1. Purpose of the Document

This document constitutes the general terms and conditions of the Certification Authority « **Banque de France AC v3 Chiffrement** » of Banque de France.
It presents, in summary, the « **Banque de France AC v3 Chiffrement** » Certification Policy, referenced under the OID **1.2.250.1.115.200.3.1.1.3.1**.

2. Definitions and Acronyms

The **Client** designates the legal entity of the holder who acquires a certificate from the CA « Banque de France AC v3 ID ».
The **Holder** designates the natural person for whom a certificate is issued.
The **Certificate Manager (CM)** designates the natural person responsible for the use of the certificate of an application service identified in the certificate, and the corresponding private key.
The **Certificate Agent** designates the natural person authorized to request certificates to the Registration Authority.
The **User Portal** designates the interface used by any user of the PKI (Holders and Certificate Managers) for requesting and managing their certificates.

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ARL	Authority Revocation List
CA	Certification Authority
CAPC	Certification Policies Approval Committee
CM	Certificate Manager
CP	Certification Policy
CRL	Certificate Revocation List
LDAP	Light Directory Access Protocol
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PDS	PKI Disclosure Statement
QSCD	Qualified Signature Creation Device
RA	Registration Authority

3. Certification Authority contact information

Responsable de la Sécurité de l'Information (RSI)
RSI Banque de France
39 rue croix des petits champs
Email : 1206-crypto-ut@banque-france.fr

4. Certificate profiles

The « **Banque de France AC v3 Chiffrement** » issues different ranges of certificates :

- Encryption certificates for Banque de France employees and contractors, and for the representatives of companies and organizations that deal with Banque de France's business areas.
- Encryption certificates for application services (Entity and machine type) of Banque de France.

Certificates profiles issued by « **Banque de France AC v3 Chiffrement** » are referenced under the following OID:

For a natural person	
Personal encryption	1.2.250.1.115.200.3.1.2.3.1.1.1

For an application service – entity type	
Entity encryption	1.2.250.1.115.200.3.1.2.3.2.1.1

For an application service – machine type	
Machine encryption	1.2.250.1.115.200.3.1.2.3.3.1.1

Certificates are issued in accordance with the certification policy published at the following address: http://pc.igcv3.certificats.banque-france.fr .
Certificates are issued through the following certification chain:

Banque de France AC v3 Racine
|
Banque de France AC v3 Chiffrement

The certificates of the certification chain are available at the following address: http://pc.igcv3.certificats.banque-france.fr .
Any third-party application wishing to use the certificates of the certification chain must make a prior request by writing to the point of contact defined above.

5. Subject of certificates

Encryption certificates issued by « **Banque de France AC v3 Chiffrement** » CA are intended for Natural persons (holders):

- Banque de France employees and contractors,
- Members of companies and organizations that deal with Banque de France's business areas.

These certificates are generated by the CA and stored in a software container protected by a password and delivered to each holder.
Generated private keys are escrowed by the Certification Authority.

Encryption certificates for application services (entity and machines) issued by the "**Banque de France AC v3 Chiffrement**" CA are intended for Banque de France application services. These certificates are generated by the CA and stored in a software container protected by a password, and delivered to each CM.
Generated private keys are escrowed by the Certification Authority.

6. Duration

The current Terms and Conditions are enforceable against the client and the holder/CM upon signature and, in the absence of signature, upon first use of the certificate.
The Terms and Conditions are enforceable throughout the certificate validity period (three years), without prejudice to their possible updates.
The CA undertakes to communicate by any means at its disposal (email, online publication, etc.) any new version of the Terms and Conditions.
Any use of the certificate after the modifications or updates of the Terms and conditions implies acceptance of the new Terms and Conditions by the client and the holder/CM.

7. Certificate application, validation and issuance procedure

7.1 Encryption certificate for a natural person

1. Preparation and presentation of the certificate application

For any application for an encryption certificate for a natural person,
the future holder must have a user account on the identity and access management system of the Banque de France. If the future holder does not have a user account, it is created when the certificate is requested.
For a Banque de France employee or contractor, the certificate request does not require a registration file.
For a member of companies or organizations that deal with Banque de France's business areas, the certificate request must be sent to the RA by a previously registrated certification agent designated by the client.
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 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,
- 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.
The holder is also informed about private key escrow conditions.

2. Verification of the certificate application

The RA controls :

- The completeness of the electronic request for a Banque de France employee or contractor,
- The completeness and consistency of the registration file, in particular consistency between the request form and the provided supporting documents, for a member of companies or organizations that deal with Banque de France business areas.

3. Decision to validate or reject the certificate request

After verification of the completeness of the certificate request, and the consistency of the registration file if applicable, the RA takes the decision to validate or reject the certificate request:

- In case of rejection : The RA informs the holder, and the certification agent if applicable,
- In case of validation: The RA triggers the certificate issuance process.

4. Certificate issuance

The holder certificate and associated private key are generated by the CA, and stored in a software container protected by a password. This container is made available to the holder on the User Portal for a one-time access.
The use of the private key is protected by entering "activation data" (password). Activation data is only available for holder after authentication on the User Portal.

5. Certificate acceptance by the holder

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 holder explicitly refuses the certificate, the certificate is revoked by the CA.

7.2 Encryption certificates for an application service (entity and machine type)

1. Preparation and presentation of the certificate application

For any application for an encryption certificate for an application service, the future CM:

- Must be a Banque de France employee or contractor,
- Must have a user account in the Banque de France identity and access management system.

The certificate request does not require a registration file for an application service certificate.
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 CM is also informed about private key escrow conditions.

2. Verification of the certificate application

The RA controls the completeness of the electronic request.

3. Decision to validate or reject the certificate request

After verification of the completeness of the certificate request, the RA takes the decision to validate or reject the certificate request:

- In case of rejection : The RA informs the CM,
- In case of validation: The RA triggers the certificate issuance process.

4. Certificate issuance

The application service certificate and associated private keys are generated and stored in a software container protected by a password. This container is made available to the CM on the User Portal for a one-time access.
The use of the private key is protected by entering "activation data" (password). Activation data is only available for CM after authentication on the User Portal.

5. Certificate acceptance by the CM

For an application service certificate, 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 an application service 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.

7.3 Registering a new CM for an application service certificate already issued

A change of the CM for an application service certificate already issued is not authorized without certificate revocation.
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.

8. New certificate request procedure

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 is at the initiative of the holder / CM or of the Certification Agent if applicable.
The procedure for processing a request for a new certificate is identical to the procedure for an initial request.
Note: The generation of a new key pair is systematic for any certificate issuance.

9. Revocation procedure

A request for a revocation can be submitted by:

- For a holder certificate :
  - the holder in whose name the certificate was issued,
  - a Certification Agent of the holder's entity,
  - legal representative of the holder's organization,
  - the CA that issued the certificate,
  - the RA attached to the CA.
- For an application service certificate :
  - 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 revocation request may be submitted:

- Online, after authentication to the User Portal, using the following address : https://igcv3.certificats.banque-france.fr ,
- By email on the following email address : 1206-r4f-ut@banque-france.fr,
- By mail to the following address :

Banque de France
39 rue croix des petits champs
26-1206 Cellule R4F
75001 Paris

If the request is admissible, the certificate is revoked by the RA within 24 hours maximum.
In all cases, except for a revocation made online by the holder/CM, the revocation is made by the RA, which thus validates the request.
The requestor, 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.

10. Limitation of responsabilities

Certificates issued by "**Banque de France AC v3 Chiffrement"** for holders (natural persons) should only be used for encryption purposes.

Certificates issued by "**Banque de France AC v3 Chiffrement**" for application services should only be used for encryption purposes.
Certificates are issued with a validity period of :

- 3 years for holders certificates,
- 3 years for application services certificates.

The "**Banque de France AC v3 Chiffrement**" CA archive data, with accordance to retention period detailed in the associated CP, in particular:

- 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. Event logs are kept for ten years at least from their generation date. When due, the event logs are destroyed.
- Certificate registration files and supported documents are archived for a period of ten years from the date of acceptance of the certificate by the holder/CM. When due, the registration files are destroyed.
- Certificates and CRL issued by the CA are archived for a period of ten years from their generation. When due, certificates and CRL are destroyed.
- OCSP responses are kept for a period of for three months at least from their expiration date. When due, the OCSP responses are destroyed.

11. Obligations of certificate holders/CM

Certificate holders/CM have the following obligations:

- 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 application service private key and corresponding certificates;
- inform the CA of any change to the information contained in certificates;
- promptly request revocation of a certificate if the private key or activation data are compromised or suspected of being compromised.

12. Certificate status checking obligations of certificate users

Certificate users have the following obligations:

- comply with the use for which a certificate was issued;
- verify that the certificate is issued by "**Banque de France AC v3 Chiffrement**" CA;
- verify that the certificate is not present in the certificate revocation list of the "**Banque de France AC v3 Chiffrement**" CA;
- 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);

The certificates of the certification chain are available at the following address: http://pc.igcv3.certificats.banque-france.fr.
The Certificate Revocation List issued by "**Banque de France AC v3 Chiffrement"** is available on following addresses:

- http://crl.igcv3.certificats.banque-france.fr/chiffrement-1.2.250.1.115.200.3.4.1.3.1.crl
- http://crl.igcv3.certificats.banque-france.org/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

Revoked certificates remain present in the CRL even after their expiry date.

Banque de France provides users with an online system to check certificate status (OCSP). The OCSP responder is available on following addresses:

- http://ocsp.igcv3.certificats.banque-france.fr/chiffrement-1.2.250.1.115.200.3.5.1.3.1
- http://ocsp.igcv3.certificats.banque-france.org/chiffrement-1.2.250.1.115.200.3.5.1.3.1

The certificate status information function is available 24/7. The maximum downtime per service stoppage of this function is 4h, and the total maximum downtime per month is 8h. The maximum time taken to respond to an OCSP query is 6 seconds.

13. Limitation of liability

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.

14. Referenced documents

The Certification Policy of « **Banque de France AC v3 Chiffrement** » is available on the following address: http://pc.igcv3.certificats.banque-france.fr.

15. 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.

16. Refund policy

No stipulation.

17. Applicable law, complaints and dispute resolution

Current terms and conditions, and the Certification Policy of « **Banque de France AC v3 Chiffrement** » CA are subject to laws and regulations in force in France.
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.

18. Applicable audits and references

The certificates issued by the « **Banque de France AC v3 Chiffrement** » CA and the associated Certification Policy, are structured according to the requirements of ETSI EN 319 411-1 standard relating to the certification authorities issuing certificates.
A conformity assessment is conducted at the request of the CAPC to check compliancy between the Certification Policy, and the Certification Practice Statements.
The CA is engaged to conduct such assessment every year, and typically, after a PKI component is first brought into service or substantially changed.

Certificate Holder / CM Signature
Date: First Name : Last Name : Signature :