Information Security

Certification Policy
« Banque de France AC v3 Racine »
Certification Authority

(OID : 1.2.250.1.115.200.3.1.1.1.1)

Date	***:***	May 28, 2020	***Version***	***:***	1.0
Author	***:***	RSI	***Number of pages***	***:***	47

DOCUMENT CONTROL SHEET

List of versions

Version	Date	Author	Amendment
1.0	28/05/2020	DM - RSI	Initial Version

Document validation: Validated by Banque de France Certification Policies Approval Committee.

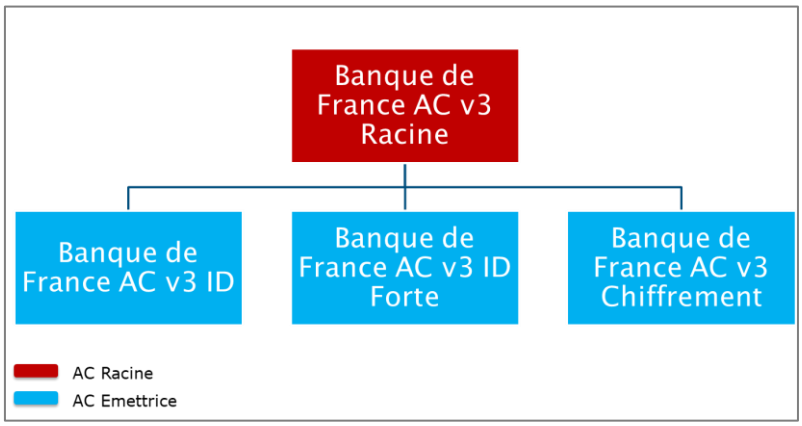
TABLE OF CONTENTS

1. Introduction

1.1. Overview

Banque de France has implemented its own Public Key Infrastructure in order to secure its information system and the exchanges of the various Banque de France business areas.

Banque de France's PKI is based on a certification hierarchy illustrated in the diagram below:



This document constitutes the certification policy (CP) for the "**Banque de France AC v3 Racine**" certification authority of Banque de France and contains the public information of the associated Certification Practice Statement (CPS).

The "**Banque de France AC v3 Racine**" Certification Authority is a self-signed root CA, issuing certificates only to other CA of the same PKI, designated as:

- **Intermediate** : CA issuing certificates to Subordinate CA,
- **Subordinate**: CA issuing certificates to end users (*natural persons and application services*).

This document follows the structure of the General Security Framework and RFC 3647.

All certificate ranges and the CP are structured according to the requirements of ETSI EN 319 411-1 standard relating to the certification authorities issuing certificates.

This CP is intended to be consulted and read by the organizations and persons using these certificates, to enable them to assess the level of trust that they may place in these certificates.

This CP has the status of "public document" under the Banque de France's confidentiality classification and shall be made publicly available in a range of forms, notably in electronic format on the Banque de France website.

1.2. Document name and identification

This CP has the following title:

Certification Policy
Banque de France AC v3 Racine

This CP is identified by the following OID : 1.2.250.1.115.200.3.1.1.1.1 and includes the certificate types identified by the following OIDs:

Certificate usage	CP OID
Intermediate or Subordinate Certification Authority	1.2.250.1.115.200.3.1.2.1.1

This CP is associated with the CPS containing information on CA practices, considered confidential by Banque de France, and identified by an OID.

1.3. Definitions and acronyms

1.3.1. Acronyms

The following table lists the acronyms used in this document.

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ARL	Authority Revocation List
CA	Certification Authority
CAPC	Certification Policies Approval Committee (cf. chapter 1.6.1)
CM	Certificate Manager
CN	Common Name
CO	Certification Operator
CP	Certification Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DRA	Delegated Registration Authority
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
ISS	Information System Security
ITU	International Telecommunication Union
LDAP	Light Directory Access Protocol
O	Organization
OCSP	Online Certificate Status Protocol
OI	Organization Identifier
OID	Object Identifier

OU	Organizational Unit
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
PS	Publication Service
PUK	PIN Unlock Key
QSCD	Qualified Signature Creation Device
RA	Registration Authority
RSA	Rivest Shamir Adelman
SAN	Subject Alternative Name
SHA256	Secure Hash Algorithm 256
TSP	Trust Service Provider
UPN	User Principal Name
URL	Uniform Resource Locator

Table 1 – List of acronyms

1.3.2. Definitions

The following table explains some of the terms used in this document.

Term	Definition
Certificate Revocation List (CRL)	List of the numbers of unexpired certificates that have been revoked. The CRL is signed by the Certification Authority to ensure integrity and authenticity.
Certification Agent	Natural person delegated to act as Registration Authority.
Certification Authority (CA)	The core component of the PKI, the Certification Authority is the entity that issues certificates to a community of holders and to other infrastructure components.
Certification Policies Approval Committee (CAPC)	Banque de France entity in charge of validating certification policies. At the time of writing, the CAPC was also the PKI steering committee. Internal Banque de France function.
Certification Policy (CP)	Set of rules that indicates the applicability of a certificate to a particular community or to applications with common security requirements.
Certification Practice Statement (CPS)	Set of practices that must be implemented to comply with the requirements of the CP.
Component	Platform operated by an entity, comprising at least a computer workstation, an application and, as the case may be cryptological capabilities, and playing an identified role in the operational implementation of at least one PKI function.
Entity or Organization	Entity with which a holder is affiliated.
Information Security Officer (RSI)	Owner of the Banque de France's PKI. Internal Banque de France function.
Issuing CA	Issuing CA is a Certification Authority whose certificate is signed by the Root CA. An issuing CA signs the holders' certificates.
Key pair	Set comprising a public key and a private key that form an indissociable pair used by an asymmetric cryptographic algorithm.
Local Security Manager (GLS)	A GLS is appointed in every unit where information security requires local procedures to be implemented and monitored. The GLS assists the head of the unit in all areas pertaining to information security. Internal Banque de France function.
Management portal	Interface used by Operators and Certification Agents for managing certificates during their life cycle
Object Identifier (OID)	Unique identifier used to reference the CP with a recognized third party organization.
Private key	Confidential component of a key pair, known only by the owner and used solely by the owner to decrypt inbound data or to sign data authored by the owner.
Public key	Non-confidential component of a key pair that may be communicated to all members of a community. A public key may be used to encrypt data for the holder of the key pair. It may also be used to verify the holder's signature.
Public key certificate	Certain type of message (e.g. X. 509 v3) that is created and signed by a recognized Certification Authority, which guarantees the authenticity of the public key contained in the message. As a minimum, a certificate contains the holder's identifier and public key. The Certification Authority signs certificates using its own private key.

Public Key Cryptographic Standards (PKCS)	Set of cryptographic standards for public keys.
Public Key Infrastructure	Set of components, functions and procedures dedicated to the management of key pairs and certificates.
Registration Authority (RA)	Cf. paragraph 1.4.2.
Root Certification Authority	Certification Authority whose certificates are self-signed. The Root Certification Authority signs the certificates of Subordinate Certification Authorities.
RSA algorithm	Invented in 1978 by Ronald L. Rivest, Adi Shamir and Leonard M. Adleman, the RSA algorithm may be used to encrypt and/or sign (digital signature) information.
User Portal	Interface used by any standard users (Holders and Certificate Manger) for requesting and managing their certificates in self-service mode

Table 2 – Definitions

1.4. Public Key Infrastructure Participants

This section describes the entities that are involved in the Public Key Infrastructure (PKI) and their obligations.

All PKI entities must:

- document and comply with agreements and contracts that bind Banque de France to other entities,
- implement the necessary technical and human resources so that the entity can meet its service performance commitments while ensuring quality and security.

1.4.1. Certification authorities

The PKI established by Banque de France provides for the issuance of several types of electronic certificates.

These certificates belong to ranges set up according to various criteria, including:

- usage,
- security level.

Banque de France uses a trust model (see below) with a Root Certification Authority (CA), several subordinate CAs and intermediate CAs.

The Root CA certificate is self-signed and does not depend on any other CAs. The Root CA signs the certificates of subordinate and intermediate CAs.

The CAs are represented by the Banque de France Information Security Officer (RSI).

The notion of certification authority as used in this CP is defined in chapter 1.3.2.

The CA is in charge of providing management services for certificates over their entire lifecycle (generation, distribution, renewal, revocation) and relies on the Public Key Infrastructure (PKI) to do this.

CA services are the result of different functions corresponding to the various lifecycle stages of key pairs and certificates.

To clarify and facilitate the identification of requirements, and consistent with documents issued by the European Telecommunications Standards Institute (ETSI) in this area (cf. ETSI EN 319 411-1), the functional decomposition of a PKI as used in this CP is as follows:

- **Registration Authority (RA)** (also called “registration service”) - This function verifies the identification information of the future Intermediate or Subordinate CA for which the certificate is issued, as well as any other specific attributes, before sending the corresponding application to the appropriate PKI function, depending on services provided and the PKI’s organization. The RA is also responsible, where necessary, for rechecking the Intermediate or Subordinate CA information when the certificate is renewed.
- **Certificate generation** - This function generates (format creation, electronic signature with CA private key) the Root CA and Intermediate or Subordinate CA certificates using information sent by the Registration Authority.
- **Secret generation function** - This function generates secret elements for the Root CA and Intermediate or Subordinate CA.
- **Certificate manager delivery** - This function delivers to the Intermediate or Subordinate CA, as a minimum, its certificate as well as, where applicable, the other elements provided by the CA (device, private key, activation codes, etc.).

- **Publication** - This function makes available to the affected parties the general terms and conditions, policies and practices published by the Root CA, the CA's certificates and any other relevant information for Intermediate or Subordinate CA and/or certificate users, excluding certificate status information.
- **Revocation management** - This function processes revocation requests (notably verifying the identity and authentication of the party making the request) and determines the steps that need to be taken. Processing results are distributed through the certificate status information function.
- **Certificate status information** - This function provides certificate users with information about the status of certificates (revoked, suspended, etc.). This function may be implemented through the publication of regularly updated lists (CRL, ARL) or a real-time query/response approach (OCSP).

Within its operational functions, the CA must, as manager of the overall PKI, ensure compliance with the following requirements:

- Be a legal entity as defined by French law.
- Have contractual, administrative or regulatory ties to the entity for which it is in charge of managing certificates. The CA may also, where applicable, have contractual, administrative or regulatory ties to the certification agent(s) selected by the entity.
- Make available all of the services described in its CP to promoters of paperless exchange applications used by the government, holders, certificate users, and those who employ its certificates.
- Ensure that the requirements of the CP and Certification Practice Statement (CPS) procedures are applied by all PKI components and are adequate and in compliance with current standards.
- Implement the various functions identified in the CP, meaning at least the mandatory functions of this CP, particularly in terms of certificate generation, delivery to holders, management of revocations and certificate status information.
- Prepare, implement, supervise and maintain security measures and the operational procedures relating to its facilities, systems and information assets. The CA shall conduct a risk analysis to determine the specific security objectives needed to address the business risks across the entire PKI and the corresponding technical and non-technical security measures that need to be implemented. It shall prepare its CPS based on this analysis.
- Implement the necessary measures to comply with the commitments defined in the CP, particularly in terms of reliability, quality and security. Accordingly, it must possess one or more information quality and security management systems suited to the certification services that it provides.
- Generate, and renew where necessary, its key pairs and the corresponding certificates (signature of certificates, CRLs and OCSP responses), or have its certificates renewed if the CA reports to a senior CA. Distribute CA certificates to Intermediate or Subordinate CA and certificate users.
- Monitor demands placed on capacity and prepare projections concerning future capacity requirements to guarantee service availability, particularly in terms of processing and storage capacity.

1.4.2. Registration authority

The RA has the role of verifying and validating the Intermediate and Subordinate CA information. To do this, it performs the following tasks:

- registers and verifies the information on the future Intermediate or Subordinate CA,
- prepares and sends requests relating to certificates to the appropriate PKI function,
- archives the items contained in the registration file (or sends the information to the component responsible for archival).

In all cases, the RA is responsible for archiving the items comprising the registration file (*in electronic or hardcopy form*) (cf. chapter 5.5).

1.4.3. Intermediate or Subordinate CA

An Intermediate or Subordinate CA certificate can only be issued to Banque de France or one of its subsidiaries.

The Certification Policy and the Certification Practices Statements of Intermediate CA or Subordinate CA must be provided to Root CA so it can validate that the requirements are consistent with those of this CP.

1.4.4. Certificate users

Users are natural persons or devices that rely on CA certificates issued by the Root CA to verify origin and validity of end users certificates delivered for their own needs.

Intermediate and Subordinate CA certificate users are detailed in their respective CP.

1.4.5. Other participants

1.4.5.1. PKI components

The details of the PKI's functions are presented in chapter 1.4.1 above.

1.4.5.2. Certification agents

A certification agent is a duly identified natural person, designated by an applicant and authorized to request an Intermediate or Subordinate CA certificate on behalf of the applicant..

1.4.5.3. Certification operator

Banque de France relies on an external third party for the provision and operation of its PKI. This third party assumes the role of Certification Operator (CO) and has the necessary expertise to take charge of the services enabling the generation and revocation of certificates.

The CO is responsible for the proper functioning of the PKI, the security of technical resources as well as the security of staff and premises.

1.5. Certificate usage

1.5.1. Appropriate certificate usages

1.5.1.1. Intermediate and Subordinate CA key pairs and certificates

The “Banque de France AC v3 Racine” CA issues only Intermediate and Subordinate CA certificates to Banque de France or one of its subsidiaries.

Intermediate and Subordinate CA key pair are used only to :

- sign certificates issued by the CA,
- sign Authority Revocation List (ARL) issued by the CA (*Intermediate CA*),
- sign Certificate Revocation List (CRL) issued by the CA (*Subordinate CA*),
- sign OCSP responder certificates issued by the CA.

1.5.1.2. Root CA and component key pairs and certificates

The key pair of the “Banque de France AC v3 Racine” Certification Authority shall be used only to:

- sign Intermediate and Subordinate CA certificates issued by the CA,
- sign Authority Revocation List (ARL) issued by the CA;
- sign OCSP responder certificates issued by the CA.

1.5.2. Prohibited certificate uses

Banque de France may not be held liable in the event that a certificate is used for a purpose other than those referred to paragraphs 1.5.1.1 et 4.5.

1.6. Certification policy administration

1.6.1. Entity administering certification policies

The Banque de France’s Information Security Officer shall prepare and update the CP of the “Banque de France AC v3 Racine” Certification Authority.

This CP is submitted for the approval of the Certification Policies Approval Committee (CAPC – cf. chapter 1.6.2), notably as regards:

- validating uses and restrictions on the use of certificates issued by this CA;
- ensuring compliance with technological developments, as well as with functional and regulatory requirements.

A table listing the different versions of the CP, the revision dates and the main amendments relative to the previous version is given on page 2 of this document.

1.6.2. CP contact information

Contact details for the person and CAPC in charge of drawing up the CP are as follows.

Information Security Officer (RSI)	RSI Banque de France 39 rue croix des petits champs 75001 Paris email : 1206-crypto-ut@banque-france.fr
Certification Policies Approval Committee, which is chaired by the RSI,	RSI Banque de France 39 rue croix des petits champs 75001 Paris email : 1206-crypto-ut@banque-france.fr

1.6.3. Entity in charge of CPS compliance with the CP

The Banque de France RSI is in charge of ensuring that the CPS complies with this CP.

1.6.4. CPS compliance approval procedures

The Certification Policies Approval Committee (CAPC – cf. chapter 1.6.2) approves CPS compliance with Banque de France CPs.

2. Responsibility for making published information available

2.1. Entities with responsibility for making information available

The Banque de France RSI is responsible for making published information available.

2.2. Published information

The CA publishes the following information for Intermediate or Subordinate CA / certificate managers and certificate users:

Published information	Location
CP of "*Banque de France AC v3 Racine* » CA	• http://pc.igcv3.certificats.banque-france.fr
Trust chain certificates	The certificates of the trust chain are published on the publication site: • http://pc.igcv3.certificats.banque-france.fr The following CA certificates are published: • « *Banque de France AC v3 Racine* » To allow users to verify the origin of certificates, their fingerprints are also published on the publication site: • « *Banque de France AC v3 Racine* » certificate fingerprint: 1f2cb835935ab103922f3a96c0c03fa2764f2a46
ARL of « *Banque de France AC v3 Racine* » CA	• http://crl.igcv3.certificats.banque-france.fr/racine-1.2.250.1.115.200.3.4.1.1.1.crl • http://crl.igcv3.certificats.banque-france.org/racine-1.2.250.1.115.200.3.4.1.1.1.crl • ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20Racine,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint • ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20Racine,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
OCSP Responder of « *Banque de France AC v3 Racine* » CA	• http://ocsp.igcv3.certificats.banque-france.fr/racine-1.2.250.1.115.200.3.5.1.1.1 • http://ocsp.igcv3.certificats.banque-france.org/racine-1.2.250.1.115.200.3.5.1.1.1

Table 3 – List of published information

The integrity of the published data is ensured by the publication of the digital fingerprints of this data.

2.3. Time and frequency of publication

The published documentary information (*CP, General Terms and Conditions, etc.*) is updated as soon as necessary to ensure consistency between the published information and the CA's actual commitments and practices.

Root CA certificates is disseminated prior to any dissemination of certificates and/or corresponding CRL/ARL. The times and frequency of updating ARLs are detailed in chapters 4.9.7 and 4.9.8.

The systems publishing this information are available 24/7.

2.4. Access controls on published information

All information published for the attention of Intermediate or Subordinate CA and users may be accessed freely and without charge. Employees in charge of supplementing, amending and deleting published data have special authorization to carry out the operation and access the publication systems through strong access control (*at least 2-factor authentication*).

3. Identification and authentication

3.1. Naming

3.1.1. Types of names

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

In each certificate, Root CA and Intermediate or Subordinate CA are identified by a Distinguished Name (as defined by standard X.501). CA identification data appear in the Subject field of the certificate, while issuing CA identification data appear in the Issuer field.

3.1.2. Need for names to be meaningful

Selected names must be meaningful.

3.1.2.1. Root CA identity

Root CA is identified by its Distinguished Name (DN), composed as follows:

DN attribute	**Value**
Country (C)	Country of residence of Root CA responsible entity
OrganizationName (O)	Full official name of Root CA responsible entity (*« Banque de France »*)
OrganizationIdentifier (OI)	Official registration number of Root CA responsible entity in accordance with [EN_319_412-1] clause 5.1.4. In France, this registration number can also consist of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country on which the organization depends.
OrganizationalUnitName (OU)	In accordance with Annex 2, section VII.1 of [RGS_v2_A4], this field must be present and contain the identification of the Root CA responsible entity: The ICD is 4 characters long; (0002 for France) Identification of the organization on 35 characters The separator between the two strings is a space. If the ICD number is equal to 0002, it must be followed by a SIREN or SIRET number since it is an establishment registered in France.
CommonName (CN)	Full name of Root CA

3.1.2.2. Intermediate and Subordinate CA identity

Intermediate and Subordinate CA are identified by their Distinguished Name (DN), composed as follows:

DN attribute	**Value**
Country (C)	Country of residence of Intermediate or Subordinate CA responsible entity
OrganizationName (O)	Full official name of Intermediate or Subordinate CA responsible entity (*« Banque de France »*)
OrganizationIdentifier (OI)	Official registration number of Intermediate or Subordinate CA responsible entity in accordance with [EN_319_412-1] clause 5.1.4.

	In France, this registration number can also consist of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country on which the organization depends.
OrganizationalUnitName (OU)	In accordance with Annex 2, section VII.1 of [RGS_v2_A4], this field must be present and contain the identification of the Intermediate or Subordinate CA responsible entity. The ICD is 4 characters long; (0002 for France) Identification of the organization on 35 characters The separator between the two strings is a space. If the ICD number is equal to 0002, it must be followed by a SIREN or SIRET number since it is an establishment registered in France.
CommonName (CN)	Full name of Intermediate or Subordinate CA

3.1.2.3. Certificates for testing

No stipulation.

3.1.3. Anonymization or pseudonymization of CA

Anonymization and the use of pseudonyms in the certificates issued is not authorized by the CA.

3.1.4. Rules for interpreting various name forms

All characters are in UTF-8 String or Printable String format.

3.1.5. Uniqueness of names

The DN Subject field identifies an Intermediate or Subordinate CA uniquely within the “Banque de France AC v3 Racine” CA domain.

3.1.6. Identification, authentication and role of registered trademarks

The CA may not be held liable in the event of unlawful use of registered trademarks, well-known brands and distinctive signs.

3.2. Initial validation of identity

3.2.1. Method to prove possession of a private key

For an Intermediate or Subordinate CA certificate, the key pair is generated under the control of the Certification Operator (CO). The requester proves the possession of the private key by transmitting to the Root CA a request signed with the generated private key.

3.2.2. Validation of organization identity

Intermediate or Subordinate CA certificates are only issued to Banque de France or one of its subsidiaries.

RA verifies however the identity of entity, its legal representative and all persons designated by the latter, directly or indirectly, to represent it to Root CA or RA

If necessary, the registration information is archived by Root CA or RA.

3.2.3. Validation of individual identity

Not applicable.

3.2.4. Non-verified information

No stipulation.

3.2.5. Validation of applicant's authority

Intermediate or Subordinate CA certificates can only be requested by authorized personnel, from Banque de France or one of its subsidiaries, designated by CA responsible to do this.

3.2.6. Interoperability criteria, CA cross-certification

Requests for agreements and recognition agreements with external CAs are studied by the RSI and submitted for approval to the CAPC.

3.3. Identification and validation of re-key requests

The renewal of the key pair of an Intermediate or Subordinate CA automatically leads to the generation and supply of a new certificate.

A new certificate cannot be provided to an Intermediate or Subordinate CA without renewal of the corresponding key pair (see chapter 4.6).

3.3.1. Identification and validation for a routine re-key

The procedure for identifying and validating any renewal request is identical to the initial registration procedure.

3.3.2. Identification and validation for a re-key following revocation

Following the definitive revocation of a certificate, whatever the cause, the procedure for identifying and validating the renewal request is identical to the initial registration procedure.

3.4. Identification and validation of revocation requests

For the reasons specified in chapter 4.9.1, the Intermediate or Subordinate CA certificates can be revoked.

The revocation request can only be submitted by the entity that initially requested the certificate (*via relevant CA responsible*) to the RA of Root CA.

4. Certificate lifecycle operational requirements

4.1. Certificate applications

4.1.1. Who can submit a certificate application

Intermediate or Subordinate CA certificates can only be requested by a Banque de France legal representative or any person authorized and designated by the latter (certificate agent) on behalf to Banque de France or one of its subsidiaries.

4.1.2. Preparing applications: process and responsibilities

An Intermediate or Subordinate CA certificate request is established by a Banque de France legal representative or by a person designated by the latter.

The request is communicated to the Root CA, which is in charge of establishing a key ceremony document describing the generating and issuing conditions of the Intermediate or Subordinate CA certificate.

4.2. Certificate application processing

4.2.1. Performing application identification and validation processes

The RA checks the identity and the authority of the person designated by the legal representative of the CA responsible entity.

4.2.2. Application acceptance or rejection

An Intermediate or Subordinate CA certificate request is accepted or refused.

If the application is rejected, the RA informs the certificate agent giving the reasons for rejection.

When the application is accepted, a key ceremony is organized to generate the Intermediate or Subordinate CA certificate.

4.2.3. Processing time

Intermediate or Subordinate CA certificate is issued during the key ceremony.

4.3. Certificate issuance

When the request is validated by the RA, a key ceremony is organized and planned to generate the Intermediate or Subordinate CA certificate.

4.3.1. CA actions during certificate issuance

For any Intermediate or Subordinate CA certificate request, the Root CA performs the following operations:

- Verification of coherence between the Intermediate or Subordinate CA information to insert in the future certificate and the key ceremony document;
- Activation of the Root CA private key in order to sign the Intermediate or Subordinate CA certificate;
- Signature of the Intermediate or Subordinate CA certificate;
- Verification of the generated certificate content;
- Deactivation of the Root CA private key.

4.3.2. CA notification of certificate issuance

The Intermediate or Subordinate CA certificate is delivered to its representative (legal representation or certificate agent) during the key ceremony. The key ceremony report signature attests to the CA certificate delivery.

4.4. Certificate acceptance

4.4.1. Certificate acceptance procedure

The key ceremony report signature implies acceptance of the certificate.

4.4.2. Certificate publication

The certificates of Intermediate or Subordinate CA of Banque de France and its subsidiaries are published (as defined in paragraph 2.2).

4.4.3. Notification by the technical CA to other entities of certificate issuance

Not applicable.

4.5. Key pair and certificate usage

4.5.1. Intermediate or Subordinate CA private key and certificate usage

The use of the private key and the associated certificate is described in chapter 1.5.1, in a restrictive way. Otherwise, they may be held liable, and the associated certificate could be revoked.

The authorized usage of the private key and the associated certificate is also indicated in the certificate itself, in the extensions concerning the key usage and limited:

- to " keyCertSign" and “cRLsign“ for certificate and revocation list (CRL) signature.

4.5.2. Certificate user public key and certificate usage

Certificate users must not use their certificates other than for the uses detailed in 1.5.1. Users undertake to comply strictly with these usage requirements and may be held liable if they fail to do so.

The authorized use of the certificate is stipulated in the certificate, in the extensions concerning key usage.

4.6. Certificate renewal (within the meaning of RFC 3647)

Certificates are never renewed alone within the meaning of RFC 3647 (*renewal by RFC 3647 means the issuance of a new certificate for which only the validity dates are modified, all other information being identical to the previous certificate, including the public key of the Intermediate or Subordinate CA*). The generation of a new key pair is systematic for any certificate issuance.

4.7. New certificate issuance following a change of key pair

4.7.1. Possible reasons for a change of key pair

The Intermediate or Subordinate CA key pairs and the corresponding certificates are renewed at least every 17 years.

In addition, a key pair and a certificate can be renewed:

- early (e.g. to mitigate cryptographic vulnerabilities),
- or following the revocation of an Intermediate or Subordinate CA certificate (*see chapter 4.9*).

Note - In the remainder of this chapter, the term "issuance of a new certificate" also covers the issuance of a new key pair to the Intermediate or Subordinate CA.

4.7.2. Who can submit an application for a new certificate

The procedure to request a new certificate is identical to the procedure for an initial request (*see chapter 4.1.1*).

4.7.3. Procedure for processing an application for a new certificate

The procedure for processing a request for a new certificate is identical to the procedure for an initial request (*see chapter 4.2*).

The identification and validation of a request for the issuance of a new certificate are governed by the provisions of chapter 3.3.

4.7.4. Notification of new certificate issuance

Cf. chapter 4.3.2.

4.7.5. New certificate acceptance procedure

Cf. chapter 4.4.1.

4.7.6. New certificate publication

Cf. chapter 4.4.2.

4.7.7. Notification of certificate issuance by the CA to other entities

Cf. chapter 4.4.3.

4.8. Certificate modification

Modification of a certificate means modifications of information without changing the public key (*cf. chapter 4.7*) and other than only modification of validity dates (*cf. chapter 4.6*), as defined in RFC 3647.

Certificate modification is not allowed. Any request for modification results in a request for a new certificate, detailed in chapter 4.2.

4.9. Certificate revocation and suspension

4.9.1. Circumstances in which a certificate may be revoked

Where one of the circumstances described below occurs and where the CA becomes aware of this (*i.e. it is informed of the events or obtains the information during one of its checks, and notably when issuing a new certificate*), the certificate in question is revoked and its serial number is put in the ARL until the certificate has not reached its expiry date.

Any revocation request may be accompanied by a reason for revocation as described in chapter 4.9.1.1 (*where appropriate, the reason will not be published, cf. chapter 4.9.3.1*).

4.9.1.1. Intermediate or Subordinate CA certificates

An Intermediate or Subordinate CA certificate may be revoked in the following circumstances:

- the information appearing in the certificate is not or is no longer consistent with the identity information or the usage provided for in the certificate,
- the Intermediate or Subordinate CA fails to comply with the procedures for using the certificate,
- the Intermediate or Subordinate CA has failed to meet their obligations under the CP governing the certificate,
- an error, whether intentional or not, is found in the Intermediate or Subordinate CA registration file,
- the private key associated with the Intermediate or Subordinate CA certificate is suspected of being compromised, or is compromised, lost or stolen (*potentially the associated activation data*),
- the legal representative (or certificate agent) of the Intermediate or Subordinate CA asks for the certificate to be revoked,
- the Intermediate or Subordinate CA entity terminates operations.

As soon as one of the circumstances described above occurs and where the Root CA becomes aware of this, the Intermediate or Subordinate CA certificate in question is revoked

4.9.1.2. PKI component certificates

The certificate of a PKI component (*including a CA certificate used to generate certificates, CRLs/ARLs, OCSP certificates*) may be revoked in the following circumstances:

- the component's private key is suspected of being compromised, or is compromised, lost or stolen,
- it is decided to change the PKI component after procedures applied in the component are found to be non-compliant with the procedures set out in the CPS (e.g. after negative results in a certification or compliance audit),
- the entity operating the component terminates operations,
- the component migrates to a different technical solution that is incompatible with the first solution.

4.9.2. Who can request revocation

4.9.2.1. Intermediate or Subordinate CA certificates

The following persons/entities are authorized to request revocation of a certificate:

- a legal representative or certificate agent of the Intermediate or Subordinate CA responsible entity,
- Root CA,
- RA attached to Root CA.

4.9.2.2. PKI component certificates

The decision to revoke a CA certificate may be taken only by the entity in charge of the CA (the RSI) or the courts.

Revocation of the other components' certificates shall be decided by the entity operating the component in question. The entity is required to promptly inform the CA of such revocation.

4.9.3. Procedure for processing revocation requests

4.9.3.1. Intermediate or Subordinate CA certificates

On receiving a request for revocation, the RA verifies the identity of the person making the request and the validity of the request, as detailed in3.4.

The revocation request must contain at least the following information:

- identity of the Intermediate or Subordinate CA used in the certificate,
- the name of the entity responsible for the Intermediate or Subordinate CA,
- revocation requester name (legal representative or certificate agent),
- information that may be used to quickly and correctly identify the certificate to be revoked (*the serial number, failing alternatives*).

If the request is admissible, the Root CA organize a key ceremony to :

- Activate the Root CA private key,
- Sign a new ARL including the Intermediate or Subordinate CA certificate serial number,
- Destroy the Intermediate or Subordinate CA private key corresponding to the revoked certificate,
- Deactivate the Root CA private key.

If the request is not admissible, the RA informs the requester.

The revocation is logged by the “Banque de France AC v3 Racine” CA. Revocation requests are recorded and archived.

The reasons for definitive certificate revocation are not published.

4.9.3.2. PKI component certificates

In the event that the “Banque de France AC v3 Racine” CA certificate belonging to a certificate’s chain of trust is revoked, the following steps must be taken:

- all affected Intermediate or Subordinate CA must be promptly informed that their certificates are no longer valid because one of the certificates in the certification chain is no longer valid,
- all organizations referencing one of the ranges issued by the CA should be notified,
- the ANSSI contact should be informed.

4.9.4. Time given to the Intermediate or Subordinate CA to prepare a revocation request

The legal representative, or certificate agent, of entity responsible for Intermediate or Subordinate CA must prepare a revocation request promptly on learning that one of the circumstances for revocation has arisen.

4.9.5. Time within which the CA should process revocation requests

4.9.5.1. Intermediate or Subordinate CA certificates

As soon as an Intermediate or Subordinate CA request for revocation is authenticated and validated, the Root CA makes every effort to organize a key ceremony as soon as possible

4.9.5.2. PKI component certificates

The certificate of a PKI component shall be revoked on detection of an event constituting a possible revocation circumstance for this type of certificate. Certificate revocation is effective when the certificate’s serial number is added to the revocation list of the CA that issued the certificate, and when this list is available to be downloaded.

The CA’s signing certificate (for certificates, CRLs/ARLs, OCSP certificates) is revoked immediately, particularly if the key is compromised.

4.9.6. Revocation checking requirements for certificate users

Banque de France makes an OCSP responder, CRLs and ARLs available to certificate users (*cf. chapter 2.2*).

Before using a certificate, every user is responsible for checking the status of certificates across the entire certification chain. The user is free to choose the method used (CRL, OCSP).

4.9.7. CRL generation frequency

ARLs are generated at least once every 24 hours.

4.9.8. Maximum latency for CRLs

The ARL is published within a maximum of 30 minutes following its generation.

4.9.9. Availability of online system to check certificate revocations and status

Banque de France provides users with an online system to check certificate status (OCSP). The system's characteristics in terms of integrity, availability and publication times are the same as for the CRL publication service (cf. chapter 4.9.5.1).

If the OCSP service is unavailable, users can view the status of certificates from the ARL distribution points.

4.9.10. Online certification revocation checking requirements for certificate users

Cf. chapter 4.9.6.

4.9.11. Other arrangements for providing revocation information

No stipulation.

4.9.12. Special requirements in the event of private key compromise

The following steps should be taken if a private key has been compromised:

Intermediate or Subordinate CA certificates

Entities (*cf. 4.9.2*) that are authorized to request revocation are required to do so promptly after learning that the private key has been compromised.

CA certificates

In the event that a certificate is revoked because the private key has been compromised, in addition to the steps detailed in 4.9.3.2, a clear message will be published online at http://pc.igcv3.certificats.banque-france.fr. This message may also be published, in conjunction with the Banque de France Communications Directorate, by other means, including in a press release or in a posting on the Banque de France's main website.

Information will be sent to the identified ANSSI contact point.

4.9.13. Circumstances for suspension

No stipulation. There is no provision for suspending the certificates by Banque de France CAs.

4.9.14. Who can request suspension

No stipulation. There is no provision for suspending the certificates by Banque de France CAs.

4.9.15. Procedure for processing a suspension request

No stipulation. There is no provision for suspending the certificates by Banque de France CAs.

4.9.16. Limits on certificate suspension period

No stipulation. There is no provision for suspending the certificates by Banque de France CAs.

4.10. Certificate status information function

4.10.1. Operational characteristics

The certificate status information function is designed to enable users to check the status of a certificate and its certification chain, i.e. to also check the signatures of the certificates in the chain and the signatures guaranteeing the origin and integrity of CRLs/ARLs.

The certificate status information function provides users with a mechanism that allows them to freely consult CRLs and ARLs. CRLs and ARLs are in CRLv2 format and are electronically published at the URLs given in 2.2. These addresses are also given in the "CRL Distribution Point" field of each certificate.

4.10.2. Function availability

The following table details availability commitments for the certificate status information function.

Service availability	24/7

Maximum downtime per service stoppage	4h
Total maximum downtime per month	8h
Maximum time taken to respond to a OCSP query	6s

Table4 – Availability of certificate status information function

4.10.3. Optional features

No stipulation.

4.11. End of relations between the Intermediate or Subordinate CA and the Root CA

If relations between the Intermediate or Subordinate CA and the Root CA are terminated before the end of the certificate validity period, the Root CA will revoke the Intermediate or Subordinate CA certificate.

4.12. Key escrow and recovery

No stipulation. Escrow is not authorized by Root CA.

4.12.1. Key escrow recovery practices and policies

No stipulation.

4.12.2. Session key encapsulation recovery policies and practices

No stipulation.

5. Non-technical security measures

The measures and controls described in this chapter are designed to ensure a high level of trust in the operation of the PKI.

5.1. Physical security measures

Physical security measures are dictated by the need to comply with rules and standards documented by Banque de France IT services departments (Banque de France's local internal security policies).

Local security policies are cited in the CPS.

In addition, for the services that the CO operates, the latter has conducted a risk analysis which has made it possible to identify the security measures described in this chapter.

5.1.1. Site location and construction

Site construction complies with current standards and regulations.

5.1.2. Physical access

Access to the premises of PKI components is controlled to prevent loss, damage or compromise of PKI resources and interruption to CA services. Any person entering these physically secured areas must be accompanied by an authorized person.

Access to functions involved in generating certificates and Intermediate or Subordinate CA secret elements and managing revocations is strictly limited to persons who are personally authorized to enter the premises, and measures will be taken to ensure that entries are traceable. Outside business hours, security is enhanced by systems to detect physical or logical intrusion. To ensure system availability, machines may only be accessed by the persons authorized to conduct work requiring physical access to the machines. For this, the relevant PKI components set up a physical security perimeter within which the machines are housed. Setting up this perimeter makes it possible to comply with the separation of trusted roles as provided for in this CP. In particular, any premises shared with functions other than those provided by the component in question shall be outside this security perimeter.

NB – Machines mean all servers, HSMs, workstations and active elements in the system used to provide the functions.

5.1.3. Power and air conditioning

The characteristics of the power and air conditioning systems comply with the usage requirements of PKI hardware and the availability commitments of CA functions, in particular the functions relating to revocation management and certificate status information.

5.1.4. Water exposures

The resources in place to protect against water damage meet the requirements of the CP and the availability commitments of CA functions, in particular the functions relating to revocation management and certificate status information.

5.1.5. Fire prevention and protection

The resources in place to prevent and protect against fire meet the requirements of the CP and the availability commitments of CA functions, in particular the functions relating to revocation management and certificate status information.

5.1.6. Media storage

The data used in the PKI's activities are identified and their security needs are defined (confidentiality, integrity and availability). The CA keeps an inventory of all these data and establishes measures to prevent them from being compromised or stolen. Media (paper, hard drives, floppy disks, CDs, etc.) holding these data are managed according to procedures that comply with these security needs. In particular, the media are handled in a secure manner to protect them against damage, theft and unauthorized access. Management procedures protect these media against obsolescence and deterioration for the period during which the CA undertakes to keep the data that they contain.

5.1.7. Waste disposal

At the end of their life, media are either destroyed or reinitialized for reuse, depending on the level of confidentiality of the information contained. Media destruction and reinitialization procedures and resources comply with this confidentiality level.

5.1.8. Off-site backup

In addition to conducting on-site backups, PKI components make off-site backups of their applications and data. These backups are organized to ensure that the PKI can resume its functions after an incident as swiftly as possible and in accordance with the requirements and commitments of this CP. Off-site backups comply with the requirements of this CP in terms of protecting data confidentiality and integrity.

PKI components in charge of revocation management and certificate status information functions conduct off-site backups to enable these functions to resume swiftly following an incident or event with a serious and lasting effect on the provision of these services, such as premises destruction. Backup and restore functions are conducted by appropriate trusted roles and in accordance with procedural security measures.

5.2. Procedural security measures

These measures are designed to ensure that tasks associated with core PKI functions are shared among several people.

Procedural controls are established for each of the entities making up the PKI. These controls are detailed in the CPS and cover the following points:

- trusted roles,
- number of individuals required per task,
- identification and authentication requirements for each role,
- roles requiring separation of duties

5.2.1. Trust roles

The CA distinguishes at least the following five functional trust roles:

- **Security manager:** The security manager is responsible for implementing the component's security policy. It manages the physical access controls to the equipment of the component systems. He is authorized to examine the archives and is responsible for analyzing event logs in order to detect any incident, anomaly, attempt to compromise, etc. He is responsible for certificate generation and revocation operations.
- **Application manager:** The application manager is responsible, within the component to which he is attached, for the implementation of the CP and the CPS of the PKI. at the application level for which he is responsible. Its responsibility covers all the functions rendered by this application and the corresponding performances.
- **System engineer:** He is responsible for the start-up, configuration and technical maintenance of the component's IT equipment. It provides technical administration of the component's systems and networks.
- **Operator:** An operator within a component of the PKI realizes, within the framework of its attributions, the exploitation of the applications for the functions implemented by the component.
- **Controller:** Person designated by a competent authority and whose role is to regularly carry out compliance checks on the implementation of the functions provided by the component in relation to CP, CPS of the PKI and component security policies.

In addition to these trusted roles, the CA has defined the role of **Secret Shareholder**. The secret Shareholder is responsible for ensuring the confidentiality, integrity and availability of the share entrusted to him.

5.2.2. Number of people required per operation

Depending on the type of operation / task to be performed, the presence of one or more people with specific roles is necessary.

The number and quality of people required per task are specified in the CPS.

5.2.3. Identification and authentication for each role

Each entity operating a component of the PKI has verified the identity and authorizations of any member of its staff required to work within the component before assigning him a role and the corresponding rights, in particular:

- that his name is added to the access control lists of the premises of the entity hosting the component concerned by the role,
- that his name is added to the list of persons authorized to physically access these systems,

- if applicable and depending on the role, that an account is created with his name in these systems,
- possibly, that cryptographic keys and / or certificate be issued to him to fulfill the role assigned to him in the PKI.

These checks comply with the component's security policy.

5.2.4. Roles requiring separation of responsibilities

Several roles can be assigned to the same person, as long as the combination does not compromise the security of the functions implemented. For trusted roles, it is nevertheless recommended that the same person does not hold several roles and, as a minimum, the following requirements for non-cumulation are respected. The attributions associated with each role comply with the security policy of the component concerned.

Regarding trust roles, the following cumulations are prohibited:

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

5.3. Personnel security measures

Personnel controls are established for each of the entities making up the PKI. These controls are detailed in the CPS and cover the following points:

- qualifications, experience and authorization requirements,
- background check procedures,
- initial training requirements,
- ongoing training requirements and frequency,
- frequency and sequence of rotations between different roles,
- disciplinary measures in the case of unauthorized acts,
- requirements with respect to the personnel of external service providers,
- documentation provided to personnel.

Furthermore, any individual taking part in a task relating to the Certification Authority or Registration Authority must not be subject to a conflict of interest regarding the Certification Authority.

Any conflicts of interest involving Banque de France employees will be addressed according to internal rules.

Any conflicts of interest involving non-Banque de France personnel with a trusted role in the PKI shall be addressed by the business area correspondent according to best practices for that area.

5.3.1. Qualifications, skills and qualifications required

Anyone working within the PKI is subject to a confidentiality commitment with their employer. It is also verified that the responsibilities of these people correspond to their professional skills.

Anyone working within the CA is aware of their responsibilities for PKI services and procedures related to system security and personnel control.

5.3.2. Background check procedures

The CA and each PKI's component implements the legal means to ensure the honesty of the personnel brought to work within the PKI or one of its components.

This background check is performed before assigning a trust role to staff.

Among these checks, the supply of a copy of "*bulletin no. 3*" of the personnel criminal record must be provided to the employer before the assignment of the roll.

People with a role of trust do not suffer from any conflict of interest which would be prejudicial to the impartiality of their duties.

5.3.3. Initial training requirements

Personnel working within the PKI are previously trained to software, hardware and internal operating and security procedures corresponding to the component in which they operate.

5.3.4. Continuing training requirements and frequency

Depending on the nature of the changes (*related to systems, procedures, organization, etc.*), the personnel concerned receive appropriate training before any change.

5.3.5. Frequency and sequence of rotation between different assignments

No stipulation.

5.3.6. Sanctions for unauthorized actions

Sanctions for actions not authorized by the CP/CPS and established procedures as well as internal PKI processes and procedures, whether negligent or malicious, are provided.

5.3.7. Requirements for staff of external service providers

The personnel of external service providers working on the components of the PKI comply with the requirements of the CA. These requirements are translated into suitable clauses in contracts with these providers.

5.3.8. Documentation provided to staff

The personnel have at least adequate documentation concerning the operational procedures and the specific tools that they implement as well as the policies (*in particular the CP*) and general practices (*in particular the CPS and the operational procedures*) of the component within which he works.

5.4. Audit logging procedures

Audit logs are created to ensure that operations can be traced and assigned. They are authenticity- and integrity-protected and are subject to strict operating rules, which are detailed in the CPS and cover the following points:

- type of events to be recorded,
- frequency of audit log processing,
- audit log retention period,
- audit log protection,
- audit log backup procedure,
- audit log collection system,
- providing notification that an event has been logged to the event-causing person,
- vulnerability assessment.

5.4.1. Type of events to record

Each entity operating a component of the PKI logs, as a minimum, the events as described below in electronic form. Logging is automatic from the start of the system and without interruption until it stops.

- creation / modification / deletion of user accounts (access rights) and the corresponding authentication data (passwords, certificates, etc.),
- start and stop of computer systems and applications,
- activity traces (logs) from firewalls and routers,
- events related to logging: start and stop of the logging function, modification of logging parameters, actions taken following the failure of the logging function, software and hardware failures,
- login / logout of Users with trusted roles, and corresponding unsuccessful attempts.

5.4.1.1. Information recorded for each event

Each record of an event in a log contains the following fields:

- type of event,
- name of the operator or reference of the system triggering the event,
- date and time of the event,
- result of the event (failure or success).

5.4.1.2. Events recorded by the RA

The events recorded by the RA are as follows:

- receipt of a certificate request (initial and renewal),
- validation / rejection of a certificate request,
- receipt of a revocation request,
- validation / rejection of a revocation request,
- transmission of the certificate to the Intermediate and Subordinate CA responsible entity,
- acknowledgment of receipt of the Intermediate and Subordinate CA responsible entity,

- explicit acceptance or rejection by the Intermediate and Subordinate CA responsible entity.

5.4.1.3. Events recorded by the CA

The events recorded by the CA are as follows:

- events related to signature keys and CA certificates (generation, backup / recovery, destruction, ...),
- generation of key pairs for Intermediate and Subordinate CA,
- generation of certificates for Intermediate and Subordinate CA,
- customization of supports and generation of activation codes,
- publication and update of information related to CAs (CP / CPS, CA certificates, PDS, ...)
- generation and publication of ARLs,
- OCSP requests and responses.

5.4.1.4. Various events

Other events are also collected. These are security-related events that are not produced automatically by the systems implemented:

- physical access,
- actions to maintain and change the configuration of the systems,
- changes made to personnel with trusted roles,
- actions to destroy and reset media containing confidential information (*keys, activation data, passwords, etc.*).

5.4.1.5. Accountability

Accountability for an action rests with the person, body or system that performed it. The name or identifier of the performer is explicitly listed in one of the fields in the event log.

Depending on the type of event concerned, the following fields can be recorded:

- recipient of the operation,
- name or identifier of the requester of the operation or reference of the system making the request,
- name of the people present (*if this is an operation requiring several people*),
- cause of the event,
- any information characterizing the event (*for example for the generation of a certificate, its serial number*).

Logging operations are performed during the relevant process. In the case of manual entry, the entry is made, barring exceptions, on the same working day as the event.

5.4.2. Frequency of event log processing

The event logs are checked and analyzed according to the frequency defined in chapter 5.4.8.

5.4.3. Retention period for event logs

Event logs are kept on site for at least 1 month. They are archived as quickly as possible after their generation and at the latest within 1 month.

5.4.4. Protection of event logs

Logging is designed and implemented to limit the risk of bypassing, modifying or destroying event logs. Integrity control mechanisms make it possible to detect any modification, voluntary or accidental, of these logs.

Event logs are protected on availability (*against loss or partial or total destruction, voluntary or not*).

The systems generating the event logs are synchronized with a reliable time source detailed in chapter 6.8.

5.4.5. Backup procedure of event logs

The procedures for saving logs are detailed in the CPS.

Event logs are protected on availability (*against loss or partial or total destruction, voluntary or not*).

The systems generating the event logs are synchronized with a reliable time source detailed in chapter 6.8.

5.4.6. Event log collection system

The collection system guarantees the level of security relating to the integrity, availability and confidentiality of event logs.

5.4.7. Notification of the recording of an event to the event responsible

No stipulation.

5.4.8. Vulnerability assessment

Each entity operating a component of the PKI is able to detect any attempt to violate the integrity of the component under consideration.

The event logs are checked at least once a day in order to identify anomalies linked to failed attempts.

The logs are analyzed in their entirety once a week and as soon as an anomaly is detected. This analysis gives rise to a summary in which the important elements are identified, analyzed and explained. The summary reveals the anomalies and falsifications noted.

A reconciliation between the various event logs of the RA and the CA is carried out at least once a month, this in order to check the concordance between dependent events and thus help to reveal any anomaly.

5.5. Data archival

The RA and the CA archive data in an effort to ensure service continuity, auditability and non-repudiation of transactions, the permanence of audit logs created by PKI components, the retention of hardcopy documents linked to certification operations and the ability to produce these documents when needed.

The RA and the CA take the necessary measures to ensure that these archives are available, reusable, integrity-protected, and subject to strict operational and destruction-protection rules.

5.5.1. Types of data to archive

The following, in particular, are archived:

- CPs and CPSs throughout the lifespan of the Root CA,
- CRLs / ARLs,
- certificates,
- software (*executable files*) and configuration files for computer hardware,
- contractual agreements with other CAs,
- receipts or notifications (*for information purposes*),
- identity documentation for legal representative or certificate agent and, where applicable, for the entity with which they are affiliated,
- audit logs of PKI entities.

Data archived in electronic form is duplicated and stored on two separate sites.

5.5.2. Archival retention period

For certificate request files:

- the files and supporting documents are archived for a period of twenty years from the date of acceptance of the certificate.
- At the end of archiving period, the file and supporting documents are destroyed.

For certificates and CRLs issued by the CA:

- the certificates and CRLs issued by the CA are kept for twenty years at least from their generation.
- At the end of archiving period, the CRL issued by the CA are destroyed.

For OCSP responses:

- OCSP responses are kept for three months at least from their expiration date.
- At the end of archiving period, the OCSP responses are destroyed.

For event logs:

- event logs are kept for twenty years at least from their generation date.
- At the end of archiving period, the event logs are destroyed.

5.5.3. Protection of archives

Throughout their preservation, the archives:

- are protected in integrity,
- are accessible only to authorized persons,
- can be read or used,
- readable and usable over their entire life cycle.

5.5.4. Archive backup procedure

No stipulation.

5.5.5. Data timestamping requirements

Chapter 6.8 specifies the date and time stamping requirements.

5.5.6. Archives collection system

No stipulation.

5.5.7. Archive recovery and verification procedures

The archives in paper or electronic format must be able to be recovered by the CA within 2 working days.

5.6. CA key changeover

The CA cannot generate a certificate whose end of validity date comes after the expiry date of the corresponding CA certificate. The validity period of certificates signed by the CA must therefore end before the CA certificate expires.

The CPS details the applicable procedures in the event of a CA key changeover.

In the event that a new key pair is generated, only the new private key is used to sign certificates. The previous CA certificate may still be used to validate previously issued certificates, at least until the expiry of all the certificates signed with the corresponding private key.

5.7. Compromise and disaster recovery

Recovery procedures for PKI components in the event of an incident or compromise are detailed in the CPS.

5.7.1. Procedures for reporting and handling incidents and compromises

Each entity acting on behalf of the PKI implements incident reporting and incident handling procedures. This is achieved through awareness and training of staff and through analysis of event logs.

In the event of a major incident, such as loss, suspected compromise, compromise, theft of the CA's private key, the triggering event is the observation of this incident at the level of the component concerned, who immediately informs the CA. The case of major incidents is imperative processed upon receipt and publication of the certificate revocation information, if any, is done with the utmost urgency, even immediately, by any useful or available means.

If one of the algorithms, or associated parameters, used by the CA or its systems becomes insufficient for its remaining intended use, then the CA informs all Intermediate or Subordinate CA and third-party users of certificates with which the CA has made agreements. In addition, all the certificates concerned are revoked.

In accordance with regulatory obligations, the national control body (ANSSI) will be informed of any security incident affecting the CA and its services within 24 (twenty-four) hours.

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

Each component of the PKI has a business continuity and service plan which makes it possible to meet the availability requirements of the various functions of the PKI arising from this CP / CPS, from the commitments of the CA.

5.7.3. Recovery procedures in case of compromise of the private key of a component

Each component of the PKI has a continuity plan.

In the event of compromise of a CA key, the corresponding certificate is immediately revoked as specified in chapter 4.9. In addition, the CA respects the following commitments:

- immediately stop using the compromised component key,
- inform without delay: all Intermediate or Subordinate CA and third-party users,

- promptly state that certificates and revocation status information issued using this CA key may no longer be valid.
- notify the ANSSI of the compromise within 24 hours,
- if necessary, file a complaint with the competent authorities.

5.7.4. Business continuity capacities following a disaster

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

5.8. PKI termination

One or more PKI components may terminate operations or transfer operations to another entity, for a variety of reasons.

The CA shall make the necessary arrangements to cover the costs required to comply with these minimum requirements in the event that the CA itself is unable to cover the costs, as far as possible in accordance with the applicable legislative requirements.

Transfer of activities shall be defined as the end of operations of a PKI component with no impact on the validity of certificates issued prior to the transfer and the resumption of operations organized by the CA in conjunction with the new entity.

Termination of operations shall be defined as the end of operations of a PKI component with an impact on the validity of certificates issued prior to termination.

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

To ensure a constant level of trust during and after such events, the CA:

- has procedures aimed at ensuring service continuity, particularly in terms of archiving (*especially archiving Intermediate or Subordinate CA certificates and certificate-related information*);
- ensures continuity of the revocation function (*registering revocation requests and publishing CRLs*), in accordance with the service availability requirements detailed in this CP.

The CA notifies all PKI entities in a special memo three months before the effective date of termination or transfer of responsibilities.

The CA shall notify all Intermediate and Subordinate CA using the method of its choosing, giving them notice of three months.

The CA sends to the ANSSI contact:

- the principles of the action plan comprising technical and organizational resources used to effect a termination of operations or organize a transfer of operations, particularly archival arrangements (for keys and certificate-related information), in order to deliver the function or to ensure that the function is delivered throughout the period initially provided for in the CP;
- changeover procedures, an inventory and an assessment of the event's legal, economic, functional, technical, communications-related and other consequences;
- an action plan to eliminate or mitigate risk for the applications as well as inconvenience for Intermediate or Subordinate CA and certificate users;
- where applicable, any obstacles or additional delays encountered during the process.

Once the three-month notice period is over, if the CA has terminated operations, all the certificates issued by that CA will be revoked.

The CPS details all CA archival procedures.

5.8.2. Termination of operations affecting the CA

Operations may be totally or partly terminated. Partial termination must be conducted gradually so that only the obligations listed below are to be performed by the CA, or a third party entity that is taking over the operations, when the last certificate issued by the CA expires.

In the event of a complete termination, the CA must ensure that the certificates are revoked and that CRLs are published in accordance with the commitments made under the CP. If the CA cannot perform the task, the steps

must be performed by another entity assigned to replace the CA by a law, regulation, court ruling or agreement reached beforehand with the entity in question.

The CA shall stipulate in its practices the measures taken in the event of a termination of operations, which include:

- notifying affected entities;
- transferring obligations to other parties;
- managing the revocation status of outstanding unexpired certificates.

In the event of a service stoppage, a procedure is in place to:

- prohibit delivery of the private key used to issue certificates;
- destroy the key or take necessary steps to render it inoperative;
- revoke the CA's certificate;
- revoke all the certificates signed by the CA that are still valid;
- inform all Intermediate and Subordinate CA whose certificate has been or will be revoked.

6. Technical security measures

6.1. Generation and installation of key pairs

6.1.1. Generation of key pairs

6.1.1.1. CA keys

CA key pairs are generated on hardware security modules (HSMs) using a formal key ceremony procedure.

PKI initialization and/or generation of CA signing keys is accompanied by the generation of PKI secrets.

Secret parts are generated according to a Shamir's secret sharing scheme (n parts among m are necessary and sufficient to reconstruct the secret). They allow to securely restore, in a new cryptographic module, the Root CA private key previously saved during a key ceremony.

Following their generation, the secret parts (shares) are given to shareholders previously designated and appointed to this trusted role by Root CA. Each share of secrets is then used only by its shareholder.

Key ceremonies are conducted under the supervision of at least two people with trusted roles and in the presence of several witnesses, at least two of whom are impartial observers who are external to the CA. The witnesses make an objective and factual record certifying that the ceremony has taken place according to the predefined script. As far as possible, one of the witnesses should be a public officer such as a bailiff or notary. The environment used guarantees the confidentiality and integrity of the CA's private keys.

6.1.1.2. Intermediate and Subordinate CA generated by Root CA

Intermediate and Subordinate CA keys are generated on hardware security modules (HSMs), according to a formal procedure called "Key Ceremony".

6.1.1.3. Intermediate and Subordinate CA generated on Intermediate and Subordinate CA server

Intermediate and Subordinate CA keys are generated directly in a secured device meeting the requirements of chapter 11 when the key pair is generated on Intermediate and Subordinate CA infrastructure.

6.1.2. Private key delivery to owners

When the key pair is generated on Intermediate and Subordinate CA infrastructure, the private key is securely transmitted to the responsible entity according to operations described in the key ceremony.

6.1.3. Public key delivery to CA

Intermediate and Subordinate CA public keys are delivered to the CA for signing purposes in a manner that guarantees their integrity and origin.

6.1.4. CA public key delivery to certificate users

The Root CA public key is delivered to users via CA certificates, which provide a guarantee of integrity and origin.

The Root CA's digital fingerprint also appears:

- in its certificate and in any other CA certificate signed by the Root CA (see chapter 1.1),
- at the following url: http://pc.igcv3.certificats.banque-france.fr,
- and may also be checked with the contact named in chapter 1.6.2.

6.1.5. Key size

The Root CA uses a 4096 bit RSA key.

Intermediate and Subordinate CAs use a 4096 bit RSA key.

These requirements will be revised to reflect changes in technology and/or legislation.

6.1.6. Key pair parameter generation and quality checking

The equipment employed to generate key pairs uses parameters that meet RSA algorithm security standards. Details are provided in the CPS.

The Intermediate and Subordinate CA key pair is generated using parameters that meet RSA algorithm security standards. The parameters and the signature algorithms are documented in chapter 7.

The Intermediate and Subordinate CA key pair is generated and protected by a secured device meeting the requirements of chapter 11 .

The Root CA key pair is generated and protected by a hardware cryptographic module meeting the requirements of Chapter 11.

6.1.7. Key usage purposes

The use of a Root CA private key and associated certificate is strictly restricted to signing certificates and ARLs.

The use of Intermediate and Subordinate CA private key and associated certificate is strictly restricted to signing certificates and ARLs / CRLs.

6.2. Private key protection and cryptographic module security measures

6.2.1. Cryptographic module security standards and measures

6.2.1.1. Root CA cryptographic modules

For the generation and implementation of its signature keys, the "Banque de France AC v3 Racine" CA uses a cryptographic module that meets the EAL4 + level of the common criteria and at the reinforced level, thus meeting the requirements of Chapter 11.

6.2.1.2. Intermediate and Subordinate CA cryptographic modules

When generated by Root CA, Intermediate and Subordinate CA key is generated and used in a cryptographic module that meets the EAL4 + level of the common criteria and at the reinforced level, thus meeting the requirements of Chapter 11.

When generated in Intermediate or Subordinate CA infrastructure, Root CA ensure that the cryptographic module meets the EAL4 + level of the common criteria through a clear and explicit contractual commitment from the entity responsible for the Intermediate or Subordinate CA.

6.2.2. Private key multi-person control

CA private keys are controlled through a secret-sharing scheme (*at least three out of five secret shareholders must participate*).

Trusted personnel are assigned the role of secret shareholders. Secret shareholders are responsible for the secrets entrusted to them. They must keep them in such a way as to guarantee their confidentiality, availability, integrity and traceability. Details are provided in the CPS.

6.2.3. Private key escrow

Root CA private keys are not escrowed.

Intermediate and Subordinate CA private keys are not escrowed.

6.2.4. Private key backup

The Root CA private key is backed up with the same level of security as the key initially generated inside the cryptographic module.

The copy operations comply with the requirements of Chapter 11, thus ensuring cryptographic operations inside the cryptographic module.

The Intermediary and Subordinate CA private keys can be backed up by their own responsible entity. If necessary, the backed up keys must be recorded in encrypted form, with a mechanism ensuring their integrity.

6.2.5. Private key archival

CA private keys are not archived.

Intermediate and Subordinate CA private keys are not archived.

6.2.6. Private key transfer into/from a cryptographic module

Intermediary and Subordinate CA private key is generated in a cryptographic module and any transfer is done in encrypted form.

The transfer of the Root CA private key to and from the cryptographic module is subject to a device implementing the sharing of secrets. The used means of transfer ensure the confidentiality and integrity of the private key.

6.2.7. Private key storage in a cryptographic module

The Root CA private key is stored in a hardware cryptographic module meeting the requirements of Chapter 11 (see paragraph 6.2.1.1).

The Intermediate or Subordinate CA private key is stored in a hardware cryptographic module meeting the requirements of Chapter 11 (see paragraph 6.2.1.2).

6.2.8. Method of activating private key

6.2.8.1. Root CA private key

Activation of Root CA private keys in cryptographic modules is controlled via activation data. At least, two of the five secret shareholders (*persons in trusted functional roles, cf. chapter 5.2*) are required to participate, in accordance with the requirements of Chapter 11.

6.2.8.2. Intermediate and Subordinate CA keys

Activation of Intermediate and Subordinate CA private keys in cryptographic modules is controlled via activation data. At least, two of the five secret shareholders (*persons in trusted functional roles, cf. chapter 5.2*) are required to participate, in accordance with the requirements of Chapter 11.

6.2.9. Method of deactivating private key

6.2.9.1. Root CA private key

Root CA private keys in a cryptographic module are automatically deactivated if the module environment changes, e.g. the module is stopped or disconnected or the operator is disconnected.

The deactivation conditions meet the requirements of Chapter 11.

6.2.9.2. Intermediate and Subordinate CA keys

Intermediate and Subordinate private keys in a cryptographic module are automatically deactivated if the module environment changes, e.g. the module is stopped or disconnected or the operator is disconnected.

The deactivation conditions meet the requirements of Chapter 11.

6.2.10. Method of destroying private key

6.2.10.1. Root CA private key

At the normal or early (e.g. owing to revocation) end of Root CA private key lifespan, keys must be destroyed, as must any copy or element that could be used to recreate the key.

6.2.10.2. Intermediate and Subordinate CA keys

At the normal or early (e.g. owing to revocation) end of Intermediate and Subordinate CA private key lifespan, keys must be destroyed, as must any copy or element that could be used to recreate the key.

6.2.11. Cryptographic module security assessment rating

Root CA cryptographic module security assessment rating is detailed in. paragraph 6.2.1.1.

Intermediate and Subordinate CA cryptographic module security assessment rating is detailed in. paragraph 6.2.1.2.

6.3. Other aspects of key pair management

6.3.1. Public key archival

Public keys are archived as part of the archival process for the corresponding certificates.

6.3.2. Key pair and certificate lifespan

Intermediate and Subordinate CA certificates have the same lifespan, which is :

- Less than or equal to 20 years for Intermediate and Subordinate CA certificates.

The end of a Root CA certificate's lifespan shall come after the end of the lifespan of the certificates that it issues.

6.4. Activation data

6.4.1. Activation data generation and installation

6.4.1.1. Root CA private key activation data generation and installation

The generation and installation of activation data for PKI cryptographic modules take place during the module initialization and personalization phase. The activation data are sent to the person responsible in a manner that ensures their confidentiality and integrity. Activation data are known only to the responsible persons, who are identified by name in the context of the roles assigned to them.

6.4.1.2. Intermediate and Subordinate CA private key activation data generation and installation

The generation and installation of activation data for PKI cryptographic modules take place during the module initialization and personalization phase. The activation data are sent to the person responsible in a manner that ensures their confidentiality and integrity. Activation data are known only to the responsible persons, who are identified by name in the context of the roles assigned to them.

6.4.2. Activation data protection

6.4.2.1. Protection of Root CA private key activation data

The activation data are protected in integrity and confidentiality until their delivery to their recipient (*secret shareholder*). Then the recipient is responsible for ensuring its confidentiality, integrity and availability.

6.4.2.2. Protection of Intermediate and Subordinate CA private key activation data

The activation data are protected in integrity and confidentiality until their delivery to their recipient (*secret shareholder*). Then the recipient is responsible for ensuring its confidentiality, integrity and availability.

6.4.3. Other aspects of activation data

No stipulation.

6.5. Computer system security measures

6.5.1. Specific computer system security technical requirements

PKI computer systems provide a level of security that is described in detail in the CPS. In particular, the following areas are covered:

- user identification and strong authentication for system access (*two-factor authentication, physical and/or logical*),
- management of user rights (*enabling implementation of the access control policy defined by the CA, particularly with a view to implementing the principles of least privilege, multiple control and separation of duties*),
- management of user sessions (*disconnection after period of inactivity, access to files controlled by role and user name*),
- protection against computer viruses and all forms of harmful or unauthorized software and software updates,
- management of user accounts, including modifying and swiftly withdrawing access privileges,
- network protection against intrusion by unauthorized persons,
- network protection to ensure the confidentiality and integrity of data conveyed on the network,
- audit functions (*non-repudiation and types of actions carried out*).
- management of any error recoveries.

Confidentiality and integrity protection arrangements for private/secret keys serving infrastructure and control purposes (*cf. chapter 1.4.1.2*) are covered by specific measures defined based on a risk analysis.

Monitoring systems (*with automatic alarms*) and procedures to audit system parameters (particularly routing aspects) are in place where necessary.

6.5.2. Computer system security assessment level

Details are provided in the CPS.

The following rules are applied on the IGC BDF systems in order to ensure an optimum level of security:

- all system engineers are Banque de France employees or from a service provider guaranteeing the same level of security;
- No user account other than that of system engineers or database administrators is created;
- an engineer's account is suspended in the event of departure or prolonged absence;
- all accounts are individual and traceable;
- the audit systems enabling accountability for everyone's actions are put in place;
- sensitive system files are monitored daily to verify their integrity;
- the Firewall server is monitored daily, possible attacks are analyzed and recorded in order to determine the strategy used by the attackers;
- the entire information system is protected by anti-viruses;
- all servers are backed up according to a backup plan associated with a disaster recovery plan;
- an integrity control device ensures that the files on each machine are not damaged.

6.6. System development security measures

Security objectives are set from the specification and design phases.

The CA uses reliable systems and products that are protected against unlawful modification.

6.6.1. System development controls

Banque de France shall ensure that RA programs and systems are developed and implemented in strict compliance with the Banque de France security policy.

Any material change to a system of a PKI component must be reported to the CA for validation. It must be documented, appear in the component's internal operating procedures and be consistent with the compliance assurance scheme, in the case of certified products.

6.6.2. Security management controls

The CA shall ensure that any system changes are recorded.

6.6.3. System life cycle security assessment level

No stipulation.

6.7. Network security controls

The interconnection between PKI systems and public networks is protected by security gateways configured to accept only the protocols necessary for the proper functioning of the PKI.

Local network components (*routers, for example*) are maintained in a physically secure environment and their configurations are periodically audited.

6.8. Time stamping / dating system

To date the events, the various components of the PKI rely on the PKI system time by ensuring synchronization of the clocks of the PKI systems with each other, at least to the minute, and in relation to a reliable source of UTC time, to the nearest second.

This precision of synchronization with respect to UTC time is not required for operations carried out offline (*e.g. administration of Root CA*).

Synchronization with respect to UTC time refers to a system comprising at least two independent time sources.

7. Certificate and CRL/ARL profiles

The attached document [IGC-BDF-v3_Profiles] details the profiles of certificates, the revocation lists (CRL / ARL) and the OCSP service implemented within the framework of this CP.

The document is available on the PKI's publication site at the following address: http://pc.igcv3.certificats.banque-france.fr.

8. Compliance audits and other assessments

Banque de France is responsible for ensuring that PKI components function properly, in accordance with the provisions set out in this document.

To do this, it carries out two types of control: it inspects PKI activities and it checks compliance with the PKI's statutory documents (CP, CPS). Inspections of the PKI's activities are conducted by means of:

- first level/first line inspections, i.e. operational inspections, checks on procedure execution by managers, who report to PKI officers,
- first level/second line inspections, i.e. line inspections of managers,
- second level inspections, which are conducted by Banque de France audit departments.

8.1. Frequency and/or circumstances of assessments

An assessment is conducted every year or exceptionally at the request of the CAPC, and typically after a PKI component is first brought into service or substantially changed.

Furthermore, at the express request of the CAPC, auditors belonging to an audit organization from outside Banque de France may perform an external assessment.

8.2. Identity/qualifications of assessors

The CA shall give responsibility for assessing a component to an audit team with expertise in information system security and in the component's area of activity.

8.3. Assessor's relationship to assessed entity

The audit team must not belong to the entity operating the audited PKI component, no matter which component is being audited. Furthermore, the team must be duly authorized to carry out the inspections in question.

8.4. Topics covered by assessments

Assessments may cover a PKI component (ad hoc controls) or the entire PKI architecture (periodic controls) and shall aim to verify compliance with the commitments and practices set out in the CA's CP and in the related CPS, as well as associated aspects, such as operational procedures and resources deployed.

8.5. Actions taken in response to assessment findings

Following an assessment, a report is provided to the CA and the CAPC.

Where necessary, the CA will prepare an action plan to address the assessors' comments and submit it to the CAPC.

8.6. Communication of results

The CA reserves the right to communicate some or all of the results.

In all cases, the results of compliance audits will be made available to the certification body responsible for certifying the CA.

9. Other business and legal matters

9.1. Fees

9.1.1. Certificate issuance or renewal fees

Certificate issuance and renewal fees are covered in a separate document.

9.1.2. Certificate access fees

No stipulation.

9.1.3. Certificate status and revocation information access fees

Certificate status and revocation information is made available free of charge.

9.1.4. Fees for other services

No stipulation.

9.1.5. Refund policy

No stipulation.

9.2. Financial responsibility

9.2.1. Insurance coverage

Risks that may incur the liability of the CA are covered by an appropriate insurance scheme as described below.

Banque de France is its own insurer and bears the consequences of incidents that incur its liability up to the maximum amounts set out in the terms and conditions of its insurance policies. Beyond these amounts and up to specified ceilings, insurers shall take over the obligations of Banque de France.

Providers of certification services and suppliers of technical infrastructure and signature creation devices used in the PKI must be able to demonstrate that they are independently covered by insurance to cover general third party liability.

9.2.2. Other assets

Own resources suffice to ensure the orderly conduct and completion of CA activities.

9.2.3. Insurance or warranty coverage for user entities

No specific requirement.

9.3. Confidentiality of professional information

9.3.1. Scope of confidential information

The following information is treated as confidential:

- the non-public part of the CPS,
- the private keys of the CA, components and issued certificate,
- activation data for the private keys of the Root CA and issued certificates,
- PKI secrets
- PKI component audit logs,
- Intermediate and Subordinate CA registration files,
- reasons for revocations, unless there is an explicit publication agreement,

9.3.2. Information not within the scope of confidential information

No stipulation.

9.3.3. Responsibility to protect confidential information

The CA has established and complies with security procedures to ensure the confidentiality of information defined as confidential within the meaning of Article 9.3.1 above.

The CA complies with the legislation and regulations in force in France. In particular, the CA may be required to make Intermediate and Subordinate CA registration files available to third parties in the event of legal proceedings.

9.4. Privacy of personal information

9.4.1. Data privacy policy

When collecting and using personal data, the CA and all its components comply strictly with the laws and regulations in force in France, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 applicable from May 25, 2018 (General Data Protection Regulation - GDPR) and Law No. 78-17 of January 6 1978 modified relating to data processing, files and freedoms,.

In accordance with the provisions of the abovementioned act, the automated processing of personal data by the Banque de France PKI has been reported to the Banque de France Data Privacy Officer (DPO).

The CA is responsible of data treatment.

9.4.2. Information treated as personal

The following is treated as personal information within the meaning of GDPR regulation:

- identification information of legal representative or certification agent of the Intermediate and Subordinate CA;
- data entered in the registration file to request a certificate for the Intermediate or Subordinate CA;
- data entered in the certificate revocation application;
- reasons for revoking Intermediate or Subordinate CA certificates (*considered to be confidential unless legal representative or certification agent gives explicit consent to publish*).

Personal data is collected and processed for the sole purpose of implementing the Banque de France PKI and for the use defined under the CP. They are destroyed when their conservation is no longer necessary for the certification and in particular in the following cases:

- Rejection of a certificate request,
- The expiration of the archival retention period specified in article 5.5.2

9.4.3. Information not deemed personal

No stipulation.

9.4.4. Responsibility to protect personal information

Cf. laws and regulations in force in France (in particular cf. chapter 9.15).

9.4.5. Notice and consent to use personal information

The CA may not use personal information for any purpose other than that defined in the framework of the CP without the express, prior consent of the person in question.

Personal information may not be divulged or transferred to a third party without the prior consent of the concerned person, a court ruling or other legal authorization.

9.4.6. Disclosure of personal information to judicial or administrative authorities

Cf. laws and regulations in force in France (in particular cf. 9.15.

9.4.7. Other personal information disclosure circumstances

No stipulation.

9.5. Intellectual and industrial property rights

The laws and regulations in force in France apply.

9.6. Representations and warranties

PKI components have the following shared obligations:

- protect and guarantee the integrity and confidentiality of their secret and/or private keys;
- use their cryptographic keys (public, private and/or secret) only for the purposes provided for when issued and with the tools specified in the terms and conditions set out in this CP and associated documents;
- comply with and enforce the part of the CPS that applies to them;
- be subject to compliance audits conducted by the audit team appointed by the CA (cf. chapter 8) and the certification body;
- comply with the agreements or contracts linking them to each other or to Intermediate or Subordinate CA;
- document their internal operating procedures;
- deploy the technical and human resources necessary to perform the services that they are committed to delivering, under conditions that ensure quality and security.

9.6.1. Certification Authorities

The Root CA is obliged to:

- be able to demonstrate to the users of its certificates that it has issued a certificate to a given Intermediate or Subordinate CA and that the legal representative or certificate agent of this CA responsible entity has accepted the certificate, in accordance with the requirements of chapter 4.4;
- guarantee and maintain the consistency of its CPS with its CP;
- take all reasonable measures to ensure that legal representative or certificate agent are aware of their rights and obligations as regards the use and management of keys, certificates, hardware and software used for the purposes of the PKI. The relationship between an Intermediate or Subordinate CA and the Root CA is formalized by contractual, administrative or regulatory ties that specify the rights and obligations of the parties and particularly the warranties made by the Root CA.

The Root CA shall be liable for any direct harmful consequence of non-compliance with its own CP either by itself or by one of its components. It shall establish the provisions necessary to cover its responsibilities in relation to its operations and/or activities and shall have the financial stability and resources needed to function in compliance with this policy.

The Root CA recognizes that it shall be held liable in the event of misconduct or negligence by it or by one of its components, irrespective of the nature or seriousness of such misconduct or negligence, that results in the personal data of legal representatives or certificate agents being read, altered or misappropriated for fraudulent purposes, whether these data are contained in or transiting through the CA's certificate management applications.

The Root CA recognizes that it has a general duty to oversee the security and integrity of the certificates issued by it or by one of its components. It shall be responsible for maintaining the level of security of the technical infrastructure that it uses to deliver its services. Any change affecting the level of security provided must be approved by the CA's most senior bodies.

9.6.2. Registration service

Cf. obligations in chapter 9.6.1.

9.6.3. Certificate agent

Certificate agent have a duty 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 certificates;
- promptly request revocation (*cf. chapters 3.4 and 4.9*) of a certificate if the private key or activation data are compromised or suspected of being compromised.

9.6.4. Certificate users

Certificate users must:

- comply with the use for which a certificate was issued;
- for each certificate in the certification chain, from the end user's certificate to that of the Root CA, verify the digital signature of the CA issuing the certificate and check the certificate's validity (validity dates, revocation status);
- comply with the obligations of certificate users set out in this CP.

9.6.5. Other participants

Regarding the CO:

As a service provider, the CO undertakes to comply with the CPS and the service contract established with the CA.

9.7. Exclusions and disclaimers of warranties

Cf. chapter 9.2.

9.8. Exclusions and limitations of liability

Article 33 of Digital Economy Confidence Act 2004-575 of 21 June 2004 defines the applicable liability regime.

The Root CA is liable for the requirements and principles established in this CP, and for any damage caused to an Intermediate or Subordinate CA or user resulting from a breach of the procedures defined in the CP and associated CPS.

The Root CA shall bear no liability with respect to the use made of certificates issued by it or of associated public/private key pairs under circumstances or for purposes other than those provided for in the CP or any other associated and applicable contractual document.

The Root CA shall bear no liability for the consequences of delays or losses that may affect electronic messages, letters or documents during transmission, or for delays, modifications or other errors that may arise during the transmission of any telecommunication. The CA shall similarly bear no responsibility for any damage arising from errors or inaccuracies in the information contained in certificates where these errors or inaccuracies are the direct result of errors in the information provided by the legal representative (or certification agent) of Intermediate or Subordinate CA entity.

The Root CA shall not be held responsible for, and makes no commitments with regard to, delays in the performance of obligations or the non-performance of obligations arising from this policy, where the circumstances causing the delay, and which may stem from the partial stoppage, total stoppage or disruption of activity, are the result of force majeure as defined in Article 1148 of the Civil Code.

In addition to the events usually referred to by French case law, the failure of external telecommunications networks or facilities shall be expressly considered to count as cases of force majeure or unforeseen circumstances.

The CA shall under no circumstances be liable for indirect losses suffered by user entities.

9.9. Indemnities

No stipulation.

9.10. CP term and termination

9.10.1. Term

This CP shall remain in effect at least until the expiry of the last certificate issued under the CP.

9.10.2. Termination

Depending on the nature and extent of modifications to the CP, the time requirement for bringing the CP into compliance will be determined in accordance with the procedures provided for under the prevailing regulations.

Furthermore, the process of bringing the CP into compliance shall not necessitate the early renewal of certificates that have already been issued, except in exceptional circumstances relating to security matters.

9.10.3. Effect of termination and survival

No stipulation.

9.11. Individual notices and communications with participants

In the event of a change of any sort to the technical composition of the PKI, the CA undertakes to:

- have the change validated through a technical assessment no later than one month before the start of the operation, in order to assess the impact on the quality and security levels of CA and component functions;
- inform the certification body no later than one month after the end of the operation.

9.12. Amendments to the CP

9.12.1. Amendment procedures

All CP amendments must be submitted to the CAPC.

9.12.2. Amendment notification mechanism and period

No stipulation.

9.12.3. Circumstances under which the OID must be changed

Any change to the CP that materially affects certificates already in issuance should be reflected in a change in the OID, so that users can clearly distinguish which certificates correspond to which requirements.

The OID will be modified in the event of a material change (which will be indicated as such) to the requirements of this CP.

9.13. Dispute resolution provisions

In the event of claims or disputes arising in question with the interpretation or execution of this document or the electronic certification service, the parties in the dispute shall endeavor to settle out of court before taking their case to court.

9.14. Governing law

The laws and regulations in force in France shall apply.

9.15. Compliance with laws and regulations

CA CP/CPS are non-discriminatory.

The laws and regulations applicable to this CP include the following:

Document
Decree 2002-535 of 18 April 2002 on assessment and certification of the security provided by information technology products and systems.
Data Privacy Act 78-17 of 6 January 1978, amended by Act 2004-801 of 6 August 2004.
Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
Digital Economy Confidence Act 2004-575 of 21 June 2004, particularly Article 31 on statements regarding the provision of cryptological services and Article 33, which specifies the liability regime for providers of electronic certification services that issue qualified electronic certificates.
Telecommunications Regulation Act 90-1170 of 29 December 1990 (amended).
Decree 98-101 of 24 February 1998 setting out the conditions for making statements and issuing authorisations concerning cryptological capabilities and services, amended by Decree 2002-688 of 2 May 2002.
Ministerial Order of 17 March 1999 determining the form and content of the file concerning statements or applications for authorisation in relation to cryptological capabilities and services.
Order 2005-1516 of 8 December 2005 on electronic exchanges between users and administrative authorities and between administrative authorities.
Decree 2010-112 of 2 February 2010 implementing Articles 9, 10 and 12 of Order 2005-1516 of 8 December 2005.
Decree 2001-272 of 30 March 2001 implementing Article 1316-4 of the Civil Code concerning electronic signatures.
Ministerial Order of 26 July 2004 on recognising providers of electronic certification services and accrediting organisations that evaluate such providers.
Annex to the Ministerial Order of 26 July 2004 – Technical specifications concerning providers of electronic certification services with a view to recognising such providers.

Table 5 – Applicable laws and regulations

9.16. Miscellaneous provisions

9.16.1. Entire agreement

No stipulation.

9.16.2. Transfer of operations

Cf. chapter 5.8.

9.16.3. Severability

No stipulation.

9.16.4. Enforcement and waiver

No stipulation.

9.16.5. Force majeure

The events usually considered to constitute force majeure in French case law shall be treated as cases of force majeure, namely any event that is unforeseeable, irresistible and beyond the control of the parties.

9.17. Other provisions

No stipulation.

10. Annex 1: Referenced documents

10.1. Regulations

[CNIL]	Law n ° 78-17 of January 6, 1978 relating to data processing, files and freedoms, modified by law n ° 2004-801 of August 6, 2004
[ORDONNANCE]	Ordinance n ° 2005-1516 of December 8, 2005 relating to electronic exchanges between users and administrative authorities and between administrative authorities
[DEC_EXEC_1506]	Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 establishing the specifications for the formats of advanced electronic signatures and advanced electronic seals to be recognized by the public sector bodies referred to in Article 27 (5) , and in Article 37 (5) of the [eIDAS] Regulation.
[eIDAS]	Regulation No. 910/2014 of July 23, 2014 on electronic identification and trust services for electronic transactions within the internal market and repealing Directive No. 1999/93 / EC.
[DécretRGS]	Decree taken for the application of articles 9, 10 and 12 of ordinance n ° 2005-1516 of December 8, 2005

10.2. Technical documents

[RGS]	General Security Repository– Version 2.0
[ETSI EN 319401]	General Policy Requirements for Trust Service Providers
[ETSI EN 319411-1]	Policy & Security Requirements for TSPs Issuing Certificates - Part 1: General requirements
[ETSI EN 319411-2]	Policy & Security Requirements for TSPs Issuing Certificates - Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETSI EN 319412-1]	Certificate Profiles - Part 1: Overview and common data structures
[ETSI EN 319412-2]	Certificate Profiles - Part 2: Certificate profile for certificates issued to natural persons
[ETSI EN 319412-3]	Certificate Profiles - Part 3: Certificate profile for certificates issued to legal persons
[ETSI EN 319412-4]	Certificate Profiles - Part 4: Certificate profile for web site certificates
[ETSI EN 319412-5]	Certificate Profiles - Part 5: QCStatements
[IGC-BDF-v3_Profils]	Certificate profiles, CRL / ARL and OCSP of Banque de France IGCv3
[PSCE_RGS_EIDAS]	Services for issuing qualified certificates for electronic signature, electronic seal and website authentication - Qualification procedures according to the eIDAS regulation for qualified services according to the RGS, applicable version.
[PSCO_QUALIF]	Qualified Trust Service Providers - Criteria for Evaluating Compliance with eIDAS Regulations, Current Version.
[RFC_5280]	Internet Engineering Task Force (IETF) - Request for Comments : 5280 X.509 Internet Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile.
[RFC_6960]	Internet Engineering Task Force (IETF) - Request for Comments : 6960 X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP.

[RFC_3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version d'août 2005 (complétée par les correctifs techniques Corrigendum 1 de janvier 2007et Corrigendum 2 de novembre 2008)
[TS_119_312]	ETSI TS 119 312 V1.1.1 (2014-11) : Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

11. Annex 2: Security requirements of the CA cryptographic module

11.1. Security objective requirements

The cryptographic module, used by the CA to generate and implement its signature keys (*for the generation of electronic certificates, CRL / ARL or OCSP responses*), as well as, if necessary, generate the key pairs of Intermediate or Subordinate CA, must meet the following security requirements:

- If the Intermediate or Subordinate CA key pairs are generated by this module, guarantee that these generations are carried out exclusively by authorized users and guarantee the cryptographic robustness of the generated key pairs;
- If the Intermediate or Subordinate CA key pairs are generated by this module, ensure the confidentiality of private keys and the integrity of the Intermediate or Subordinate CA private and public keys when they are under the responsibility of the CA and during their transfer to the protection of the Intermediate or Subordinate CA secret elements and ensuring their safe destruction after this transfer;
- Ensure the confidentiality and integrity of the CA's private keys throughout their life cycle, and ensure their safe destruction at the end of their life;
- Be able to identify and authenticate its users;
- Limit access to its services according to the user and the role assigned to him;
- Be able to conduct a series of tests to verify that it is functioning properly and enter a safe state if it detects an error;
- Allow the creation of a secure electronic signature, to sign the certificates generated by the CA, which does not reveal the CA private keys and which cannot be falsified without knowledge of these private keys;
- Create audit records for each security change;
- If a backup and restore function for the CA's private keys is offered, guarantee the confidentiality and integrity of the backed up data and require at least a double check of the backup and restore operations.
- Detect attempted physical tampering and enter a safe state when an attempted tampering is detected.

11.2. Certification requirements

The module is certified in accordance with the above requirements, and has been subject to a qualification (*EAL4 + with high resistance of the mechanisms*).