV.Certificate life cycle operational requirements

IV.1. Request for a Certificate

A subordinate CA certificate is requested by means of a contract agreed between the requesting organization and CERTEUROPE.

CERTEUROPE may also submit a request for a subordinate CA certificate. In this case, the request is formalized through the establishment of a statement during the key ceremony necessary for the creation of the subordinate CA and the corresponding key pair.

IV.1.1. Origin of the request

A subordinate CA certificate is requested by the requesting organization's legal representative or by a person appointed by this organization.

IV.1.2. Processes and responsibilities for establishing a request for a certificate

If it does not come from CERTEUROPE, a certificate request comprises:

- a written request signed by the legal representative or the certification agent
- a statement by the applicant, accepting their commitments
- a postal address for the organization responsible for the subordinate CA
- the name of the person responsible for the subordinate CA certificate
- the subordinate CA's public key to be certified
- the identification data for the organization (DN X509)
- The type of certificates issued by the new subordinate CA (natural person certificate, server certificate, CA certificate, etc.)
- The uses of certificates issued by the new subordinate CA (signature, authentication, encryption, etc.).

IV.2. Certificate application processing

IV.2.1. Execution of the identification and validation process for the request

The RA verifies the identity and powers of the certification agent.

IV.2.2. Approval or rejection of the request

The request is accepted or rejected before the key ceremony. The applicant's face-to-face meeting with the RA constitutes acceptance of the certificate and obligations binding the CA CertEurope eID Root CA.

IV.2.3. Time to generate the certificate

A subordinate CA's certificate is generated during the key ceremony.

IV.3. Delivery of the certificate

IV.3.1. Actions to be taken by the CA regarding the delivery of the certificate

A subordinate CA's key pair and certificate is generated during the key ceremony.

IV.3.2. Notification by the CA of the delivery of the certificate to the bearer

A representative (e.g. certification agent) of the entity responsible for the subordinate CA is present during the key ceremony. As a result, the applicant is systematically notified of the generation of the certificate.

IV.4. Certificate acceptance

IV.4.1. Conduct constituting acceptance of the certificate

At the end of the key ceremony, the certificate is considered to be accepted.

IV.4.2. Publication of the certificate

Subordinate CA certificates are published by the CA CertEurope eID Root on the website http://www.certeurope.fr/.

IV.4.3. Notification by the CA to other entities of the issuance of the certificate

Not applicable.

IV.5. Key pair and certificate usage

IV.5.1. The use of the private key and certificate by the certificate bearer

The use of a subordinate CA's private key and its associated certificate is strictly limited to:

- the signature of EndUser certificates
- the signature of CRLs

Subordinate CAs must strictly observe the authorized uses of the key pairs and the certificates. If they fail to do so, they shall be held liable.
The authorized use of the subordinate CA's key pair and the associated certificate is indicated on the certificate itself, through the extensions concerning key uses.

IV.5.2. The use of the public key and of the certificate by the certificate user

See the preceding section and section I.4. Certificate users must strictly observe the authorized uses of the certificates. If they fail to do so, they shall be held liable.

IV.6. Certificate Renewal

The life of the Certification Authority CertEurope eID Root CA's certificates is thirty years. The Certification Authority CertEurope eID Root does not allow its certificates to be renewed.

IV.6.1. Possible grounds for renewal of a certificate

Not applicable.

IV.6.2. Origin of a request for renewal

Not applicable.

IV.6.3. Procedure for processing a request for renewal

Not applicable.

IV.6.4. Notifying the bearer of the issue of a new certificate

Not applicable.

IV.6.5. Procedure for accepting a new certificate

Not applicable.

IV.6.6. Publication of a new certificate

Not applicable.

IV.6.7. Notification of other entities by the CA of the issue of the new certificate

Not applicable.

IV.7. Delivery of a new certificate following a change to the key pair

Note - in compliance with [RFC3647], this section addresses the issuance of a new certificate to the bearer in connection with the generation of a new key pair.

IV.7.1. Possible grounds for changes to a key pair

Key pairs generated for subordinate CAs have a life of 20 years.
Moreover, a key pair and a certificate cannot be renewed:

- in advance, in order to guarantee continuity of service
- following the revocation of the subordinate CA certificate (see section IV.9, particularly section IV.9.1.1 for the different possible causes of revocation).

IV.7.2. Origin of a request for a new certificate

The origin of a request for a new certificate is identical to that of an initial request.

IV.7.3. Procedure for processing a request for a new certificate

The procedure for processing a request for a new certificate is identical to that for an initial request (see section IV.3.1)

IV.7.4. Notifying the bearer of the generation of a new certificate

See section IV.3.2

IV.7.5. Procedure for accepting a new certificate

See section IV.4.1

IV.7.6. Publication of a new certificate

See section IV.4.2

IV.7.7. Notification by the CA to other entities of the issuance of the certificate

See section IV.4.3

IV.8. Modification of the certificate

Modifications to CertEurope eID Root CA Certificates are not permitted.

IV.8.1. Possible grounds for modifying a certificate

Not applicable.

IV.8.2. Origin of a request to modify a certificate

Not applicable.

IV.8.3. Procedure for processing a request to modify a certificate

Not applicable.

IV.8.4. Notifying the bearer of the creation of a modified certificate

Not applicable.

IV.8.5. Procedure for acceptance of the modified certificate

Not applicable.

IV.8.6. Publication of the modified certificate

Not applicable.

IV.8.7. Notification by the CA to other entities by the CA of the delivery of the modified certificate

Not applicable.

IV.9. Revocation and suspension of the certificate

A CertEurope eID Root CA certificate can only exist in one of three states: valid, expired or revoked.

IV.9.1. Possible grounds for a revocation

IV.9.1.1. Bearer certificates

The following scenarios may be grounds for the revocation of a subordinate CA certificate:

- the subordinate CA’s private key is suspected of being compromised, has been compromised or has been lost
- the CA CertEurope eID Root CA's private key is suspected of being compromised, has been compromised or has been lost
- modification of information contained in the certificate

- decision to change a component of the Root CA or RA following a non-compliance with CPS procedure
- cessation of activity affecting the subordinate CA
- the CertEurope eID Root CA must be revoked

In addition to the cases for certificate revocation mentioned above, the CA CertEurope eID Root revokes a subordinate CA certificate as soon as it is in possession of information indicating a loss of confidence in a subordinate CA certificate.

More generally, the CertEurope eID Root CA may revoke a subordinate CA certificate of an identified entity if it does not comply with the obligations specified in this CP and in any contract document or any applicable law or regulation.

IV.9.1.2. PKI component certificates

Not applicable.

IV.9.2. Origin of a request to revoke a Bearer Certificate

IV.9.2.1. Bearer certificates

A request to revoke a subordinate CA's certificate may be originated by:

- a certification agent
- a legal representative or entity responsible for the subordinate CA
- the CertEurope eID Root CA

IV.9.2.2. PKI component certificates

Not applicable.

IV.9.3. Procedure for processing a revocation request

IV.9.3.1. Revocation of a bearer certificate

The requirements for the identification and validation of a revocation request are described in section III.4. The revocation request is made by the RA.
The person responsible for the subordinate CA is notified of the publication of the revocation. The grounds for the revocation are not published.

IV.9.3.2. Revocation of certificate issued by a PKI component

Not applicable.

IV.9.4. Revocation request grace period

As soon as the certification agent (or an authorized person) becomes aware that one of the possible grounds for a revocation for one of his or her certificates is effective, he or she must submit a revocation request as promptly as possible.

IV.9.5. Time within which the CA must process a revocation request

IV.9.5.1. Revocation of a bearer certificate

The CertEurope eID Root CA uses all means necessary to process the revocation as quickly as possible, as soon as the revocation request has been authenticated and validated.

IV.9.5.2. Revocation of certificate issued by a PKI component

Not applicable.

IV.9.6. Verification requirements for revocations by certificate users

The user of a certificate issued by the CertEurope eID Root CA is required to verify, prior to use, the status of the certificates throughout the relevant certification chain. The method used (CRL) is available to the user subject to its availability and to the constraints related to its use.

IV.9.7. CCRL issuance frequency

CRLs are published every 24 hours.

IV.9.8. Maximum time limit for publishing a CCRL

The CCRL must be published no later than 30 minutes after it is issued.

IV.9.9. Availability of an online system for verifying revocations and the status of certificates

There is no OCSP server.

IV.9.10. Requirements for the online verification of certificate revocations by certificate users

See section IV.9.6 above.

IV.9.11. Other available means of obtaining information regarding revocations

Not applicable.

IV.9.12. Specific requirements for revocations due to compromised private keys

Not applicable.

IV.9.13. Possible grounds for a suspension

Suspension of certificates is not authorized.

IV.9.14. Origin of a request for a suspension

Not applicable.

IV.9.15. Procedure for processing a request to suspend a certificate

Not applicable.

IV.9.16. Limitations to the suspension period for a certificate

Not applicable.

IV.10. Certificate status information service

IV.10.1. Operational characteristics

Access to the Subordinate CA Certificate Revocation List (in this case, the CRL for the CertEurope eID Root CA is available via the two LDAP V3 directories and via a web server. These CRLs are in “CRL V2” format.

IV.10.2. Service availability

The certificate status information service is available 24 hours a day, 7 days a week.

The maximum period of non-availability due to service interruptions (breakdowns or maintenance) is 2 hours and the total maximum duration of non-availability per month is 8 hours.

IV.10.3. Optional procedures

Not applicable.

IV.11. Termination of the relationship with the bearer

In the event of the termination of the contractual/hierarchical/regulatory relationship between the CertEurope eID Root CA and the subordinate CA prior to the expiry of the certificate, the certificate will be revoked.

IV.12. Key escrow and recovery

IV.12.1. Policy and practices for recovery through key escrow

Not applicable.

IV.12.2. Policy and practices for recovery through session key encapsulation

Not applicable.

V. Non-technical security measures

The various controls described herein aim to ensure, through appropriate risk management, a high level of confidence in the operation of the CertEurope eID Root CA.

V.1. Physical security measures

V.1.1. Geographic location and site construction

The geographic location of the production sites complies with the requirements of the document [CERT_PS].

V.1.2. Physical access

The areas housing the computer systems of the CertEurope eID Root CA are physically protected against unauthorized external access.
There is a list of personnel who are authorized to access these areas. This list is strictly limited to those personnel who require access to ensure the correct operation of the service. Access by authorized personnel is physically monitored and recorded.

V.1.3. Electrical systems and air conditioning

Electrical and air conditioning systems are adequate for the proper operation of the CertEurope eID Root CA's computer systems.

V.1.4. Vulnerability to flood damage

The CertEurope eID Root CA's computer systems are not located in a flood zone, and are not placed in a location that is vulnerable to damage due to flooding or faulty plumbing.

V.1.5. Fire prevention and protection

The premises housing the CertEurope eID Root CA's computer systems are protected against fire (automatic detection and suppression). The physical distribution of the machines makes it possible to ensure maximum service availability.

V.1.6. Media storage

Backup media containing saved or archived data must be retained with a level of security at least equal to that of the systems that generated the original data.
The means used to achieve this objective are stipulated in the CPS.

V.1.7. Decommissioning media

The destruction or resetting of media is to be executed with a level of security at least equal to that of the systems that generated the original data.
The means used to achieve this objective are stipulated in the CPS.

V.1.8. Offsite data backup

The organization of backup data will be structured in such a way as to ensure the most rapid disaster recovery possible, particularly for the services involved in the revocation of certificates.

The information stored offsite must meet the requirements of this CP with respect to preserving the confidentiality and integrity of such information.

The means used to achieve this objective are stipulated in the CPS.

V.2. Procedural security measures

Controls for these procedures have been implemented by the CertEurope eID Root CA and are stipulated in the CPS that corresponds to this CP, structured around the following themes:

V.2.1. Positions of trust

Each component of the PKI must identify at least the following positions of trust:

Head of security: The head of security is responsible for implementing the component's security policy. He or she controls the physical access to the component's system equipment. He or she is authorized to read the archives and is responsible for analyzing the audit logs in order to detect any incident, anomaly, compromise attempt, etc.;

Head of operations/application: The head of operations is responsible, within the component to which he or she is attached, for implementing the PKI's certification policy and certification practice statement at the request level for which he or she is responsible. His or her responsibility covers all the services provided by this application and the corresponding performances.

Operator: An operator within a PKI component ensures the use of applications for the services implemented by the component within his or her area of responsibility.

Systems engineer: he or she is responsible for the initiation, configuration and technical maintenance of the component's IT equipment. He or she ensures the technical administration of the component's systems and networks.

Controller: The person designated by a competent authority whose role is to monitor, on a regular basis, the compliance of the implementation of the services provided by the component with respect to certification policies, the PKI's certification practice statements and the component's security policies.

Secret holder: the person responsible for ensuring the confidentiality, integrity and availability of the private keys entrusted to them.

The general responsibilities of each of these roles are set out in the CPS.

V.2.2. Number of persons required per task

Depending on the task to be carried out, one or more persons must be present during the execution of the task. The CPS will specify, in accordance with risk analysis for each of the tasks related to certificate administration, the number of people and the roles required.

V.2.3. Identification and authentication for each role

Each component of the CertEurope eID Root CA must verify the identity and the authorizations of the personnel who must participate, before:

- his or her name is added to the list of personnel who have physical access to the CA's IT systems;
- an account is opened for him or her on the CertEurope eID Root CA's computer systems.

V.2.4. Roles requiring separation of duties

More than one role may be assigned to the same person, to the extent that the combination of roles does not compromise security functions. For positions of trust, however, it is recommended that the same person not hold multiple roles and, at a minimum, the following restrictions regarding combinations of roles must be respected.

Regarding positions of trust, the following combinations of roles are prohibited:

- head of security and systems engineer/operator
- auditor/controller and any other role
- systems engineer and operator

The functions associated with each role are described in the CPS and comply with the security policy of the relevant component.

V.3. Security measures with respect to personnel

V.3.1. Required qualifications, skills and abilities

All personnel who work within a PKI component are subject to a confidentiality clause with respect to their employer.

Every entity that operates a PKI component must ensure that the responsibilities assigned to its personnel who have been assigned to work within the component are consistent with their professional skills.

The managerial staff must possess the appropriate expertise for their roles and must be familiar with the security procedures in place within the PKI.

The CA must ensure that all members of staff who perform duties related to the operation of a CA:

- are appointed to their position in writing
- are required by contract or by law to comply with the obligations of their position, particularly with respect to confidentiality
- have no duties or interests that may conflict with their obligations with respect to the CA

V.3.2. Background check procedures

Every entity that operates a PKI component uses all legal means necessary to assure the honesty of the personnel who are assigned to work within the component.

These personnel must not have a criminal record that is incompatible with their duties. They must provide their employer with a copy of their criminal record (bulletin n°3), prior to being assigned to a position of trust, then at any time upon request.
Individuals holding positions of trust may not have any conflict of interest prejudicial to the impartiality of their duties.

These background checks must be carried out prior to the assignment of an individual to a position of trust and must be reviewed regularly (at least every 3 years), except for the criminal record.

V.3.3. Initial training requirements

Personnel must be trained in the software, hardware and the safety and operating procedures of the component to which they are assigned.
The CA must ensure that all personnel who perform duties related to the management of the CA have received appropriate training on the CA's principles of operation and security mechanisms, and are familiar with the latest safety rules.

V.3.4. Requirements and frequency with regard to further training

The relevant personnel shall receive information and adequate training prior to any changes to systems, procedures, the structure of the organization, etc., appropriate to the nature of these changes.

V.3.5. Frequency and sequence of rotation between various positions

The CA does not require the rotation of its authorized personnel.

V.3.6. Sanctions for unauthorized actions

In the event of known or suspected misconduct on the part of a member of the CA in the fulfillment of his or her duties, the CA blocks the access of the individual to the CA's systems and, where necessary, takes all appropriate disciplinary action.

V.3.7. Requirements with respect to independent contractors

Requirements with respect to independent contractors shall be governed by contract.

V.3.8. Documentation supplied to personnel

The CA shall ensure that its personnel have access to all laws and contracts that apply to the positions that they hold.
Documents available to personnel include the following:

- the CP supported by the component to which the staff member belongs;
- the CPS appropriate to the area of certification;
- internal operating procedures;
- the user manuals for the hardware and software used.

V.4. Audit logging procedures

Audit logging consists of recording events manually or electronically, through manual or automatic data input. The resulting files, in paper or electronic format, must make it possible to track and attribute operations.

V.4.1. Types of events recorded

Each entity that operates a component of the PKI must, at a minimum, log the following events. These events must be logged automatically, in electronic format, from the moment of startup for all systems related to the functions that the entity operates within the PKI:

- creation/modification/deletion of user accounts (access rights) and the corresponding authentication data (passwords, certificates, etc.)
- startup and shutdown of computer systems and requests
- events related to logging: startup and shutdown of the logging function, changes to log settings, actions taken following a failure of the logging function
- log on and log off attempts by users in positions of trust, and any related unsuccessful attempts

In addition to these log requirements, which are common to all of the components and functions of the PKI, events specific to the various different functions of the PKI are logged, including:

V.4.1.1. Events registered by the RA

The events registered by the RA are:

- receipt of a request for a certificate
- approval/rejection of a request for a certificate
- receipt of a request for a revocation
- approval/rejection of a request for a revocation
- CA requests for and proofs of delivery

V.4.1.2. Events recorded by the CA

The events registered by the CA are:

- events related to CA certificates (generation (key ceremony), backup/recovery, revocation, renewal, destruction, etc.)
- publication and updating of information related to the CA (CP, CA certificates, etc.)
- generation and subsequent publication of CRLs

V.4.1.3. Event description

Each registration of an event in an event log contains, at a minimum, the following fields:

- type of event
- name of the individual or system reference that caused the event
- data and time of the event
- result of the event (failure or success)

V.4.1.4. Accountability

Accountability for action rests with the person, entity or system that executed the action. The name or identifier of the executor is explicitly noted in one of the fields in the event log.
In addition, depending on the type of event, each record also contains the following fields:

recipient or addressee of the operation

- name of the person who requested the operation or the reference of the system that made the request
- name(s) of the individuals present (if the relevant operation required the presence of more than one individual)
- cause of the event
- all information unique to the event (for example, for the generation of a certificate, the series number of the relevant certificate)

Logging operations are performed during the processes.

If the log is created manually, the log for the event must, without exception, be written on the same business day as the event.

V.4.1.5. Other events

Other events are also recorded, either manually or electronically. These are events that concern security and that are not automatically generated by the IT systems, including:

- physical access
- maintenance and system configuration changes
- personnel changes
- actions involving the destruction and reinitialization of media containing confidential information (keys, activation data, personal information regarding bearers, etc.)

V.4.2. Audit log processing frequency

See section V.4.8

V.4.3. Audit log retention period

Events logs must be retained on site for a period of at least 1 month.
They must be archived no later than 1 month following the date of the recorded event.

V.4.4. Audit log protection

The logging process is designed and implemented to limit the risks of the circumvention, alteration or destruction of the event logs. Integrity monitoring mechanisms make it possible to detect any alteration, intentional or accidental, of these logs.

The availability of these logs is protected (against theft and against partial or total destruction, whether deliberate or involuntary). Event logs are accessible exclusively to authorized CA personnel.

The event dating system complies with the requirements of section 0.

V.4.5. Backup procedure for audit logs

Incremental logs are backed up daily using delta compressed storage, and full backups are performed weekly. These logs are subsequently archived by the CA.
Each entity operating a component of the PKI shall implement the necessary measures to ensure the integrity and availability of the audit logs for the component concerned, in accordance with the requirements of the CertEurope Security Policy [CERT_PS] and based on the results of the CA's risk analysis.

V.4.6. Audit log collection system

An automatic event log collection system is in place. This system ensures the integrity, confidentiality and availability of these event logs.

V.4.7. Notification of event recording provided to the individual responsible for the event

Not applicable.

V.4.8. Vulnerability assessment

The event logs are reviewed daily in order to be able to anticipate any vulnerability.

Audit logs are checked at least once every 24 hours, in order to identify discrepancies linked to failed attempts.

The logs are analyzed in their entirety at least once a week and upon detection of a discrepancy. This analysis is used to create a summary in which the important elements are identified, analyzed and explained. The summary will highlight any discrepancies or falsifications that may be discovered.

In addition, a reconciliation between the various audit logs of services that interact with each other (the registration authority and the certificate generation service, the revocation management service and the certificate status information service, etc.) is performed at least once a month, in order to check the correlation between dependent events and thus help to reveal any discrepancies.

V.5. Records archival

V.5.1. Types of records to be archived

The CA archives the following data, and reserves the right to delegate all or part of these obligations to a third party with whom it contracts on the basis of these obligations.

By archiving its own data, the CA ensures the retention of the logs created by the various components of the PKI. This also makes possible the retention of paper documentation related to certification operations, as well as ensuring the availability of these documents where necessary.

The records to be archived are:

- software (executable files) and configuration files for IT equipment
- CPs and CPSs

- contractual agreements with other CAs
- issued and published certificates and CRLs
- receipts and notifications (for information purposes)
- undertakings signed by the CTAs
- bearer identity documents and, where appropriate, the entities with which the bearers are associated
- event logs of the various entities of the PKI

V.5.2. Archive retention period

Certificate application file

Registration files (requests for subordinate CA certificates) are archived for 10 years.

Certificates and CRL issued by the CA

Subordinate CA certificates, as well as CRLs produced by the CertEurope eID Root CA are archived for a period of ten years from the date on which the certificate was generated.

Audit logs

Audit logs are archived for a period of ten years from the date on which the log was generated.
The archiving methods used by the CA provide a level of security at least equal to that provided at the time that the data was generated. In particular, the integrity of the records is ensured throughout the life cycle of the records.

V.5.3. Archive protection

Throughout the whole of the retention period, the archives and their backup copies are:

- protected, in terms of integrity of content
- accessible to authorized persons
- readable and usable throughout their life cycle

V.5.4. Backup procedures for archives

Not applicable.

V.5.5. Requirements for time stamping of records

See section V.4.4 for dating requirements for the audit logs.
Section 0 stipulates the requirements with respect to dating and time stamping.

V.5.6. Archive collection system

Not applicable.

V.5.7. Archive retrieval and verification procedures

Archives (paper and electronic) are retrieved within a period of 2 business days, given that only the CA can access all of the archives (as opposed to an entity operating a component of the PKI, which can retrieve and view only the archives of the component in question).

V.6. CA key changeover

The CertEurope eID Root CA key is valid for a period of 30 years.

As subordinate CA certificates are valid for a period of 10 years, the renewal of the CA key must take place before the end of its period of validity, at the latest. The CA reserves the right to renew its key prior to its expiry date. The decision to renew the key may be taken prior to its expiry date based on various criteria (improvements in cryptographic techniques, longer validity period, etc.).

The new key pair that is generated may be used to sign newly issued subordinate CA certificates and CRLs.

The previous certificate will continue to be usable for validating subordinate CA certificates issued prior to the renewal date until such time as all certificates signed with the corresponding private key have expired.

V.7. Compromise and disaster recovery

V.7.1. Incident and compromise handling procedures

Procedures (awareness raising and training of personnel) and methods for reporting and processing incidents (analysis of different audit logs) are implemented.
In the event of a major incident, such as the loss, suspicion of compromise, compromise or theft of the CA's private key, the triggering event is the discovery of the incident at the level of the component concerned, which must immediately notify the CA. It is imperative that a major incident be handled as soon as it is detected. If the certificate is revoked, this information must be published immediately by any available effective means (media, website, etc.). The CA directly and immediately notifies the contact identified on the website: www.ssi.gouv.frhttp://www.references.modernisation.gouv.fr/.

V.7.2. Recovery procedures in the event of corruption of IT resources (hardware, software and / or data)

In accordance with the risk analysis performed by the CA, the CA is in charge of all IT resources, and has a business continuity plan that describes the recovery procedures.

V.7.3. Recovery procedures in the event of compromise of a component's private key

Cases in which secret elements of other components are compromised are dealt with in the business continuity plan.

V.7.4. Business continuity capabilities following a disaster

The various PKI components have the necessary means available to ensure the continuity of their business, in compliance with the requirements of this CP.

V.8. PKI termination

One or more components of the PKI may cease its activities or transfer these activities to another entity.

The transfer of an activity does not affect the validity of certificates issued prior to the transfer in question, and the resumption of the activity is organized by the CA in collaboration with the new entity.

Cessation of activity is defined as the end of the activity of a PKI component, affecting the validity of certificates issued prior to the termination.

Transfer of activity or cessation of activity affecting a PKI component

The CA components that can terminate their activity without jeopardizing the PKI are the RAs and the CO.

<u>CO component</u>
The contract between the CO and the CA includes a reversibility clause enabling the CA to change operators. In the event of the CO ceasing its business activity, the CA undertakes to transfer the services provided by the CO to another CO.

In particular, the CA shall:

- Create an action plan and address the risk analysis for the CA. In particular, the action plan must address the:
    - transfer of the records archived under the responsibility of the CO
    - transfer of services provided by the CO
    - continuity of services during the transfer
    - transfer of the CA's keys hosted by the CO
    - cancellation of the CO's authorizations to provide emergency revocations
    - modification of the CA's documentary standards: CP, CPS, etc.
    - training of authorized CA personnel
    - communication to other PKI components
    - communication to subordinate CAs and certificate users

- Communicate the action plan to the contact identified on the website www.ssi.gouv.fr, together with any changes that may arise during the transfer.

Cessation of activity affecting the CA

In the event of a total cessation of activity, the CA or, if this is not possible, any entity that can be substituted by virtue of a law, regulation, court decision or an agreement previously reached with this entity, will ensure the revocation of the certificates and the publication of the CRLs in accordance with commitments made in this CP.

During the shutdown of its service, the CA undertakes to:

1) refrain from transmitting the private key that enabled it to issue certificates
2) take all necessary steps to destroy or disable the private key
3) revoke its certificate
4) revoke all of the certificates that it has signed and that are still valid
5) notify all of the CTAs of certificates that have been revoked or that are to be revoked, as well as the entities with which they are affiliated, where necessary (see section III.2.3).

In the event of a planned cessation of activity, the CA will observe a period of 6 months between the administrative notification and the revocation of its CA certificate, and will undertake to enter into specific agreements with other authorities to ensure compliance with the requirements governing the transfer of its archives.

VI.Technical security controls

VI.1. Key pair generation and installation

VI.1.1. Key pair generation

VI.1.1.1. CA keys

CertEurope eID Root CA signature keys are generated in a secure environment (see section V).

CertEurope eID Root CA signature keys are generated during the key ceremony and incorporated into an encryption module that meets the requirements of section XI below for the relevant level of security.
The CA's key ceremony takes place under the supervision of a public ministerial officer, who ensures the proper implementation of the procedures and compliance with the safety requirements set out in this document and in the CPS. It is carried out by a minimum of two people holding positions of trust (see section V.2.1), as part of the "key ceremony". These ceremonies must follow predefined scripts.

CertEurope eID Root CA's keys are generated in an encryption module for which the secret elements already exist and have already been distributed to bearers who have been identified and authorized for this position of trust.

VI.1.1.2. Bearer keys generated by the CA

The key pair is generated directly in a cryptographic module equivalent to that of the CertEurope eID Root CA.

VI.1.1.3. Bearer keys generated by the bearer

Not applicable.

VI.1.2. Delivery of the private key to its owner

Not applicable.

VI.1.3. Delivery of the public key to the CA

Not applicable.

VI.1.4. Delivery of the CA's public key to certificate users

The CA's public key can be downloaded from the CA's website.
The "fingerprint" of the CA's public key certificate makes it possible to establish its authenticity.

VI.1.5. Key size

The RSA subordinate CA keys used have a size of 4096 bits, and will be upgraded as and when changes in technology and/or legislation arise.
The size of the CertEurope eID Root CA's key is 4096 bits.

VI.1.6. Key pair parameter generation and quality verification

A subordinate CA's key pair (for the signature of certificates and CRLs) is generated and protected by a hardware cryptographic module. This module meets the requirements of section XI.

Generating or renewing the CA's key pair using this module requires the presence of at least 3 people.

VI.1.7. Key usage purposes

The use of the private key of the CertEurope eID Root CA and its associated certificate is strictly limited to the signature of subordinate CA certificates, and of CRLs/CCRLs.
The use of a subordinate CA's private key and its associated certificate is strictly limited to the signature of certificates and of CRLs.

VI.2. Security measures for the protection of private keys and cryptographic modules

VI.2.1. Security measures and standards for cryptographic modules

VI.2.1.1. The CA's cryptographic modules

The cryptographic module used by the CA to generate and initiate its signature keys is a cryptographic module that meets the EAL4+ Common Criteria and therefore meets the requirements of section XI below with respect to the level of security of this module **.

VI.2.1.2. The subordinate CA's cryptographic modules

The cryptographic module used by a subordinate CA to generate and initiate its signature keys is a cryptographic module that meets the EAL4+ Common Criteria and therefore meets the requirements of section XI below with respect to the level of security of this module **.

VI.2.2. Control of the private key by more than one person

The control of the CA's private signature keys is ensured by personnel in positions of trust (the PKI's secret holders) and through the use of a tool that implements the sharing of these secrets (systems that require that a minimum of 3 of the 5 authorized users authenticate themselves).

VI.2.3. Escrow of the private key

The CertEurope eID Root CA does not permit either the CA's or the subordinate CA's private keys to be held in escrow.

VI.2.4. Private key backup

An encrypted backup copy of the private CA key is made, incorporating an integrity control mechanism. These backup copies are handled with the same level of security as the original private key.
An encrypted backup copy of a subordinate CA's private key is made, incorporating an integrity control mechanism. These backup copies are handled with the same level of security as the original private key.
The encryption and decryption operations are performed inside the cryptographic module and require the participation of 3 secret holders.

VI.2.5. Private key archival

The CA's private keys are not archived.

Private keys of subordinate CAs are not archived by either the CertEurope eID Root CA or by any PKI component.

VI.2.6. Transfer of the private key into/from the encryption module

For private keys of the CertEurope eID Root CA and of subordinate CAs, any transfer must take place in encrypted format, in accordance with the requirements of section VI.2.4.

VI.2.7. Private key storage on cryptographic modules

Private keys of CertEurope eID Root CA are stored in a cryptographic module that meets the requirements of section XI below for the relevant level of security.
Private keys of subordinate CAs are stored in a cryptographic module that meets the requirements of section XI below for the relevant level of security.

VI.2.8. Private key activation method

VI.2.8.1. Private CA Keys

Activation of the CA's private key requires the presence of at least three secret holders and makes it possible to meet the requirements set out in section XI for the relevant level of security.

VI.2.8.2. Private bearer keys

Activation of a subordinate CA's private key requires the presence of at least three secret holders and makes it possible to meet the requirements set out in section XI for the relevant level of security.

VI.2.9. Method for deactivating the private key

VI.2.9.1. Private CA Keys

Deactivation of a CA's private keys in a cryptographic module takes place automatically as soon as the module's environment changes: module stoppage or disconnection, logging off by the operator, etc.

A private CA key may also be deactivated after a certain period of inactivity. These deactivation conditions make it possible to meet the requirements set out in section XI for the relevant level of security.

VI.2.9.2. Private bearer keys

Deactivation of a subordinate CA's private keys in a cryptographic module takes place automatically as soon as the module's environment changes: module stoppage or disconnection, logging off by the operator, etc.

A subordinate CA's private key may also be deactivated after a certain period of inactivity. These deactivation conditions make it possible to meet the requirements set out in section XI for the relevant level of security.

VI.2.10. Method of destroying private keys

VI.2.10.1. Private CA Keys

The destruction of private CA keys can only take place using a cryptographic module.
At the end of the life of a private CA key, whether through normal expiry or in advance (revocation), the key is systematically destroyed, together with any copies and any elements that could make it possible to reconstitute the key.

VI.2.10.2. Private bearer keys

A subordinate CA's private keys can only be destroyed using the cryptographic module.

At the end of the life of a subordinate CA's private key, whether through normal expiry or in advance (revocation), the key is systematically destroyed, together with any copies and any elements that could make it possible to reconstitute the key.

VI.2.11. Assessment of the level of security of the cryptographic module

The cryptographic module for the CA CertEurope eID Root CA is assessed at security level EAL4+, corresponding to its anticipated use, as specified in section XI below.
The cryptographic module for subordinate CAs is assessed at security level EAL4+, corresponding to their anticipated use, as specified in section XI below.

VI.3. Other aspects of key pair management

VI.3.1. Public key archival

The public keys of the CA CertEurope eID Root CA and of subordinate CAs are archived as part of the archiving of the corresponding certificates.

VI.3.2. Certificate operational periods and key pair usage periods

The life of the key pair and certificate of CertEurope eID Root CA is 20 years.
The life of the key pair and certificate of a subordinate CA is 20 years.

VI.4. Activation data

VI.4.1. Activation data generation and installation

VI.4.1.1. Activation data generation and installation for the CA private key

Activation data for the cryptographic module of CertEurope eID Root CA are generated and installed during the initialization and customization phase of the module.

VI.4.1.2. Activation data generation and installation for the bearer private key

Activation data for the subordinate CA's cryptographic module are generated and installed during the initialization and customization phase of the module.

VI.4.2. Activation data protection

VI.4.2.1. Activation data protection for the CA private key

Following the CA key ceremony, the CA activation data are delivered to several bearers who have the responsibility of ensuring the data's confidentiality, integrity and availability.

VI.4.2.2. Activation data protection for the bearer private keys

Following the subordinate CA's key ceremony, the subordinate CA's activation data are delivered to several bearers who have the responsibility of ensuring the data's confidentiality, integrity and availability.

VI.4.3. Other aspects of activation data

Not applicable.

VI.5. Computer security controls

VI.5.1. Specific computer security technical requirements

The workstations of PKI components require an optimal level of security, and makes it possible to meet the following needs:

- identification and authentication of workstation users
- management of user sessions (disconnection following a period of inactivity, access to files controlled by role and by the name of the user)
- protection against computer viruses
- network protection (confidentiality, integrity, etc.)
- audit functions
- accountability

The minimum level of security achieved should meet these security objectives. Applications using the services of the components may have additional security requirements, which must be taken into account in determining the minimum level of security provided by the workstations.

VI.5.2. Computer security rating

Not applicable.

VI.6. Life cycle technical controls

VI.6.1. System development controls

CA applications have been implemented in strict compliance with the preliminary risk analysis and with the resulting security policy.
The implementation of the CA and its hosting platform has been documented.
Any modification to the CA or its hosting platform must be documented.

VI.6.2. Security management controls

Any changes to the systems are recorded in the CA’s activity log and are reported.

VI.6.3. Life cycle security control ratings

Not applicable.

VI.7. Network security controls

The CA is built on a network protected by at least two levels of security gateways (firewalls). These gateways are configured in such a way as to accept only essential flows.

VI.8. Time stamping / dating system

To date events, the various PKI components use the PKI's time system, ensuring the synchronization of the clocks within the PKI system to within one minute, and, with respect to a reliable source of UTC time, to the nearest second. For operations that are conducted offline (e.g. administration of a Root CA), this level of precision of synchronization with respect to UTC time is not required. The system should, however, be able to order events with sufficient accuracy. Synchronization with respect to time UTC refers to a system that includes two independent time feeds.

VII. Certificate and CRL profiles

The complete profile is detailed in the document [PROFILES_CERTEUROPE] available on the CertEurope website at the URL: https://www.certeurope.fr/chaine-de-confiance

VIII. Compliance audit and other assessments

Annual monitoring audits are conducted, in compliance with the accreditation scheme. To ensure the compliance of its CP with its CPS, the CA conducts internal audits.

The remainder of this section deals only with PKI compliance assessments.

VIII.1. Frequency and / or circumstances of assessment

The CertEurope eID Root CA conducts a compliance audit of the CP at least every two years.

VIII.2. Identity / qualifications of the assessors

The assessment of the component is assigned by the CA to a team of auditors qualified in security and information systems and in the area of activity of the component under assessment.

VIII.3. Assessor's relationship to assessed entities

The audit team does not belong to the entity operating the component of the PKI under assessment, regardless of which component is being assessed, and is duly authorized to perform the required assessments.

VIII.4. Topics covered by the assessments

The periodic assessments conducted by the audit team shall cover the whole of the architecture of the PKI, with the aim of verifying its compliance with the commitments and practices stipulated in the CA's CP and in the corresponding CPS, together with the elements that fall under it (operational procedures, resources implemented, etc.).

VIII.5. Actions taken following the conclusion of the assessments

Following the assessments, corrective actions must be taken in accordance with the outline set out below:
At the conclusion of the compliance assessment, the audit team must provide the assessed entity with an audit report. Any non-compliance issues detected during the audit shall be classified as "notes", "minor non-compliance" or "major non-compliance".

The "notes" and the "minor non-compliance" issues shall be corrected based on the recommendations and within the time frame suggested by the audit team. The CA will specify how and under what time frame the non-compliance issues will be resolved.

The "major non-compliance" issues must be resolved as rapidly as possible, under penalty of the temporary or permanent termination of the activity, depending on the recommendations of the audit team.

VIII.6. Communication of results

The results of the compliance audits shall be made available to the qualification organization responsible for qualifying the CA.

IX. Other business and legal matters

IX.1. Fees

CertEurope reserves the right to bill for the service of creating subordinate CA certificates.

IX.1.1. Certificate issuance or renewal fees

Not applicable.

IX.1.2. Certificate access fees

Not applicable.

IX.1.3. Revocation or status information access fees

Not applicable.

IX.1.4. Fees for other services

Not applicable.

IX.1.5. Refund policy

Not applicable.

IX.2. Financial responsibility

IX.2.1. Insurance coverage

The CertEurope eID Root CA deems it appropriate to maintain a sufficient financial guarantee, dedicated to the payment of any sums that it may owe to users, in the form of professional indemnity insurance. CertEurope declares that it has purchased professional indemnity insurance covering its electronic certification services from the company HISCOX under policy number HA RCP0081352.

IX.2.2. Other assets

Not applicable.

IX.2.3. Extended warranty coverage

Not applicable.

IX.3. Confidentiality of business information

IX.3.1. Scope of confidential information

The following information is considered to be confidential:

- the private keys associated with the certificates
- the grounds for the revocation of the certificates

- the event logs for components of the PKI CertEurope eID Root CA
- the request for subordinate CA certificate
- the audit reports
- the CPS

This data shall not be used and shall not be the subject of external communication except for the sole purpose of the requirements of the management of operations in implementing the CPS associated with this CP, to meet legal requirements or for the execution of works or the provision of services entrusted to the service providers.

The individuals to whom the personal information refers have the right to obtain copies of this information from the RA, and to request correction of this information, if necessary, as specified in the law no. 7817 of January 6, 1978 relating to information technology, computer files and freedoms.

The individuals whose personal data are collected and processed are also entitled to object specifically to the use of their data for purposes other than those stipulated in this CP, in a letter addressed to the address given above.

All personal data collected and held by the PKI or a component is considered confidential and should not be disclosed without the prior consent of the person concerned.

In accordance with Article 33 of the law relating to information technology, computer files and freedoms, as amended, other than with the express permission of the individual concerned, the personal data collected by the CertEurope eID Root CA for the purposes of issuing and conservation of certificates must be provided directly by the individual and may not be used for any other purpose other than the purpose for which they were collected.

Procedures for exemption from this confidentiality policy may be established for particular Communities. Under these circumstances, it is the specific procedures duly validated by CertEurope that shall prevail.

IX.3.2. Information not within the scope of confidential information

Not applicable.

IX.3.3. Responsibility to protect confidential information

The CA is required to comply with the laws and regulations in force on French territory.

IX.4. Privacy of personal information

IX.4.1. Policy for the protection of private information

The CA is required to comply with the laws and regulations in force on French territory, and in particular law [CNIL].

The CA's corresponding policy with respect to information technology and freedoms has included this procedure in the list of procedures carried out by the CA.

IX.4.2. Information treated as private

For the CertEurope eID Root CA, private information means the personal information of the certification agent, registered in the registration file. It is composed of the following information: surname/first name/address/telephone/job title/email.

IX.4.3. Information not deemed private

Not applicable.

IX.4.4. Responsibility to protect of private information

See the laws and regulations in force on French territory.

IX.4.5. Notification and consent with regard to the use of private information

Not applicable.

IX.4.6. Disclosure of private information to the judicial or administrative authorities

See the laws and regulations in force on French territory.

IX.4.7. Other circumstances of disclosure of private information

Not applicable.

IX.5. Intellectual property rights

During the execution of the services defined in this document and/or other contractual document relating to the certification service, material protected by copyright laws may be provided.

These materials, together with the copyright attached thereto, shall remain the property of the relevant copyright holder. The beneficiary of these services shall have the right to reproduce these materials for his or her internal use. However, he or she may not, without the prior authorization of the copyright holder, make available to third parties, extract or reuse in whole or in part, these materials or derivative works or copies thereof, especially software or databases.

Subject to the provisions of this section of the CP, no license, express or implied, is granted by the holder of rights regarding inventions, patents or patent applications owned by him or her and created outside of this document and/or any other contractual document relating to the certification service.

IX.6. Representations and warranties

The obligations common to the components of the PKI are the following:

- to protect and ensure the integrity and confidentiality of their private keys;
- to use their public and private keys only for the purposes for which they were issued and with the specified tools, in accordance with this Certification Policy
- to respect and apply the CP and the CPS with which it is associated with respect to those sections that apply to them
- to submit to compliance checks conducted by CERTEUROPE or any other entity mandated by CERTEUROPE, and to respect the findings and address the non-compliance that these checks may reveal
- to respect the agreements or contracts that bind them to each other as well as to bearers
- to document their internal operating procedures
- to implement the means (technical and human) required to achieve the services that they have undertaken to provide, under conditions that ensure quality and security

IX.6.1. Certification Authorities

The CertEurope eID Root CA guarantees its compliance with the requirements stipulated in this CP as well as in the associated CPS. Where the CA employs external entities to carry out its certification activity, the CA guarantees the compliance of each of these entities with these requirements.

As part of its operational functions, which it may undertake directly or outsource to external entities, the requirements incumbent on the CERTEUROPE CA, as the head of the PKI as a whole, are the following:

- To be a legal entity as defined under French law.
- To be in a contractual/hierarchical/regulatory relationship with the entity for which it administers the certificates of the entity's bearers. The CA may also, where appropriate, be in a contractual/hierarchical/regulatory relationship with the certification agents chosen by the entity.
- To make accessible all the services set out in the CP to promoters of digitized transfer applications for the government, bearers, certificate users, etc., that implement its certificates.
- To ensure that the requirements of the CP and procedures of the CPS are applied by each PKI component and are adequate and in compliance with its standards.
- To conduct a risk analysis to determine the specific security objectives necessary to cover the business risks of the whole of the PKI and the corresponding technical and non-technical security measures to be implemented. The CPS is developed based on this analysis.
- To implement the various functions identified in the CP, especially with regard to the generation of certificates, delivery to the bearer, and the administration of revocations and of the certificate status information service.
- To implement everything that is necessary in order to meet the commitments set out in the CP, especially in terms of reliability, quality and security.
- To generate, and renew when necessary, its key pairs and corresponding certificates (signature of certificates, CRLs). Distribute its CA certificates to the bearers and the certificate users.

The CA CertEurope eID Root CA has an obligation to:

- be able to demonstrate to applications using its certificates that it has issued a certificate for a given bearer and that this bearer has accepted the certificate, in accordance with § IV.4.
- make available for the bearers and users the list of certificates that have been revoked. This list is published as a CRL.
- ensure the consistency between the CP and the associated CPS.

IX.6.2. Registration service

See section IX.6.1.

IX.6.3. Certification Agent

The certification agent has an obligation to:

- provide accurate and up-to-date information when applying for or renewing a certificate.
- inform the CA of any change to the information contained in its certificate.
- immediately request a revocation from the CA CertEurope eID Root CA in the event of the loss, compromise or suspected compromise of a private key.
- immediately and definitively interrupt the use of private keys in the event of compromise.

IX.6.4. Certificate Bearers

Not applicable.

IX.6.5. Certificate users

User applications and users certificates must:

- respect the purpose for which a certificate was issued;
- verify the digital signature of the CertEurope eID Root CA that issued the certificate as well as that of the CertEurope eID Root CA.
- verify the validity of the certificates (validity date and revocation status).
- verify and comply with the certificate user obligations described in this CP.

IX.6.6. Other participants

Not applicable.

IX.7. Disclaimers of warranties

Not applicable.

IX.8. Limitations of liability

Not applicable.

IX.9. Indemnities

Not applicable.

IX.10. Term and Termination

IX.10.1. Term

This document is applicable until the end of life of the last certificate issued under this CP.

IX.10.2. Termination

Barring unforeseen events related to security, modifications to this document do not require the revocation of certificates that have already been issued.

IX.10.3. Effect of termination and survival

Not applicable.

IX.11. Individual notices and communications between the participants

In the event of any change of any type affecting the composition of the PKI, the CA shall have this change validated by commissioning a technical expert to assess the impact on the quality and security of the functions of the CA and its various components.

IX.12. Amendments to the CP

IX.12.1. Amendment procedures

The CA shall verify that any proposed change in its CP shall remain in compliance with the requirements of this CP. In the event of a significant change, the CA may call upon a technical expert to monitor the impact.

IX.12.2. Notification mechanism and period

Not applicable.

IX.12.3. Circumstances under which the OID must be changed

Amendments to this CP shall be reflected in a change of version number, allowing changes to be assessed on 3 levels (for example, version 1.0 Updated 01):

- Major version (1.): corresponds to an important amendment such a change to the CA's keys or a significant or total revision of the CP
- Minor version (.0): corresponds to amendments that have a noticeable impact on bearers or existing users.
- Update number (01): corresponds to amendments that have no noticeable impact on bearers or existing users and do not require the OID of the CP to be changed.

IX.13. Dispute resolution provisions

See the general terms and conditions of subscription. This CP is governed by French law.

All disputes arising under this Agreement may be settled by arbitration if the parties to the dispute agree on this method of resolving the conflict. If this is the case, the rules governing the arbitration shall be those of the ATA (Center of Conciliation and Arbitration for Advanced Techniques, 57, avenue de Villiers 75017 Paris - Tel: +33 (0)1 56 21 10 00 - Fax: +33 (0)1 56 21 10 10 – http://www.legalis.net/ata), which the parties hereby expressly agree to consult.

If this is not the case, the parties shall have recourse to ordinary courts, with the understanding that CertEurope confers jurisdiction on the Tribunal de Grande Instance of Paris, due to the location of CertEurope’s corporate headquarters.

If necessary, including by derogation to the arbitration rules of the ATA, the arbitration award may be appealed in a court of law.

IX.14. Governing law

This Certification Policy is governed by French law.
Any dispute relating to the validity, interpretation or execution of this Certification Policy shall be subject to the competent courts of the Court of Appeal of Paris.

IX.15. Compliance with applicable laws and regulations

See the laws and regulations in force on French territory.

IX.16. Miscellaneous provisions

IX.16.1. Entire agreement

Not applicable.

IX.16.2. Assignment

See section V.8

IX.16.3. Severability

Not applicable.

IX.16.4. Application and waiver

Not applicable.

IX.16.5. Force majeure

All events usually held by the French courts to be acts of force majeure shall be held to be force majeure events under the terms of this CP, including events that are irresistible, insurmountable and unpredictable.

IX.17. Other provisions

Not applicable.

X. Annex 1 – Referenced documents

X.1. Regulations

Law no. 78-17 of January 6, 1978 relating to information technology, files and freedoms.

European directive 95/46/EC relating to the protection of personal information.

European directive (1999/93/EC) relating to electronic signatures was adopted on 12/13/1999.

Law no. 2000-230 of March 13, 2000 adapting the right of proof to information technologies and relating to electronic signatures.

Decree no. 2001-272 of March 30, 2001 with respect to article 1316-4 of the civil code and relating to electronic signatures.

Decree no. 99-199 of March 17, 1999 establishing the categories of cryptographic devices and services for which the procedure of advance declaration is substituted for that of authorization.

Decree no. 99-200 of March 17, 1999 establishing the categories of cryptographic devices and services dispensing with all advance formalities.

Order of March 17, 1999 establishing the form and content of the file concerning the declarations or applications for authorization with respect to cryptographic devices and services.

Order defining the specific provisions that may be provided in the authorization for providing a cryptographic device or service, no. PRMX9802730A of March 13, 1998.

Order defining the form of prior notification by the supplier of the identities of intermediaries used for the provision of cryptographic devices or services submitted for approval, no PRMX9802732A of March 13, 1998.

X.2. Technical documents

Reference	Version	Document titles
[PC RGS]		CP – GSS standard
[PROFILS]		GSS – Certification Policy Types – Profiles of Certificates, CRLs, OCSP and cryptographic algorithms
[ETSI_CERT]		
[RFC3647]		
[RFC3739]		
[CERT_PS]		CertEurope – Security Policy
[PC RGS V2.3]		CP – GSS standard

XI. Annex 2: Security requirements for the CA's cryptographic module

XI.1. Requirements regarding security objectives

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

- if the bearer key pairs for authentication and signature are generated by the module, ensure that these generations are executed exclusively by authorized users and ensure the cryptographic robustness of the key pairs that are generated
- if the authentication and signature key pairs are generated by this module, ensure the confidentiality of the private keys and the integrity of the private and public bearer keys while they are under the responsibility of the CA and during their transfer to the authentication device and the signature of the bearer and ensure their complete destruction following this transfer
- ensure the confidentiality and integrity of the CA's private signature keys throughout the whole of their life cycle and ensure their complete destruction at the end of their life cycle
- be capable of identifying and authenticating its users
- limit the access to its services with reference to the function of the user and the role to which he or she has been assigned
- be capable of running a series of tests to verify that it is functioning correctly and that it enters security mode if it detects an error
- are able to create a secure electronic signature for signing the certificates generated by the CA, which do not reveal the CA's private keys and which cannot be falsified without the knowledge of these private keys
- create audit log entries for each change that affects security
- if a backup and restore function for the CA's private keys is available, ensure the confidentiality and integrity of the backed up data and establish, at a minimum, a dual level of controls over the backup and restore operations

The CA's cryptographic module must detect physical attempts to make alterations and must enter into a secure mode when an alteration attempt is detected.

XI.2. Certification requirements

The cryptographic module used by the CA must, under the conditions anticipated by decree no. 2002-535 of April 18, 2002 relating to the evaluation and the certification of the security offered by information technology products and systems, be certified by the Prime Minister as being in compliance with the requirements of section XI.1 above.
The certification must make it possible to provide assurance that the cryptographic module meets these requirements (equivalent to a level EAL2+ of the common criteria with high resistance mechanisms) and result in a standard level qualification [QUALIF_STD].