Information Security

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

(OID : 1.2.250.1.115.200.3.1.1.3.1)

Date	***:***	August 18, 2020	***Version***	***:***	1.1
Author	***:***	RSI	***Number of pages***	***:***	**61**

DOCUMENT CONTROL SHEET

List of versions

Version	Date	Author	Amendment
1.0	28/05/2020	DM - RSI	Initial Version
1.1	18/08/2020	RT - RSI	Minor updates

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

TABLE OF CONTENTS

1. INTRODUCTION 5
1.1. OVERVIEW 5
1.2. DOCUMENT NAME AND IDENTIFICATION 6
1.3. DEFINITIONS AND ACRONYMS 6
1.4. PUBLIC KEY INFRASTRUCTURE PARTICIPANTS 9
1.5. CERTIFICATE USAGE 13
1.6. CERTIFICATION POLICY ADMINISTRATION 13
2. RESPONSIBILITY FOR MAKING PUBLISHED INFORMATION AVAILABLE 15
2.1. ENTITIES WITH RESPONSIBILITY FOR MAKING INFORMATION AVAILABLE 15
2.2. PUBLISHED INFORMATION 15
2.3. TIME AND FREQUENCY OF PUBLICATION 16
2.4. ACCESS CONTROLS ON PUBLISHED INFORMATION 16
3. IDENTIFICATION AND AUTHENTICATION 17
3.1. NAMING 17
3.2. INITIAL VALIDATION OF IDENTITY 20
3.3. IDENTIFICATION AND VALIDATION OF RE-KEY REQUESTS 23
3.4. IDENTIFICATION AND VALIDATION OF REVOCATION REQUESTS 23
4. CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS 24
4.1. CERTIFICATE APPLICATIONS 24
4.2. CERTIFICATE APPLICATION PROCESSING 26
4.3. CERTIFICATE ISSUANCE 26
4.4. CERTIFICATE ACCEPTANCE 27
4.5. KEY PAIR AND CERTIFICATE USAGE 28
4.6. CERTIFICATE RENEWAL (WITHIN THE MEANING OF RFC 3647) 28
4.7. NEW CERTIFICATE ISSUANCE FOLLOWING A CHANGE OF KEY PAIR 28
4.8. CERTIFICATE MODIFICATION 29
4.9. CERTIFICATE REVOCATION AND SUSPENSION 29
4.10. CERTIFICATE STATUS INFORMATION FUNCTION 32
4.11. END OF RELATIONS BETWEEN THE HOLDER/CM AND THE CA 32
4.12. KEY ESCROW AND RECOVERY 32
5. NON-TECHNICAL SECURITY MEASURES 35
5.1. PHYSICAL SECURITY MEASURES 35
5.2. PROCEDURAL SECURITY MEASURES 36
5.3. PERSONNEL SECURITY MEASURES 37
5.4. AUDIT LOGGING PROCEDURES 38
5.5. DATA ARCHIVAL 40
5.6. CA KEY CHANGEOVER 41
5.7. COMPROMISE AND DISASTER RECOVERY 41
5.8. PKI TERMINATION 42
6. TECHNICAL SECURITY MEASURES 44
6.1. GENERATION AND INSTALLATION OF KEY PAIRS 44
6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE SECURITY MEASURES 45
6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT 46
6.4. ACTIVATION DATA 46
6.5. COMPUTER SYSTEM SECURITY MEASURES 47
6.6. SYSTEM DEVELOPMENT SECURITY MEASURES 48

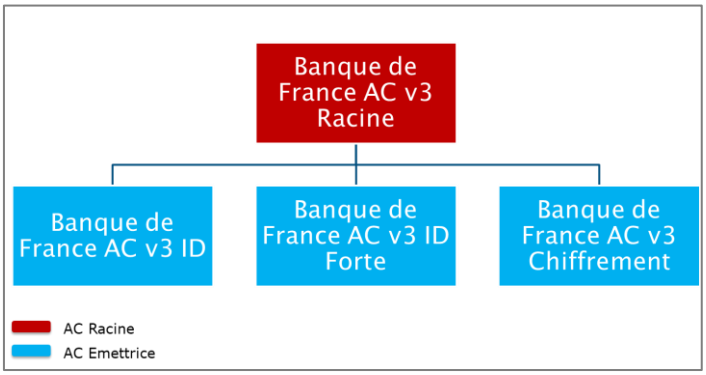
6.7. NETWORK SECURITY CONTROLS 48
6.8. TIME STAMPING / DATING SYSTEM 48
7. CERTIFICATE AND CRL/ARL PROFILES 49
8. COMPLIANCE AUDITS AND OTHER ASSESSMENTS 50
8.1. FREQUENCY AND/OR CIRCUMSTANCES OF ASSESSMENTS 50
8.2. IDENTITY/QUALIFICATIONS OF ASSESSORS 50
8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 50
8.4. TOPICS COVERED BY ASSESSMENTS 50
8.5. ACTIONS TAKEN IN RESPONSE TO ASSESSMENT FINDINGS 50
8.6. COMMUNICATION OF RESULTS 50
9. OTHER BUSINESS AND LEGAL MATTERS 51
9.1. FEES 51
9.2. FINANCIAL RESPONSIBILITY 51
9.3. CONFIDENTIALITY OF PROFESSIONAL INFORMATION 51
9.4. PRIVACY OF PERSONAL INFORMATION 52
9.5. INTELLECTUAL AND INDUSTRIAL PROPERTY RIGHTS 52
9.6. REPRESENTATIONS AND WARRANTIES 53
9.7. EXCLUSIONS AND DISCLAIMERS OF WARRANTIES 54
9.8. EXCLUSIONS AND LIMITATIONS OF LIABILITY 54
9.9. INDEMNITIES 54
9.10. CP TERM AND TERMINATION 54
9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 54
9.12. AMENDMENTS TO THE CP 55
9.13. DISPUTE RESOLUTION PROVISIONS 55
9.14. GOVERNING LAW 55
9.15. COMPLIANCE WITH LAWS AND REGULATIONS 55
9.16. MISCELLANEOUS PROVISIONS 56
9.17. OTHER PROVISIONS 56
10. ANNEX 1: REFERENCED DOCUMENTS 57
10.1. REGULATIONS 57
10.2. TECHNICAL DOCUMENTS 57
11. ANNEX 2: SECURITY REQUIREMENTS OF THE CA CRYPTOGRAPHIC MODULE 59
11.1. SECURITY OBJECTIVE REQUIREMENTS 59
11.2. CERTIFICATION REQUIREMENTS 59
12. ANNEX 3: SECURITY REQUIREMENTS OF THE SECURED DEVICE 60
12.1. SECURITY OBJECTIVE REQUIREMENTS 60
12.2. CERTIFICATION REQUIREMENTS 60
13. ANNEX 4: SECURITY REQUIREMENTS FOR THE SECURED DEVICE 61

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 Chiffrement**" certification authority of Banque de France and contains the public information of the associated Certification Practice Statement (CPS).

The "**Banque de France AC v3 Chiffrement**" Certification Authority issues certificates to members of Banque de France personnel and to the representatives of companies and organizations that deal with Banque de France's business areas.

It issues different range of certificates:

- For Natural persons :
  - Encryption certificates on a software device.
- For application services (Entity type) :
  - Encryption certificates on a software device.
- For application services (Machine type) :
  - Encryption certificates on a software device.

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 Chiffrement

This CP is identified by the following OID : **1.2.250.1.115.200.3.1.1.3.1** and includes the certificate profiles identified by the following OIDs:

Certificate usage	CP OID
Personal encryption	1.2.250.1.115.200.3.1.2.3.1.1.1
Entity encryption	1.2.250.1.115.200.3.1.2.3.2.1.1
Machine encryption	1.2.250.1.115.200.3.1.2.3.3.1.1

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
ESCB	European System of Central Banks
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 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 Banque de France Information Security Officer (RSI) is responsible of the Certification Authorities of Banque de France PKI.

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 certificate holder, 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 holder’s information when the certificate is renewed.
- **Delegated Registration Authority (DRA)** – This function verifies at least the identification information of the certification agent.
- **Certificate generation** - This function generates (format creation, electronic signature with CA private key) certificates using information sent by the Registration Authority and the holder’s public key, provided

either by the holder, or by the holder's secret generation function, if the latter generates the holder's key pair.

- **Holder's secret generation function** - This function generates secret elements for the holder/certificate manager, if the CA is responsible for such generation, and prepares them for delivery to the holder/certificate manager (e.g. personalization of the chip & pin card for the holder, secure mail with activation code, etc.). These secret elements may include, for example, the key pair, activation and unfreezing codes linked to the storage system for the holder's private key or the codes or temporary keys used by the holder/certificate manager to remotely perform the process of generating / retrieving a certificate.
- **Holder/certificate manager delivery** - This function delivers to the holder/certificate manager, as a minimum, his or her 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 CA, the CA's certificates and any other relevant information for holders and/or certificate users, excluding certificate status information. It may also provide, depending on the CA policy, valid holder certificates.
- **Revocation management** - This function processes revocation requests (especially 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).
- **Recovery management function** - This function processes private keys recovery requests (especially verifying the identity and authentication of the party making the request) and determines the steps that need to be taken. In the case of a positive decision, recovery is carried out by the escrow and recovery function.
- **Escrow and recovery function** - This function provides the ability to securely escrow the private key of confidentiality certificates delivered to holders/application services, then to recover them if necessary, on the basis of authenticated requests, by the recovery management function.

A number of outside entities and natural persons also interact with the PKI, including:

- **Holder** – The natural person identified in the certificate and who holds the private key corresponding to the public key in the certificate.

- **Certificate manager for a server or an entity** - Person in charge and responsible for the server's or entity's certificate.

- **Certification agent** – The certification agent is appointed by and placed under the authority of the client entity (holder's entity). The agent deals directly with the RA and performs certain checks on the identity and, where applicable, the attributes of the entity's holders. In particular, the agent handles face-to-face meetings to authenticate holders when this is required.

- **Certificate user** – The entity or natural person who receives a certificate and uses it to verify an electronic signature, or authentication value provided by the certificate holder, or to encrypt data intended for the certificate holder.

- **Authorized person** – A person other than the holder or certification agent who is authorized under the CA's certification policy or an agreement with the CA to perform certain actions on behalf of the holder (such as revocation or renewal requests). Typically, in a company or government agency, this may be the holder's superior or an HR manager.

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 holders' 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 holders 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 the identity of future certificate holders or future certificate managers. To do this, it performs the following tasks:

- registers and verifies:
  - the information on the future holder and the entity with which the holder is affiliated and compiles the registration file;
  - the information on the future certificate manager and the entity with which the certificate manager is affiliated and compiles the registration file;
- where applicable, registers and verifies the information on the future certification agent (cf. last paragraph) and the entity with which the agent is affiliated and compiles the registration file;
- 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);
- stores the personal authentication data of the holder or, where applicable, the certification agent, and protects the confidentiality and integrity of these data, including in exchanges with other PKI functions (compliance with data privacy legislation).

It is also responsible for the secure transmission of private key activation data.

The RA may rely on a certification agent appointed by and placed under the responsibility of the holder's entity to carry out some or all information verification tasks (cf. chapter 1.4.6.2 below). The RA makes sure that requests are complete, exact and carried out by a duly authorized certification agent.

In some cases (*case of a Certificate Manager for an external entity*), the RA can delegate the control of the completeness of the registration file of an External Certificate Manager to an DRA.

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. Certificate holders

The certificate holder is a natural person who may be:

- a Banque de France agent,
- or a Banque de France contractor,
- or the representatives of companies and organizations that deal with the Banque de France's business areas (Natural *person external to Banque de France*). The holder uses his or her private key and corresponding certificate in dealings with the entity identified in the certificate and to which the holder has contractual, administrative or regulatory ties.

Holders must comply with the terms and conditions of this CP.

Banque de France does not issue certificates to private individuals.

1.4.4. Certificate manager

As part of the present CP, a certificate manager (CM) is a natural person who is responsible for the usage of a given server certificate (*entity or machine*) and its corresponding private key.

An application service certificate for an entity can only be issued internally at Banque de France. Any personnel of Banque de France can be a CM for the entity to which they are attached.

An application service certificate for a machine can only be issued to a Banque de France machine. In this case, the CM is the operator of the machine and is necessarily a personnel of Banque de France and in any case cannot be external.

The CM must respect the conditions of use as defined in the present CP.

It should be noted that even if the certificate identifies an application service, it remains attached to the CM. Consequently, in case of CM departure, the certificate of the application service is revoked.

1.4.5. Certificate users

Users are natural persons or devices that use certificates issued by Banque de France.

For the encryption certificates, a user may include:

- An online service that uses an encryption device either to encrypt data or messages sent to a encryption certificate holder;
- A natural person who sends an encrypted message to an encryption certificate holder.

Areas of usage are detailed in Part 1.5.1 of this CP.

Certificate users must comply with the terms defined in this certification policy, especially the requirements of chapter 9.6.4.

1.4.6. Other participants

1.4.6.1. PKI components

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

1.4.6.2. Certification agents

Certification agents are persons who have been authorized to apply for certificates.

Certification agents are natural persons whom Banque de France has recognized as having the authorization to submit certificate applications to the RA. They act as representatives of the RA and deal directly with the PKI's RA.

Certification agents do not have access to resources that would allow them to activate and use the private key associated with the public key contained in the certificate delivered to the holder. The certification agent's commitments towards the CA are specified in a written contract with the entity with which the certification agent is affiliated. Certification agents undertake to:

- perform independent ID checks on future holders of the entity for which they are the certification agent;
- comply with applicable obligations of the CA's CP and CPS.

Internal Banque de France Holders:

No certification agent is involved in the registration process for an internal holder.

External Banque de France Holders:

External holders are authenticated by a certification agent. An entity may use one or more certification agents. A legal representative of the organization in question shall formally notify the Banque de France business area correspondent of the identity of the certification agent. The Banque de France business area correspondent provides the RA with a list of certification agents authorized to submit applications on an organization's behalf.

The entity must notify the CA, if possible beforehand but at least promptly, if a certification agent ceases to perform those functions, and, where applicable, appoint a replacement.

For Banque de France application services (*entity and machine*):

No certification agent is involved in the registration process for an internal Certificate Manager of Banque de France.

"Banque de France AC v3 Chiffrement" CA does not issue an application service certificate to an external entity. There is therefore no intervention of certification agent in this case.

1.4.6.3. 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 uses

1.5.1.1. Holder/application service key pairs and certificates

The “Banque de France AC v3 Chiffrement” CA issues only:

- Encryption certificates *to natural persons*;
- Encryption certificates *to entities and machines*.

Encryption certificate

Holders of encryption certificate can use their certificate to protect data confidentiality (*documents, messages*…) as part of their professional activity when dealing with one of the business areas of Banque de France.

Encryption certificates for application service are used to encrypt data.

Encryption certificate usages are:

- Decryption : with his private key, a certificate holder decrypt received data from electronic exchanges, data having been encrypted with the public key;
- Encryption : with the recipient public key, someone encrypts data

TEST Certificate

In addition, the "Banque de France AC v3 Chiffrement" CA also issues certificates for technical testing and are clearly identified with the mention "TEST" in the DN of the certificate issued.

1.5.1.2. CA and component key pairs and certificates

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

- sign certificates for holders/application services issued by the CA;
- sign the Certificate Revocation Lists (CRLs) issued by the CA;
- sign certificate for OCSP responder.

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 and 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 Chiffrement” 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 holders / certificate managers and certificate users:

Published information	Location
CP/CPS of "*Banque de France AC v3 Chiffrement*» 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* » • « *Banque de France AC v3 Chiffrement*» 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 • « *Banque de France AC v3 Chiffrement*» certificate fingerprint: 39742a74758ea3cca6fe82727471a3d74e744d79
Registration file	The documents of the registration file are available on the publication site: • http://pc.igcv3.certificats.banque-france.fr
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
CRL of « *Banque de France AC v3 Chiffrement*» CA	• http://crl.igcv3.certificats.banque-france.org/chiffrement-1.2.250.1.115.200.3.4.1.3.1.crl • http://crl.igcv3.certificats.banque-france.fr/chiffrement-1.2.250.1.115.200.3.4.1.3.1.crl • ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20Chiffrement,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%20Chiffrement,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 Chiffrement*» CA	• http://ocsp.igcv3.certificats.banque-france.org/chiffrement-1.2.250.1.115.200.3.5.1.3.1 • http://ocsp.igcv3.certificats.banque-france.fr/chiffrement-1.2.250.1.115.200.3.5.1.3.1
General terms and conditions	The General terms and conditions are published on the publication site: • http://pc.igcv3.certificats.banque-france.fr

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.

CA certificates are disseminated prior to any dissemination of certificates for holders/application services and/or corresponding CRL/ARL. The times and frequency of updating CRLs 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 holders/certificate managers 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, a Distinguished Name (as defined by standard X.501) identifies the holder/application service and the issuing CA. Holder 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. Identity of the holders/ application services

Identity of the holders

Holders are identified using the DN, whose composition is as follows:

DN attribute	Value
Country (C)	Applicant's country of residence
OrganizationName (O)	Full official name of the entity (on which the holder depends) as registered with the competent authorities
OrganizationIdentifier (OI)	Official registration number of the entity (on which the holder depends) 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 entity on which the holder depends: 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 organization registered in France.
SerialNumber	Complementary element to distinguish homonyms: SHA-1 fingerprint of the holder's unique internal registration number within the PKI.
CommonName (CN)	The full name of the holder as it should be displayed by the applications. The holder's first name, followed by a space, then the marital status or the holder's last name.

Identity of the application services (*for entity*)

Application services (for entity) are identified using the DN, whose composition is as follows:

DN attribute	**Value**
Country (C)	Applicant's country of residence
OrganizationName (O)	Full official name of the entity (on which the application service depends) as registered with the competent authorities
OrganizationIdentifier (OI)	Official registration number of the entity (on which the application service depends) 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 entity on which the application service depends: 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 organization registered in France.
OrganizationalUnitName (OU)	Name of entity
CommonName (CN)	Meaningful name of the service implementing the certificate

Identity of the application services (*for machine*)

Application services (for machine) are identified using the DN, whose composition is as follows:

DN attribute	**Value**
Country (C)	Applicant's country of residence
OrganizationName (O)	This field is mandatory if the applicant is a legal person, otherwise this field is optional Full official name of the entity (on which the application service depends) as registered with the competent authorities
OrganizationIdentifier (OI)	This field is mandatory if the applicant is a legal person, otherwise this field is optional Official registration number of the entity (on which the application service depends) 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)	This field is mandatory if the applicant is a legal person, otherwise this field is optional In accordance with Annex 2, section VII.1 of [RGS_v2_A4], this field must be present and contain the identification of the entity on which the application service depends: 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 organization registered in France.
OrganizationalUnitName (OU)	Name of the application
CommonName (CN)	Common name of the machine / server.

3.1.2.2. Certificates for testing

Holder certificates used for testing are identifiable with the specific chain “TEST” added in the CN attribute of the DN and preceding the first name and the last name.

Application service certificates used for testing are identifiable with the specific chain “TEST” added in the CN attribute of the DN and preceding the significant name of the service.

3.1.3. Anonymization or pseudonymization of holders/application services

The CA does not authorize anonymization and the use of pseudonyms in the issued certificates.

3.1.4. Rules for interpreting various name forms

Banque de France applies the following rules:

- all characters are in UTF-8 String or Printable String format;
- the CN attribute of encryption certificates for holders includes the first name of the holder followed by a space and then the name of the holder (for married women, the usual name can be entered at following the patronymic name);
- composite given and surnames are separated by dashes " - ",
- the CN attribute of certificates for application services necessarily contains the significant name of the service (*for entity*) or the server implementing the certificate (*for machine*).

3.1.5. Uniqueness of names

The DN Subject field identifies a holder/application service uniquely within the “Banque de France AC v3 Chiffrement” CA.

For an encryption certificate issued to a certificate holder, the uniqueness of the DN within the CA domain is ensured by the attribute "SerialNumber" present in the DN and containing:

- The fingerprint (SHA1) of the unique internal registration number for an internal holder of Banque de France,
- The fingerprint (SHA1) of the email address for an external holder of Banque de France. The email address is a unique data within the Banque de France user identity management system. An email address can only be assigned to one user.

For an application service certificate, the uniqueness of the DN within the CA domain is ensured by the attributes CN and O containing respectively the application service name and the full name of the entity responsible for the certificate. The name of the application service attached to an entity cannot be assigned to another entity.

3.1.6. Identification, authentication and role of registered trademarks

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

3.2. Initial validation of identity

A certificate creates a bond of trust between the holder/application service and the public key contained in the certificate. The initial validation of the identity of a holder/certificate manager, certification agent and organization serves as the basis for the trust placed in certificates issued by “Banque de France AC v3 Chiffrement”.

- For holder certificate:
  - The registration of an internal holder of Banque de France is carried out without Certification Agent.
  - The registration of an external holder of Banque de France must be done with an authorized Certification Agent.

- For an application service certificate for an entity (*exclusively within Banque de France*), the registration of an internal Certificate Manager of Banque de France must be carried out and without Certification Agent.

- For an application service certificate for a machine (*exclusively within Banque de France*), the registration of an internal Certificate Manager of Banque de France must be carried out and without Certification Agent.

When its intervention is needed, the Certification Agent is previously registered by the RA or its registration takes place at the same time of the certificate request.

The "Banque de France AC v3 Chiffrement" CA distinguishes several cases in which the initial validation of the identity of a natural person and / or an entity takes place:

- **Registration of a holder without Certification Agent:** registration during which the identity of the future holder and his attachment to the entity are verified and validated directly by the RA,

- **Registration of a Certificate Manager without Certification Agent for an application service certificate to be issued or registration of a new Certificate Manager for an application service certificate already issued:** registration during which the identity of the future Certificate Manager, his authorization to be Certificate Manager for the application service considered and the entity considered are verified and validated directly by the RA,

- **Registration of a Certification Agent:** registration during which the identity of the Certification Agent entity, the identity of the future Certification Agent and its attachment to the entity are verified and validated by the RA,

- **Registration of a holder via a Certification Agent:** registration during which the identity of the future holder and his attachment to the entity for which the Certification Agent intervenes are verified and validated by the Certificate Agent,

The different registration cases are detailed in chapter 3.2.3.

3.2.1. Method to prove possession of a private key

A certificate creates a bond of trust between a holder and a public key and hence a private key.

For a holder/application service encryption certificate, the key pair is generated by the CA.

3.2.2. Validation of organization identity

Holders use their certificate (*encryption*) as part of their activity in relation to the organization on which they depend and can therefore legally bind this organization. Consequently, the identity of organizations is verified during the validation of the holder identity.

The encryption certificates for a holder are issued exclusively:

- To personnel belonging to Banque de France (*case of internal holders*),
- Or to personnel belonging to external organizations in relation with Banque de France (*case of external holders*). Within the Banque de France, each business area guarantees the relationship established between Banque de France and the organizations.

The encryption certificates for application service (*for entity*) are issued exclusively to services of Banque de France under the responsibility of a Certificate Manager belonging to Banque de France.

The encryption certificates for application service (*for machine*) are issued exclusively to Banque de France servers under the responsibility of a Certificate Manager belonging to Banque de France.

The validation of the entity identity:

- Is considered as carried out for certificate requests for internal Banque de France holders and for internal Banque de France application services (*entity and machine*),

- Is carried out as part of the Certification Agent registration by the RA for certificate requests to external holders of Banque de France. An official proof of the identity of the entity must be provided.

A DRA may be required to verify and send this supporting document to the RA.

The validation of the identity of an entity is detailed in chapter 3.2.3.

3.2.3. Validation of individual identity

Holders and future holders, certificate managers, certification agents, and the legal representatives of organizations are all considered to be individuals.

3.2.3.1. Registering a certification agent

The intervention of a Certification Agent is mandatory for any request for an external holder of Banque de France. Consequently, this section exclusively concerns the registration of a Certification Agent for an external entity.

Certification Agents are registered with the RA in order to verify their authorization to submit requests.

The registration file of a Certification Agent also serves as a reference to formally identify the entity of the future external holders presented by this Certification Agent.

Eventually, a Certification Agent can request certificates issued by “Banque de France AC v3 ID Forte” CA for himself, which can be used afterwards to :

- Sign the holder registration files and send them under electronic form.
- Access an interface to manage certificates of holders or future holders of his entity.

The Certification Agent is appointed by a legal representative of the organization to which he belongs.

The registration of a Certification Agent relies on the provision of a registration file including:

- a signed mandate, and dated within the past 3 months, by a legal representative of the entity designating the Certification Agent. This mandate must be signed by the Certification Agent for acceptance;
- a commitment, dated within the past 3 months, from the Certification Agent, to the CA, to correctly and independently carry out checks on applicants' files;
- a signed commitment, dated within the past 3 months, from the Certification Agent to notify the RA of his departure from the entity;
- any document, valid at the time of the certificate request (*Kbis, or Certificate of identification in the National directory of companies and their establishments, or registration in the trades directory, ...*), attesting to the existence of company and bearing its SIREN number, or, failing this, another document attesting to the unique identification of the company which will appear in the certificate;
- a valid official identity document from the Certification Agent including an identity photograph (*in particular a national identity card, passport or residence permit*), which is presented to the RA who keeps a copy.
- a valid official identity document of the Legal representative including an identity photograph (*in particular national identity card, passport or residence permit*), which is presented to the RA who keeps a copy.
- a signed commitment dated within the past 3 months, by the Certification Agent to validate certificate requests only for users that deal with Banque de France’s business areas.

If necessary, the DRA verifies, signs and transmits the complete registration file for an external Certification Agent to the RA.

A user account on the identity management system of Banque de France is created for any registered Certification Agent *(internal Certification Agent and external Certification Agent*).

The Certification Agent is informed that the use of its user account is necessary to authenticate any certificate request or any revocation request.

3.2.3.2. Registering a holder without certification agent

This section exclusively concerns internal holders of Banque de France. The intervention of a Certification Agent (internal Certification Agent) is not applicable in their case.

For an encryption certificate request, the future holder:

- Must be a member of Banque de France personnel
- Must have a user account on the Banque de France identity management system.

A Banque de France agent or contractor can request an encryption certificate directly from the “Banque de France AC v3 Chiffrement” CA without the need of a registration file.

The holder is informed that the use of his user account is necessary to authenticate any request for a certificate or any request for revocation.

The holder is also informed of the escrow conditions of the private key corresponding to his certificate.

The identity validation for an internal certificate holder is carried out by HR processes. Following the hiring process, a user account is created on the Banque de France identity management system. The holder must then use this user account to authenticate any certificate request.

3.2.3.3. Registering without Certification Agent a Certificate Manager for an application service certificate to be issued or a new Certificate Manager for an application service certificate already issued

This section exclusively concerns internal Banque de France agents or contractors. The intervention of a Certification Agent (internal) is not applicable in their case.

For a request for an application service certificate (*for an entity or a machine*), the future CM:

- Must be a Banque de France agent or contractor,
- Must have a user account on the Banque de France identity management system.

The CM is informed that the use of its user account is necessary to authenticate any request for a certificate or any request for revocation.

The RC is also informed of the escrow conditions of the private key corresponding to the certificate issued for the application service for which he is responsible.

The identity validation for an internal CM is carried out by HR processes. Following the hiring process, a user account is created on the Banque de France identity management system. The CM must then use this user account to authenticate any certificate request.

For an application service – entity type

Any Banque de France agent or contractor can be a CM for the entity to which they are attached.

For an application service – machine type

Banque de France agent or contractor, and responsible for operating a machine is recognized as such on the Banque de France's identity management system and therefore recognized as a CM of the machine by the PKI.

For an application service certificate (*for an entity or a machine*) already issued:

An entity certificate is attached to the requesting CM (*and who receives the certificate*). A change of this user is not possible without certificate revocation.

A machine certificate is attached to an application and to the CM which made the request and received the certificate. Changing this user is not possible without certificate revocation.

In addition, an application is identified by Application Managers, who receive notifications related to the certificate lifecycle. The change of an Application Manager is possible at any time, but there is no direct link between the Application Manager and the CM (*user who made the request*).

3.2.3.4. Registering a holder via a certification agent

This section exclusively concerns external holders of Banque de France. External holders must be authenticated by a Certificate Agent of their entity (*external Certificate Agent*) which must constitute a registration file.

For a request for an encryption certificate, the future holder:

- Must have a user account on the Banque de France identity management system. If he does not have a user account, it is created when the certificate is requested.

For a certificate request for a holder of its perimeter, the Certification Agent constitutes and transmits to the RA a registration file containing:

- a certificate request form, dated within the past 3 months, co-signed by the future holder and by the Certification Agent, indicating in particular:
  - the identity of the holder,
  - the postal address and the email address allowing the CA to contact the holder,
  - private key escrow conditions,
- a copy of the holder's identity document (*valid, containing an identity photograph, in particular a national identity card, passport or residence card*),
- the General Terms and Conditions signed by the holder.

The holder is informed that the use of its user account is necessary to authenticate any further request for a certificate or any request for revocation.

3.2.4. Non-verified holder information

Only UPN and the holder's email address are not subject to any verification.

3.2.5. Validation of applicant's authority

The RA validates the authority of a Certification Agent at the same time of its registration.

For Banque de France agents or contractors, no specific verification is necessary. All agents or contractors of Banque de France are authorized to request a holder certificate for themselves or for an application service depending on their authorization on the PKI.

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 application holder / service automatically leads to the generation and supply of a new certificate.

A new certificate cannot be provided to the holder / application service 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 certificates of the holders / application services can be revoked.

The revocation request may be submitted:

- online, after authentication to the User Portal, using the following address : https://igcv3.certificats.banque-france.fr
- by email (1206-r4f-ut@banque-france.fr),
- or by mail (Banque de France - 39 rue croix des petits champs - 26-1206 Cellule R4F - 75001 Paris),

When the revocation request is made using the online service, the requester is formally authenticated by verification of its username and password (*initially transmitted during its registration*) allowing him to access the online revocation service.

When the revocation request is made by postal mail or email, it should be signed by the applicant and be accompanied by a copy of the applicant's identity document *(national identity card, passport or residence card*). The RA checks the identity of the applicant (*verification of the handwritten signature against the previously recorded signature*), and validate that applicant is authorized to request the certificate revocation.

4. Certificate lifecycle operational requirements

4.1. Certificate applications

A certificate request can be made by all or some of the actors listed below and who have an account on the Banque de France's identity management system:

- The future holder / future CM (*in the case of an application service certificate*)
- A Certification Agent authorized to request certificates (*exclusively in the case of an external holder of Banque de France*),

4.1.1. Who can submit a certificate application

4.1.1.1. Certificate for a holder

A request for a holder encryption certificate can be made for:

- An Internal agent or contractor of Banque de France: in this case, the certificate request is initiated by the future holder.
- An external person of Banque de France: in this case, a certificate request can only be sent to the RA by a Certification Agent with the prior consent of the future holder.

4.1.1.2. Certificate for an application service

A request for an application service encryption certificate can only be made on behalf of:

- An internal Banque de France entity: in this case, the request for a certificate comes from internal agent or contractor of Banque de France attached to the entity concerned.
- An internal Banque de France machine: in this case, the certificate request comes from internal agent or contractor of Banque de France declared as responsible for operating the application in connection with the machine concerned.

4.1.2. Preparing applications: process and responsibilities

A certificate request for a holder or for an application service is initiated:

- Either directly by the future holder / CM from the User Portal,
- Or by the Certification Agent from the Management Portal,
- Either by paper form sent directly to the RA,

In all cases :

- The holder/CM is informed of the escrow conditions of the private key corresponding to the requested certificate,
- The certificate request is processed by the RA.

Request initiated by the future holder / CM on the User portal without Certification Agent:

In this specific case, the future holder / CM is internal agent or contractor of Banque de France and its registration follows the following actions:

- The future holder / CM initiates a certificate request on the User Portal:
  - Case of the holder: for himself,
  - Case of the CM:
    - For an entity type application service only for the entity to which it is attached to the PKI,
    - For a machine-type application service only for a server linked to the application for which it is declared as operations manager on the PKI.
- The future holder / CM accepts general terms and conditions of use online using the User Portal, before submitting the request,
- The RA is notified of the creation of the certificate request on the portal,
- When the electronic request is received on the Management Portal, the RA checks the completeness of the request,
- If the electronic request is complete, the RA validates the certificate request and triggers the issuance of the certificate.

Request initiated by the future holder on the User portal with Certification Agent:

In this specific case, the future holder is an external person of Banque de France and its registration follows the following actions:

- The future holder initiates a certificate request on the User Portal,
- The Certification Agent checks the legitimacy of the electronic request and validates it from the User Portal or from the Management Portal,
- After the validation of the Certification Agent and concomitantly:
    - The RA is informed of the creation of the certificate request on the portal,
    - A certificate request file in electronic format (PDF) is generated and is sent by email to the Certification Agent.
- The Certification Agent prints the request file and meets the future holder / CM to sign together the printed request file.
- The Certification Agent sends the RA the complete and signed request file.
- When the signed request file is received, the RA checks the request file and its consistency with the electronic request on the Management Portal,
- If the file is complete and consistent with the electronic request, the RA validates the certificate request and triggers the issuance of the certificate.

Request initiated by the Certification Agent on the Management Portal:

In this specific case, the future holder is an external person of Banque de France and its registration follows the following actions:

- The Certification Agent initiates the certificate request for a future holder on the Management Portal,
- At the end of the creation of the Certification Agent request and concomitantly:
    - The RA is informed of the creation of the certificate request on the portal,
    - A certificate request file in electronic format (PDF) is generated and is sent by email to the Certification Agent.
- The Certificate Agent prints the request file and meets the future holder to sign together the printed request file.
- The Certificate Agent sends to the RA the complete and signed request file.
- When the signed request file is received, the RA checks the request file and its consistency with the electronic request on the Management Portal,
- If the file is complete and consistent with the electronic request, the RA validates the certificate request and triggers the issuance of the certificate.

Request sent in paper format to the RA:

The certificate request can be sent by an authorized Certification Agent in paper format to the RA. This system only concerns certificate requests requiring the intervention of a Certification Agent (*requests for external holders of Banque de France*).

If necessary, the elements of the certificate request file, as well as those of the Certification Agent registration, can be downloaded from the institutional site of Banque de France.

In that case:

- The Certification Agent downloads the blank certificate request file available on the Banque de France institutional site,
    - The request file contains the elements of the certificate request and, if applicable, the elements of the Certification Agent registration file if it is not yet registered.
- The Certification Agent prints the request file and meets the future holder to sign together the printed request file.
- The Certification Agent sends the RA the complete and signed request file.
- When the signed file is received, the RA checks the file then creates the certificate request on the Management Portal and triggers the issuance of the certificate.

4.1.2.1. For a holder’s certificate

An encryption certificate request for a holder contains at least the following information:

- the surname and first name (s) of the holder;
- internal registration number (for an internal agent or contractor of Banque de France) ;
- the holder's email address;
- the name of the holder's entity and its identifier (In France, *SIREN or SIRET number*).

4.1.2.2. For an application service certificate (*entity type*)

An encryption certificate request for an entity type application service contains at least the following information:

- The significant name of the entity or service;
- The surname and first name (s) of the CM;
- The internal registration number of the CM;
- The CM's email address;
- The name of the entity and its identifier (*SIREN or SIRET number*);

4.1.2.3. For an application service certificate (*machine type*)

An encryption certificate request for a machine-type application service contains at least the following information:

- The significant name of the server;
- The surname and first name (s) of the CM;
- The CM's email address;
- The name of the entity to which the server is attached and its identifier (*SIREN or SIRET number*);

4.2. Certificate application processing

4.2.1. Performing application identification and validation processes

The identities of "natural persons" and "legal entities" are verified in accordance with the requirements of chapter 3.2.

The identification and validation processes of the request are explained in chapter 4.1.2.

At the end of the request validation, the RA sends the request to generate the certificate to the appropriate PKI function (see chapter *1.4.1*).

Then the RA keeps a record of the proof of identity presented in particular in the case of a certificate request for an external holder of Banque de France.

4.2.2. Application acceptance or rejection

If the application is rejected, the RA informs the holder / CM and the Certification Agent giving the reasons for rejection.

4.2.3. Processing time

Complete files will be processed within ten working days following receipt of the application (signed application file if external holder).

4.3. Certificate issuance

When the request is validated by the RA, the RA triggers the certificate generation process to the CA certificate management function.

The holder/application service encryption certificate and the associated private key are generated and stored by the CA in a software container protected by a password. This container is made available to the holder/CM for a one-time access on the User Portal.

The use of the private key is protected by entering "activation data" (*password*). Activation data is only available for holder/CM after authentication on the User Portal.

Retrieval of activation data can only be done if the software archive has been previously retrieved from the User Portal. Activation data is not made available at the same time as the software archive on the User Portal.

4.3.1. CA actions during certificate issuance

For any request for a holder encryption certificate, the CA performs the following operations:

- Authentication of the origin of the request (RA);
- Verification of the integrity of the request;

- Technical verification of the request;
- Generation of the key pair by the CA;
- Creation of the certificate of the future holder;
- Signing of the certificate using the CA's private key;
- Software container creation, including private key and certificate.

For any request for an application service encryption certificate for entity, the CA performs the following operations:

- Authentication of the origin of the request (RA);
- Verification of the integrity of the request;
- Technical verification of the request;
- Generation of the key pair by the CA;
- Creation of the service certificate;
- Signing of the certificate using the CA's private key;
- Software container creation, including private key and certificate;

All of these operations are detailed in the CPS.

The conditions for generating keys and certificates, as well as the mandatory security measures, are specified in chapters 5 and 6.

4.3.2. CA notification of certificate issuance to holder / CM

The CA notifies the holder/CM of the issuance of the certificate and of the availability of the certificate software container. The holder/CM is requested to retrieve this software container on the User Portal.

4.4. Certificate acceptance

4.4.1. Certificate acceptance procedure

The acceptance of a certificate implies acceptance of the CP of the CA "Banque de France AC v3 Chiffrement".

4.4.1.1. For a holder's certificate

The acceptance process is carried out once the holder has retrieved successively his certificate software container and the associated password from the User Portal.

Acceptance of the certificate by the holder is carried out online on the User Portal.

The holder has a period of 21 days to accept his certificate. After this period, the CA takes measures up to the revocation of the certificate.

However, the holder is required to notify the RA and his Certification Agent if applicable of any inaccuracy or defect in the certificate or in the retrieved certificate software container. If applicable, the certificate is revoked by the CA.

If the certificate is explicitly refused by the certificate holder, the certificate is revoked by the CA.

Online acceptance

At the end of the password retrieval process, the holder is invited to verify the information of the certificate (*at least the DN of the certificate and the serial number*). On this occasion, the certificate information is presented to the holder who must confirm that it is correct or not.

4.4.1.2. For an application service certificate (entity or machine type)

The acceptance process is carried out once the CM has retrieved successively his certificate software container and the associated password from the User Portal.

The acceptance of the entity certificate by the CM is carried out online on the User Portal.

The CM has 21 days to accept the certificate. After this period, the CA takes measures up to the revocation of the certificate.

However, the CM is required to notify of any inaccuracy or defect in the retrieved certificate or in the certificate software container. If applicable, the certificate is revoked by the CA.

If the certificate is explicitly refused by the CM, the certificate is revoked by the CA.

Online acceptance

At the end of the certificate retrieval process, the CM is invited to verify the certificate information (*at least the certificate DN and the serial number*). On this occasion, the certificate information is presented to the CM who must confirm that it is correct or not.

4.4.2. Certificate publication

The certificates of Banque de France CAs are published (as defined in paragraph 2.2).

Holder certificates are published in a database accessible from the internal network of Banque de France.

Application service certificates are not published.

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

The RA and the Certification Agent if applicable are informed of the issuance of the certificate.

4.5. Key pair and certificate usage

4.5.1. Holder / CM 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. Holders / CM undertake to strictly respect the authorized uses. Otherwise, they may be held liable, and the associated certificate could be revoked.

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

- For holders:
  - to “keyEncipherment“for encryption certificates,
- For application services (*entity and machine type*):
  - to “keyEncipherment“for encryption certificates,

4.5.2. Certificate user public key and certificate usage

Certificate users should 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 holder / application service*). The generation of a new key pair is systematic for any certificate issuance.

However, a notification is sent to the holder / CM at the approach of the expiration date of the certificate to prepare a renewal in the sense of the issuance of a new certificate (see chapter 4.7).

4.7. New certificate issuance following a change of key pair

4.7.1. Possible reasons for a change of key pair

The key pairs of holders / application services and the corresponding certificates are renewed respectively at least every 3 years and 2 years.

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

- early,
- or following the revocation of the holder's certificate / application service (*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 holder.

4.7.2. Who can submit an application for a new certificate

A notification is sent to the holder / CM before the expiration date of the certificate in order to prepare for the issuance of a new certificate.

The trigger for the issuance of a new certificate can be:

- either automatic (*as part of the notification when the certificate expires*),
- either at the initiative of the holder / CM or of the Certification Agent if applicable.

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 to holder / CM

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 and other than only modification of validity dates (*cf. chapter*), 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

When one of the circumstances described below occurs and when 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 CRL until the certificate has not reached its expiry date.

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

4.9.1.1. Holder / application services certificates

A holder's / application service's certificate may be revoked in the following circumstances:

- the holder information appearing in the certificate is not or is no longer consistent with the identity information or the usage provided for in the certificate (*including if the holder leaves the entity or changes function*) and the certificate has not reached its normal expiry date,
- the holder / CM fails to comply with the procedures for using the certificate,
- the holder / CM and/or, as the case may be, the Certification Agent / entity have failed to meet their obligations under the CP governing the certificate,
- an error, whether intentional or not, is found in the holder's / CM's registration file,
- the private key associated with the holder's /application service's certificate is suspected of being compromised, or is compromised, lost or stolen (*potentially the associated activation data*),
- the holder / CM or an authorized entity (*legal representative of the entity or the certification agent for example*) asks for the certificate to be revoked (*particularly if the holder's private key and/or the device on which the key is stored is destroyed or modified*),
- the holder / CM dies,
- the holder's / CM's entity terminates operations.

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. Holder / application service certificates

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

- For a holder certificate:
  - the holder in whose name the certificate was issued,
  - a Certification Agent of the holder's entity (*exclusively for an external holder of Banque de France*),
  - a legal representative of the holder's organization,
  - the CA that issued the certificate,
  - the RA attached to the CA.
- For an application service certificate (*entity or machine*)
  - the CM registered for the application service considered,
  - a legal representative of the CM's organization,
  - the CA that issued the certificate,
  - the RA attached to the CA.

The requestor authentication, and the request validity, are done according to the procedures described in 3.3.2.

The certificate holder / CM is notified when an authorized requestor makes a revocation request.

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

The holder / CM (*or authorized person or entity*) must prepare a revocation request promptly on learning that one of the circumstances for revocation has arisen.

4.9.3.1. Holder / application service 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 in 3.3.2.

The revocation request must contain at least the following information:

- identity of the certificate holder / application service used in the certificate (*including surname and given names / service or server name*),
- the name of the party requesting revocation,
- 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 RA will revoke the certificate by changing its status and then informing the certificate status information function of the new status. The revocation notification is disseminated by a real-time responder (OCSP) and by adding the certificate's serial number and revocation date to the CRL.

If the request is not admissible, the RA informs the party making the request via the DRA or the Certification Agent.

The party making the request, the holder/CM and, via the Certification Agent, the entity, are informed by email that the revocation request has been registered by an acknowledgement of receipt issued by the RA.

The revocation is logged by the "Banque de France AC v3 Chiffrement" CA. The RA records and archives revocation requests.

The reasons for definitive certificate revocation are not published. Any revoked certificate is systematically removed from the internally accessible database if necessary.

The CPS provides additional information on the procedure for processing revocations.

4.9.3.2. PKI component certificates

The CPS details the procedure that must be followed to revoke the certificate of a PKI component.

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

- all affected holders/CM must be promptly informed via their Certification Agent 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 holder/CM to prepare a revocation request

The holder/CM 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. Holder/application service certificates

The RA processes requests as soon as they arrive

The CA updates and publishes the CRL no more than 24 hours after the RA records the authenticated revocation request.

The revocation management function is available 24/7.

This function has a maximum duration of unavailability per interruption of service (*breakdown or maintenance*) in accordance with 2 hours and a maximum total duration of unavailability per month in accordance with 8 hours.

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 holder’s/application service’s 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

CRLs are generated at least once every 24 hours.

4.9.8. Maximum latency for CRLs

The CRL 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 CRL 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:

Holder/application service 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.

The holder/CM:

- shall immediately and definitively interrupt the use of his encryption certificate;
- Undertake, as far as possible, to decrypt the data previously encrypted using the compromised encryption certificate and to protect their confidentiality by any other means.

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 holder/CM and the CA

If relations between the holder and the CA are terminated before the end of the certificate validity period, the Registration Authority will revoke the holder's certificate.

The CA revokes any electronic certificate for which there is no longer an explicitly identified CM.

4.12. Key escrow and recovery

A key escrow of holder/application service private keys is realized as part of the present CP.

Key escrow is restricted to private keys corresponding to encryption certificates issued by the CA "Banque de France AC v3 Chiffrement".

4.12.1. Key escrow recovery practices and policies

4.12.1.1. Key escrow request

Any request for an encryption certificate (for a holder or an application service) issued by the CA "Banque de France AC v3 Chiffrement" includes systematically the private key escrow.

Registration requests and registration files systematically include information about the key escrow which is mandatory for certificates issued by the CA "Banque de France AC v3 Chiffrement".

Private key escrow retention period for encryption certificates issued by the CA "Banque de France AC v3 Encryption" is ten years from the key pair generation.

The holder/CM is informed of the private key escrow realized for the certificate he is requesting as well as of its retention period.

4.12.1.2. Key escrow processing

Once the request for an encryption certificate has been validated by the RA, this triggers the certificate issuing process including the generation of the key pair and the certificate delivery. The private key corresponding to the certificate issued by the CA "Banque de France AC v3 Chiffrement" is systematically subject to a key escrow following its generation.

The private key is stored by the CA's escrow and recovery function in an encrypted form for a period of ten years and is recoverable over this period even if the associated certificate has expired or been revoked.

The private key stored within the CA's escrow and recovery function is identified by the serial number of the associated certificate.

The escrow conditions are detailed in the CPS.

4.12.1.3. Origin of a recovery request

A recovery request for a holder private key can be made by:

- The holder himself,
- A legal representative of the holder's entity,
- The CM if applicable,
- RA,
- Any entity authorized by law.

A recovery request for of an application service private key can be made by:

- The registered CM,
- A legal representative of the entity responsible for the application service,
- RA,
- Any entity authorized by law.

4.12.1.4. Identification and validation of a recovery request

A key recovery request for a holder/application service private key can be made via:

- An online service,
- By mail (Banque de France - 39 rue croix des petits champs - 26-1206 Cellule R4F - 75001 Paris),

When the recovery request is made via the online service, the requester is duly authenticated by verifying his username and password (initially transmitted during their registration) allowing them to access the online recovery service.

When the recovery request is made by mail, it must be signed by the applicant and include a copy of an identity document of the applicant (e.g. identity card, passport or residence permit). The recovery management service verifies the identity of the requester (verification of the handwritten signature against the previously recorded signature) and his authority on the certificate associated to the private key to recover.

In all cases, the recovery request includes at least:

- The reason for recovering the private key,
- Information to identify the private key to be recovered (serial number of the associated certificate, name of the certificate holder).

4.12.1.5. Recovery request processing

Following the applicant identification and recovery request validation, the recovery management service issues the request to the CA's escrow and recovery function. The request is protected in integrity and confidentiality.

At least two RA operators, specifically authorized to recover keys, are necessary to perform the recovery of the holder/ application service private key. These operators are authenticated by the escrow and recovery function prior to the recovery operation.

4.12.1.6. Destruction of escrowed keys

At the end of the retention period of an escrowed private key, any copy of this key stored by the CA is destroyed in a reliable manner, so that no one can neither recover nor reconstitute the key.

4.12.1.7. Availability of escrow and recovery functions

The escrow and recovery function is available 24/7.

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 holder 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 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, 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 role.

People with a trusted role 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,
- sending the key and certificate software container to the holder / CM,
- acknowledgment of receipt of the holder / CM

- explicit acceptance or rejection by the holder / CM,
- activation of the support by the holder,
- receipt of a recovery request for a holder/application service private key,
- validation / rejection of a recovery request,
- delivery of a recovered private key to the requester.

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 holders / application services,
- generation of certificates for holders / application services,
- 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 CRLs,
- OCSP requests and responses,
- holder/application service private key escrow
- private key recovery.

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 or holder code, 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*),
- commitments signed by Certification Agents,
- identity documentation for holders / CM 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.

The archives can be made available to authorized persons (*defined in the CPS relating to this CP*) within two (2) working days.

5.5.2. Archival retention period

For certificate request files:

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

For holder/application service private key recovery request files:

- the files and supporting documents are archived for a period of five (5) years from the end date of the corresponding private key by the CA of the.
- At the end of the 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 ten years at least from their generation.

- When due, the CRL issued by the CA are destroyed.

For OCSP responses:

- OCSP responses are kept for three months at least from their expiration date.
- When due, the OCSP responses are destroyed.

For event logs:

- event logs are kept for ten years at least from their generation date.
- When due, 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 holders / CMs 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 holders / CM 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 holder 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 holders/CM and Certification Agents using the method of its choosing, giving them notice of two 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 holders/CM 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;
- provide notification to all Certification Agents and/or to holders/CM of certificates that have been or will be revoked, as well as to their affiliated entity (cf. chapter 3.2.3).

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. These secrets are managed according to the provisions of the Root CA's CP.

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. Holder keys generated by CA

Holders' keys are generated by the CA in a secured environment. Generated private keys are escrowed by the CA.

6.1.1.3. Application service keys generated by CA

The application services keys (entity and machine) are generated by the CA in a secured environment. Generated private keys are escrowed by the CA.

6.1.2. Private key delivery to holders

The private key and the associated holder/application service certificate are generated by the CA and then stored in a software container protected by a password. This container is made available to the holder/CM for a one-time access through the User Portal.

6.1.3. Public key delivery to CA

Holders'/application services' 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 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.

Subordinate CAs use a 4096 bit RSA key.

Holders and application services use an RSA key with a length equal to or greater than 2048 bits.

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 holder/application service's key pair is generated and stored in a software container protected by a password.

6.1.7. Key usage purposes

The use of a CA private key and associated certificate is strictly restricted to signing certificates, CRLs/ARLs and OCSP signing certificates.

The use of holder/application service's private keys is restricted to confidentiality service.

6.2. Private key protection and cryptographic module security measures

6.2.1. Cryptographic module security standards and measures

6.2.1.1. CA cryptographic modules

For the generation and implementation of its signature keys, the "Banque de France AC v3 Chiffrement" 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. Holder secured device

The holder's key pair and the associated holder certificate are generated by the CA, and stored in a software container protected by a password. Private key and certificate are then installed on the holder computer.

6.2.1.3. Secured devices for application services

The key pair and the associated application service certificate are generated by the CA, and stored in a software container protected by a password. Private key and certificate are then installed on the affected server.

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

CA private keys are not escrowed.

Holders'/application services' private keys associated to certificates issued by « Banque de France AC v3 Chiffrement » are escrowed by the CA.

6.2.4. Private key backup

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

Private keys of the holders / application services are escrowed by the CA. Escrow and recovery operations are detailed in the CPS

6.2.5. Private key archival

CA private keys are not archived.

Holders'/application services' private keys are not archived.

6.2.6. Private key transfer into/from a cryptographic module

The holder/application service private key stored in a software container and protected by a password is made available directly to the holder/CM through the User Portal, hence ensuring its integrity and confidentiality.

The use of a secured device is not intended for the private key of a holder / application service.

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

6.2.7. Private key storage in a cryptographic module

The CA uses a cryptographic module to store its private key.

See paragraph 6.2.1.1.

6.2.8. Method of activating private key

6.2.8.1. CA private key

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

6.2.8.2. Holder private keys

Private keys in software containers are activated by entering a password (*cf. chapter 6.4*). Passwords are delivered through the User Portal.

6.2.8.3. Private key of an application service

The private key stored in a software container, is activated by entering a password (*see chapter 6.4*). The password is transmitted through the User Portal.

6.2.9. Method of deactivating private key

6.2.9.1. CA private key

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.

6.2.9.2. Holder private keys

The private key deactivation method corresponds with key deletion from the holder's computer..

6.2.9.3. Private key of an application service

The private key deactivation method corresponds with key deletion from the server.

6.2.10. Method of destroying private key

6.2.10.1. CA private key

At the normal or early (e.g. owing to revocation) end of 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. Holder private keys

The "logical" destruction of a holder's private key can only be done on the holder's computer.

6.2.10.3. Private key of an application service

The "logical" destruction of an application service's private key can only be done on the affected server.

6.2.11. Cryptographic module security assessment rating

Cf. paragraph 6.2.1.

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

Holders'/application services' certificates and key pairs have the same lifespan.

This lifespan is less than or equal to 3 years;

The end of a 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. 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. Holder private key activation data generation and installation

Holders' keys are generated by the CA, and stored in a PKCS#12 software container protected by a password initialized by the CA. Activation data (passwords) are made available directly to the holder through the User Portal, hence ensuring their integrity and confidentiality.

PKCS#12 software container and activation data are never available at the same time on User Portal. They are transmitted at different moments.

The procedure is detailed in the CPS.

6.4.1.3. Application service private key activation data generation and installation

The keys of the application services are generated by the CA, and stored in a PKCS#12 software container protected by a password initialized by the CA. Activation data (passwords) are made available directly to the CM through the User Portal, hence ensuring their integrity and confidentiality.

PKCS#12 software container and activation data are never available at the same time on User Portal. They are transmitted at different moments

The operations are described in the CPS.

6.4.2. Activation data protection

6.4.2.1. Protection of CA private key activation data

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

6.4.2.2. Holder private key activation data protection

Activation data is protected in confidentiality until it is delivered to the holder. When this data is saved by the CA, it is protected in confidentiality.

6.4.2.3. Application service private key activation data protection

The activation data are protected in integrity and confidentiality until their delivery to the CM. When this data is saved by the CA, it is protected in integrity and confidentiality.

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 [Banque_De_France_PKI_Certificate_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 IGCv3 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 certificate holders,
- activation data for the private keys of the CA and holders/application services,
- PKI secrets
- PKI component audit logs,
- holder/CM 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 holders'/CMs' registration files available to third parties in the event of legal proceedings.

The CA also gives holders/CMs access to their information.

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 information

The following is treated as personal information:

- identification information of the holder/CM, certification agent or legal representative of the organization dealing with Banque de France;
- data entered in the registration file to request a certificate for the holder/application service;
- data entered in the certificate revocation application;
- reasons for revoking holder/application service certificates (*considered to be confidential unless holder/CM gives explicit consent to publish*).

The personal data collected is 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 holder/CM, 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 holders/CM;
- 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 CA is obliged to:

- be able to demonstrate to the users of its certificates that it has issued a certificate to a given holder and that this holder 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 holders 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 a holder and the 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 CA.

The 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 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 holders being read, altered or misappropriated for fraudulent purposes, whether these data are contained in or transiting through the CA's certificate management applications.

The 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 holders/CM

Holders/CM have a duty to:

- provide accurate and up to date information when applying for or renewing a certificate;
- protect their private key/the server private key by means that are appropriate to their environment;
- protect their activation data and use them only when necessary;
- comply with the terms for using private keys/ the server private key and corresponding certificates;
- 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.

The relationship between a holder/CM and the CA or its components shall be formalized by a commitment on the part of the holder/CM certifying the accuracy of the information and documents provided.

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 holder'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 CA is liable for the requirements and principles established in this CP, and for any damage caused to a certificate holder or user resulting from a breach of the procedures defined in the CP and associated CPS.

The 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 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 holder or certification agent.

The 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

Since the OID of the CA's CP is written in the certificates that the authority issues, any change to the CP that materially affects certificates already in issuance (e.g. strengthened registration requirements for holders, which cannot apply to previously issued certificates) must 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 case in French 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
[Banque_De_France_PKI_Certificate_Profiles]	Certificate profiles, CRL / ARL and OCSP of Banque de France PKI
[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 holders, must meet the following security requirements:

- If the holder' 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 holders' key pairs are generated by this module, ensure the confidentiality of private keys and the integrity of the holders' private and public keys when they are under the responsibility of the CA and during their transfer to the protection of the holder's 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*).

12. Annex 3: Security requirements of the secured device

12.1. Security objective requirements

The device for protecting the holder's secret elements, used by the holder to store and use his private key and, if necessary, generate his key pair, must meet the following security requirements:

- If the holder's key pair is generated by the device, guarantee that this generation is carried out exclusively by authorized users and guarantee the cryptographic robustness of the generated key pair;
- Detect faults during the initialization, personalization and operation phases and have secure techniques for destroying private keys;
- Guarantee the confidentiality and integrity of private keys;
- Ensure correspondence between the private key and the public key;
- Generate a security function which cannot be falsified without knowledge of the private key;
- Ensure the security function for the legitimate holder only and protect the private key against any use by third parties;
- Guarantee the authenticity and integrity of the public key when it is exported from the device.

12.2. Certification requirements

No certification is required for the secured device used by the holder or the CM except to comply with the requirements set out above.

13. Annex 4: Security requirements for the secured device

The device for protecting secret elements, used by the application service to store and use its private key and, if necessary, generate its key pair, must meet the following security requirements:

- If the application service key pair is generated by the device, ensure that this generation is carried out exclusively by authorized users and guarantee the cryptographic robustness of the key pair generated;
- Ensure correspondence between the private key and the public key;
- Generate an authentication which cannot be falsified without the knowledge of the private key.

In addition, organizational, procedural or technical security measures must be put in place in order to:

- Detect faults during the initialization and operation phases and have reliable techniques for destroying the private key in the event of re-generation of the private key;
- Guarantee the confidentiality and integrity of the private key;
- Guarantee the authenticity and integrity of the public key when it is exported from the device.
- Ensure for the legitimate server only, on the one hand, the authentication function and, on the other hand, the decryption function of symmetric session keys, and protect the private key against any use by third parties;
- Ensure the authenticity and integrity of the symmetric session key, once decrypted, when exported from the device to the data decryption application.