



Information security

Certificate profiles, OCSP, CRL and ARL
Trust chain of the Banque de France PKI
Production environment

Date : August 18, 2020
Author : RSI
Classification : Public

Version : 1.1
Number of pages : 54

List of versions

Version	Date	Author	Modification
1.0	16/06/2020	RT - RSI	Initial version
1.1	18/08/2020	RT - RSI	Minor updates

Document validation

Validated by the Certification Policy Approval Committee of the Banque de France.

Reference documents

Document	Version	OID
Certification Policy « Banque de France AC v3 Racine » Certification Authority	1.0	1.2.250.1.115.200.3.1.1.1.1
Certification Policy « Banque de France AC v3 ID » Certification Authority	1.0	1.2.250.1.115.200.3.1.1.2.1
Certification Policy « Banque de France AC v3 ID Forte » Certification Authority	1.0	1.2.250.1.115.200.3.1.1.4.1
Certification Policy « Banque de France AC v3 Chiffrement » Certification Authority	1.0	1.2.250.1.115.200.3.1.1.3.1

Table of contents

List of versions.....	2
Document validation	2
Reference documents	2
Table of contents.....	3
1 Introduction.....	5
2 Certificate profiles	5
2.1 Certificate profiles of Certificate Authorities	5
2.1.1 The root Certificate Authority of the Banque de France PKI.....	5
2.1.2 Banque de France AC v3 ID	6
2.1.3 Banque de France AC v3 Chiffrement	8
2.1.4 Banque de France AC v3 ID Forte.....	9
2.2 Certificate profiles issued by the CA Banque de France AC v3 ID	12
2.2.1 Certificate profile related to a natural person	12
2.2.1.1 Authentification et Signature Personne	12
2.2.1.2 Authentification Spécifique Personne POBI (A2A)	14
2.2.1.3 Authentification Spécifique Personne SOFACT	15
2.2.1.4 Authentification Spécifique Personne TEFACT.....	17
2.2.2 Certificate profile related to an Entity application service.....	18
2.2.2.1 Authentification et Signature Entité.....	18
2.2.2.2 Signature Entité	20
2.2.3 Certificate profiles related to a machine-type application service	22
2.2.3.1 Authentification Machine Client et Serveur SSL.....	22
2.2.3.2 Authentification Machine Client	24
2.2.3.3 Signature Machine.....	26
2.2.3.4 Authentification Forte Machine (DC)	28
2.3 Certificate profiles issued by the CA Banque de France AC v3 ID Forte.....	31
2.3.1 Certificate profiles related to a natural person.....	31
2.3.1.1 Authentification Forte Personne	31
2.3.1.2 Authentification Forte Personne TELMA.....	33
2.3.1.3 Authentification Forte Spécifique POBI (U2A)	34
2.3.1.4 Authentification Forte Spécifique 3CB-4CB.....	36
2.3.1.5 Signature Forte Personne	38
2.3.2 Certificate profiles related to an entity-type application service	39
2.3.2.1 Authentification Forte Entité.....	39
2.3.2.2 Signature Forte Entité	41

2.3.3	Certificate profiles related to a machine-type application service	43
2.3.3.1	Authentication Forte Machine	43
2.4	Certificate profiles issued by the CA Banque de France AC v3 Chiffrement.	45
2.4.1	Certificate profiles related to a natural person.....	46
2.4.1.1	Chiffrement Personne	46
2.4.2	Certificate profile related to an Entity-type application service	47
2.4.2.1	Chiffrement Entité	47
2.4.3	Certificate profile related to a machine	49
2.4.3.1	Chiffrement Machine	49
3	CRL and ARL profiles.....	52
3.1	CRL and ARL fields	52
3.2	CRL and ARL extensions.....	52
4	Online Certificate Status Protocol (OCSP)	53
4.1	Common fields for OCSP signature certificate	53
4.2	OCSP certificates profiles	54

1 Introduction

This document presents the profiles of certificate profiles issued by the Certification Authorities of The Banque de France PKI (Production environment) according to security levels and uses. It also presents the OCSP and CRL/ARL profiles.

The following diagram describes the hierarchy of Certificate Authorities for the production environment.



2 Certificate profiles

2.1 Certificate profiles of Certificate Authorities

2.1.1 The root Certificate Authority of the Banque de France PKI

Certificate of the root Certificate Authority of the Banque de France PKI

This CA is a self-signed CA issuing certificates exclusively to Banque de France Certificate Authorities called :

- Intermediate CAs: CA issuing certificates for Issuing CAs
- Issuing CAs: CA issuing certificates for end-entities (Natural persons, legal entities, application services)

The *OrganizationIdentifier* field (2.5.4.97) uses the ANSSI nomenclature (**NTRFR**) followed by the Banque de France SIREN number: **NTRFR-572104891**

The *OrganizationUnitName* field uses the RGSv2 requirements by specifying the ICD identifier for France (0002) followed by the Banque de France SIREN number: **0002 572104891**

The value of these two fields is the same for the Root CA as well as the Intermediate / Issuing CAs.

Column "C" indicates whether the field is critical (Y) or not (N).

Banque de France AC v3 Racine		
<i>Fiel</i>	<i>C</i>	<i>Value</i>
Version		V3
SerialNumber		Issued by the CA
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Issued by the CA
Validity		20 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 20 years
SubjectPublicKeyInfo		The public key with a length of 4096 bits (RSA)
Issuer		
OrganizationIdentifier		NTRFR-572104891
CommonName		Banque de France AC v3 Racine
OrganizationUnitName		0002 572104891

Banque de France AC v3 Racine		
OrganisationName		Banque de France
CountryName		FR
Subject		
OrganizationIdentifier		NTRFR-572104891
CommonName		Banque de France AC v3 Racine
OrganizationUnitName		0002 572104891
OrganizationName		Banque de France
CountryName		FR
Extensions		
KeyUsage	Y	
keyCertSign		Set
crlSigning		Set
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the CA "Banque de France AC v3 Racine" Public Key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the CA "Banque de France AC v3 Racine" Public Key
BasicConstraints	Y	
CA		True
pathLenConstraint		None

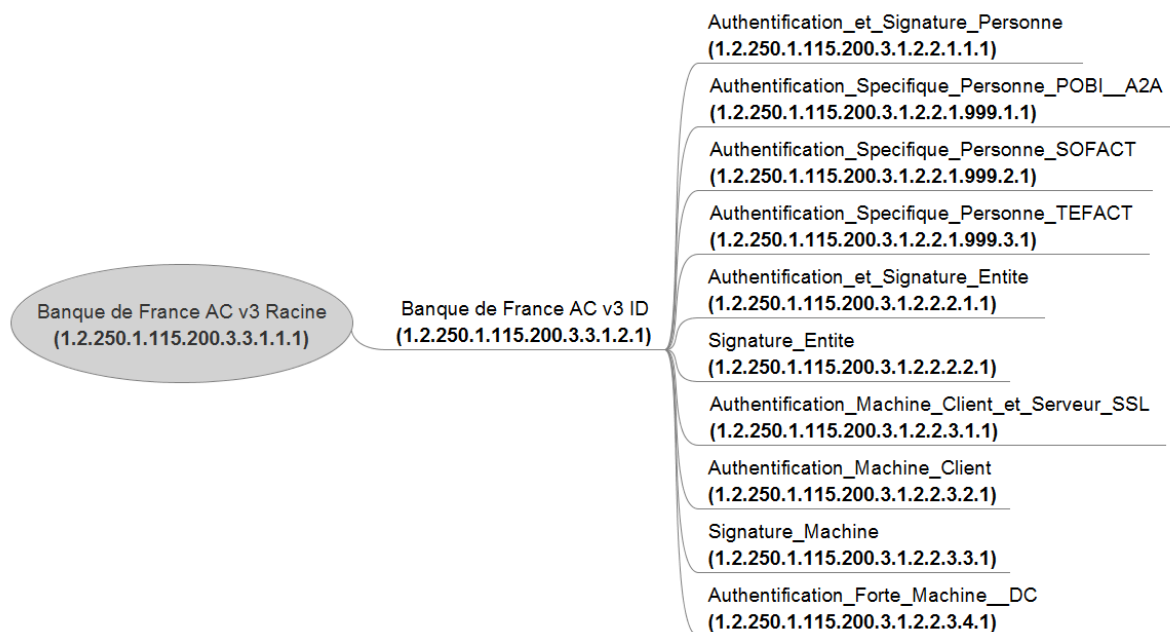
2.1.2 Banque de France AC v3 ID

Certificate Authority issuing Authentication and Signature software Certificates. It is signed by the root CA "Banque de France AC v3 Racine".

Banque de France AC v3 ID		
Field	C	Value
Version		V3
SerialNumber		Issued by the CA
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Issued by the CA
Validity		20 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 20 years
SubjectPublicKeyInfo		The public key with a length of 4096 bits (RSA)
Issuer		
OrganizationIdentifier		NTRFR-572104891
CommonName		Banque de France AC v3 Racine
OrganizationUnitName		0002 572104891
OrganisationName		Banque de France
CountryName		FR
Subject		
OrganizationIdentifier		NTRFR-572104891
CommonName		Banque de France AC v3 ID
OrganizationUnitName		0002 572104891
OrganizationName		Banque de France
CountryName		FR
Extensions		

Banque de France AC v3 ID		
KeyUsage	Y	
keyCertSign		Set
crlSigning		Set
Certificate Policies	N	
PolicyIdentifier		2.5.29.32.0 (anyPolicy)
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	• 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
Authority Information Access	N	AIA OCSP • http://ocsp.igcv3.certificats.banque-france.fr/racine-1.2.250.1.115.200.3.5.1.1.1 • http://ocsp.igcv3.certificats.banque-france.org/racine-1.2.250.1.115.200.3.5.1.1.1 AIA calssuer • http://cert.igcv3.certificats.banque-france.fr/racine-1.2.250.1.115.200.3.3.1.1.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the “Banque de France AC v3 Racine” CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the “Banque de France AC v3 ID” CA public key
BasicConstraints	Y	
CA		True
pathLenConstraint		0

Below is a diagram that describes the certificate profiles issued by this CA.



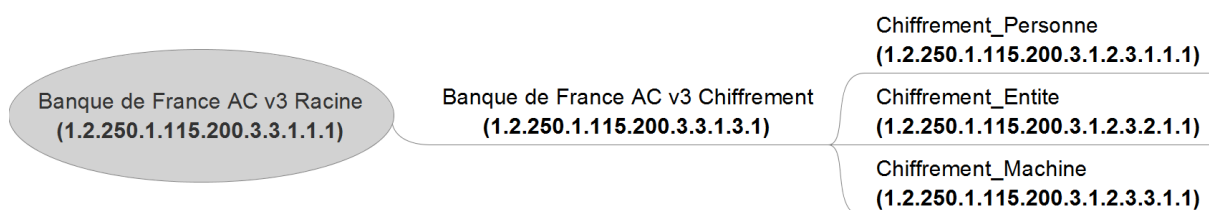
2.1.3 Banque de France AC v3 Chiffrement

Certificate Authority issuing encryption software certificates. It is signed by the root CA Banque de France AC v3 Racine.

Banque de France AC v3 Chiffrement		
Field	C	Value
Version		V3
SerialNumber		Issued by the CA
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Issued by the CA
Validity		20 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 20 years
SubjectPublicKeyInfo		The public key with a length of 4096 bits (RSA)
Issuer		
OrganizationIdentifier		NTRFR-572104891
CommonName		Banque de France AC v3 Racine
OrganizationUnitName		0002 572104891
OrganisationName		Banque de France
CountryName		FR
Subject		
OrganizationIdentifier		NTRFR-572104891
CommonName		Banque de France AC v3 Chiffrement
OrganizationUnitName		0002 572104891
OrganizationName		Banque de France
CountryName		FR
Extensions		
KeyUsage	Y	
keyCertSign		Set
crlSigning		Set
Certificate Policies	N	

Banque de France AC v3 Chiffrement		
PolicyIdentifier		2.5.29.32.0 (anyPolicy)
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	• 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
Authority Information Access	N	AIA OCSP • http://ocsp.igcv3.certificats.banque-france.fr/racine-1.2.250.1.115.200.3.5.1.1.1 • http://ocsp.igcv3.certificats.banque-france.org/racine-1.2.250.1.115.200.3.5.1.1.1 AIA calssuer • http://cert.igcv3.certificats.banque-france.fr/racine-1.2.250.1.115.200.3.3.1.1.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the “Banque de France AC v3 Racine” CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the “Banque de France AC v3 Chiffrement” CA public key
BasicConstraints	Y	
CA		True
pathLenConstraint		0

Below is a diagram that describes the certificate profiles issued by this CA.



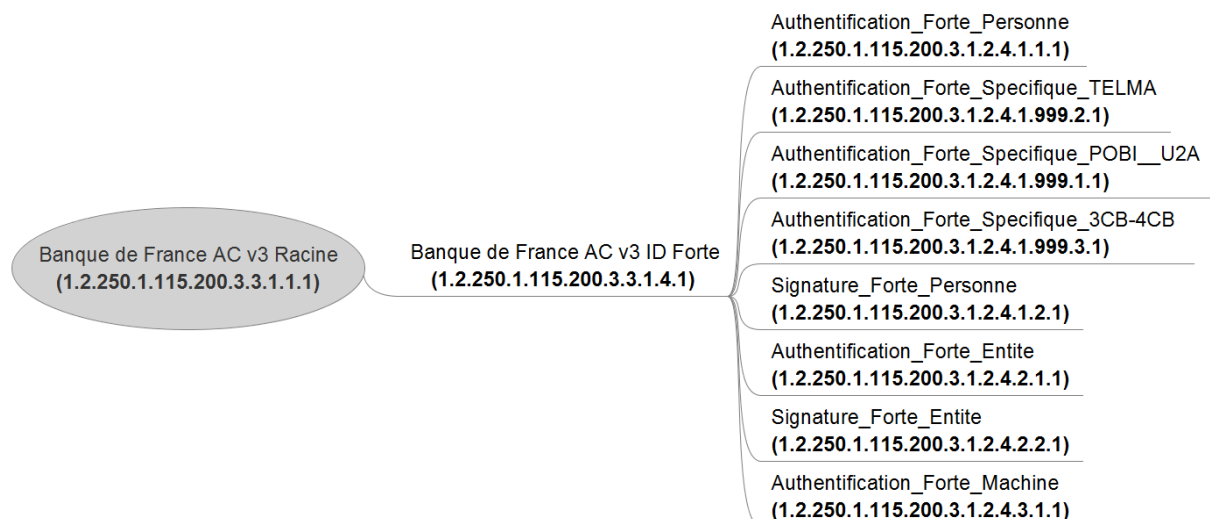
2.1.4 Banque de France AC v3 ID Forte

Certificate Authority issuing hardware Authentication or Signature Certificates. It is signed by the root CA “Banque de France AC v3 Racine”.

Banque de France AC v3 ID Forte		
Field	C	Value
Version		V3
SerialNumber		Issued by the CA
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Issued by the CA
Validity		20 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 20 years
SubjectPublicKeyInfo		The public key with a length of 4096 bits (RSA)
Issuer		
OrganizationIdentifier		NTRFR-572104891
CommonName		Banque de France AC v3 Racine
OrganizationUnitName		0002 572104891
OrganisationName		Banque de France
CountryName		FR
Subject		
OrganizationIdentifier		NTRFR-572104891
CommonName		Banque de France AC v3 ID Forte
OrganizationUnitName		0002 572104891
OrganizationName		Banque de France
CountryName		FR
Extensions		
KeyUsage	Y	
keyCertSign		Set
crlSigning		Set
Certificate Policies	N	
PolicyIdentifier		2.5.29.32.0 (anyPolicy)
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	- 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
Authority Information Access	N	AIA OCSP

Banque de France AC v3 ID Forte		
		• http://ocsp.igcv3.certificats.banque-france.fr/racine-1.2.250.1.115.200.3.5.1.1.1 • http://ocsp.igcv3.certificats.banque-france.org/racine-1.2.250.1.115.200.3.5.1.1.1 AIA calssuer • http://cert.igcv3.certificats.banque-france.fr/racine-1.2.250.1.115.200.3.3.1.1.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the “Banque de France AC v3 Racine” CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the “Banque de France AC v3 ID Forte” CA public key
BasicConstraints	Y	
CA		True
pathLenConstraint		0

Below is a diagram that describes the certificate profiles of this CA.



2.2 Certificate profiles issued by the CA Banque de France AC v3 ID

This chapter describes all certificate profiles issued by the CA Banque de France AC v3 ID

This chapter is divided into 3 sub-sections:

- Certificate profiles related to a natural person;
- Certificate profiles related to an Entity-type application service;
- Certificate profiles related to a Machine-type application service.

2.2.1 Certificate profile related to a natural person

2.2.1.1 Authentication et Signature Personne

Authentication and signature software certificate.

LCP		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4
		In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
serialNumber		Complementary element to distinguish homonyms: SHA-1 hash value of the holder's unique number within the PKI
commonName		The full name of the holder as it should be displayed by applications. The holder's first name in use, followed by a space, followed by the holder's last name in use.
organizationUnitName		In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - the ICD is on 4 characters; (0002 for France) - organization identification on 35 characters - the separator between the two chains is a space. If the ICD number is equal to 0002, it should be followed by a SIREN or SIRET number since it refers to an organisation registered in France
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities

countryName		Requester's country of residence
Validity		3 years
NotBefore		Date of bi-key generation
NotAfter		Date of bi-key generation + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	nonRepudiation, digitalSignature
ExtendedKeyUsage	N	emailProtection (1.3.6.1.5.5.7.3.4), clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.2.1.1.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP 1		http://crl.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP 2		http://crl.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP 3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID,O=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP 4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.5.1.2.1
		http://ocsp.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.5.1.2.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.3.1.2.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash of the Issuing CA public key (Banque de France AC v3 ID)
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	
otherName (UPN)		Holder's identifier 'User Principal Name'

rfc822Name		Holder's email address
------------	--	------------------------

2.2.1.2 Authentification Spécifique Personne POBI (A2A)

Authentication software certificate, with specific fields used by a Banque de France specific application of the Banque de France

LCP		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		The full name of the holder as it should be displayed by applications : Account number in the application
organizationUnitName		Identification of the entity to which the holder belongs
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence
Validity		3 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	DigitalSignature, KeyEncipherment, KeyAgreement
ExtendedKeyUsage	N	clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.2.1.999.1.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.4.1.2.1.crl

CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.5.1.2.1 http://ocsp.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.5.1.2.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.3.1.2.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash of the Issuing CA public key (Banque de France AC v3 ID)
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	
otherName (UPN)		Holder's identifier 'User Principal Name'
rfc822Name		Holder's email address

2.2.1.3 Authentification Spécifique Personne SOFACT

Authentication software certificate, with specific fields used by a specific Banque de France application.

LCP		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR

Subject		
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		The full name of the holder as it should be displayed by applications : Account number in the application
organizationUnitName		Identification of the entity to which the holder belongs
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence
Validity		3 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	DigitalSignature, KeyEncipherment, KeyAgreement
ExtendedKeyUsage	N	clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.2.1.999.2.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID, OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID, OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.5.1.2.1
		http://ocsp.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.5.1.2.1

AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.3.1.2.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key (Banque de France AC v3 ID)
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	
otherName (UPN)		Holder's identifier 'User Principal Name'
rfc822Name		Holder's email address

2.2.1.4 Authentification Spécifique Personne TEFACT

Authentication software certificate, with specific fields used by a specific Banque de France application

LCP		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
serialNumber		Account number in the application
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Account number in the application
organizationUnitName		Identification of the entity to which the holder belongs
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence
Validity		3 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
PublicKeyAlgorithm		rsaEncryption

SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	DigitalSignature, KeyEncipherment, KeyAgreement
ExtendedKeyUsage	N	clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.2.1.999.3.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NT RFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NT RFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.5.1.2.1 http://ocsp.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.5.1.2.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.3.1.2.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key (Banque de France AC v3 ID)
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	
otherName (UPN)		Holder's identifier 'User Principal Name'
rfc822Name		Holder's email address

2.2.2 Certificate profile related to an Entity application service

2.2.2.1 Authentication et Signature Entité

Authentication and signature software certificate for an entity.

LCP		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		DN of the Issuing CA
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Significant name of the service implementing the certificate for an Entity.
organizationUnitName2		Entity name
organizationUnitName		In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - the ICD is on 4 characters; (0002 for France) - organization identification on 35 characters - the separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France.
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Country where the entity responsible for the certificate is registered
Validity		3 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	NonRepudiation, digitalSignature
ExtendedKeyUsage	N	emailProtection (1.3.6.1.5.5.7.3.4), clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	N	

PolicyIdentifier		1.2.250.1.115.200.3.1.2.2.1.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.5.1.2.1
		http://ocsp.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.5.1.2.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.3.1.2.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	
otherName (UPN)		Entity's identifier 'User Principal Name'
rfc822Name		Entity's email address

2.2.2.2 Signature Entité

Software signature certificate for an entity.

LCP		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)

Issuer		DN of the Issuing CA
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Significant name of the service implementing the certificate for Entity
organizationUnitName2		Entity's name
organizationUnitName		In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - the ICD is on 4 characters; (0002 for France) - organization identification on 35 characters - the separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Country where the entity responsible for the certificate is registered
Validity		3 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	nonRepudiation
ExtendedKeyUsage	N	emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.2.2.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.4.1.2.1.crl

CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.5.1.2.1 http://ocsp.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.5.1.2.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.3.1.2.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	
otherName (UPN)		Entity's identifier 'User Principal Name'
rfc822Name		Entity's email address

2.2.3 Certificate profiles related to a machine-type application service

2.2.3.1 Authentication Machine Client et Serveur SSL

Server SSL Authentication certificate.

DVCP		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		DN of the Issuing CA
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR

Subject		
organizationIdentifier		This field is mandatory if the requester is a legal entity, optional otherwise. Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Machine / Server common name
organizationUnitName2		Name of the application linked to the certificate
organizationUnitName		This field is mandatory if the requester is a legal entity, optional otherwise. In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - the ICD is on 4 characters; (0002 for France) - organization identification on 35 characters - the separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France.
organizationName		This field is mandatory if the requester is a legal entity, optional otherwise. Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence or country where the requester's is established
Validity		3 years
NotBefore		Date of certificate issuance
NotAfter		Date of certificate issuance + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	digitalSignature, keyEncipherment, keyAgreement
ExtendedKeyUsage	N	serverAuth (1.3.6.1.5.5.7.3.1) , clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.2.3.1.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.4.1.2.1.crl

CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NT RFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NT RFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.5.1.2.1
		http://ocsp.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.5.1.2.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.3.1.2.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key (Banque de France AC v3 ID)
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name (SAN)	N	
otherName (UPN)		(Optional) The server FQDN
dnsName		One or more domain names managed by the person in charge of the certificate. This field is mandatory
iPAddress		(Optional) One or more IP addresses managed by the person in charge of the certificate.

2.2.3.2 Authentication Machine Client

Client SSL Authentication certificate.

DVCP		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		DN of the Issuing CA
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France

countryName		FR
Subject		
organizationIdentifier		This field is mandatory if the requester is a legal entity, optional otherwise. Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Machine / Server common name
organizationUnitName2		Name of the application linked to the certificate
organizationUnitName		This field is mandatory if the requester is a legal entity, optional otherwise. In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - the ICD is on 4 characters; (0002 for France) - organization identification on 35 characters - the separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France.
organizationName		This field is mandatory if the requester is a legal entity, optional otherwise. Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence or country where the requester's is established
Validity		3 years
NotBefore		Date of certificate issuance
NotAfter		Date of certificate issuance + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	digitalSignature
ExtendedKeyUsage	N	clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.2.3.2.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.4.1.2.1.crl

CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID,O=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.5.1.2.1
		http://ocsp.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.5.1.2.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.3.1.2.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name (SAN)	N	
otherName (UPN)		(Optional) The machine/ server FQDN
rfc822Name		(Optional) Main email address
rfc822Name		(Optional) Secondary email address

2.2.3.3 Signature Machine

Signature certificate for a machine.

Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		DN of the Issuing CA
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		

organizationIdentifier		This field is mandatory if the requester is a legal entity, optional otherwise. Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Machine / Server common name
organizationUnitName2		Name of the application linked to the certificate
organizationUnitName		This field is mandatory if the requester is a legal entity, optional otherwise. In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - the ICD is on 4 characters; (0002 for France) - organization identification on 35 characters - the separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France.
organizationName		This field is mandatory if the requester is a legal entity, optional otherwise. Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence or country where the requester's is established
Validity		3 years
NotBefore		Date of certificate issuance
NotAfter		Date of certificate issuance + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	nonRepudiation, digitalSignature
ExtendedKeyUsage	N	emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.2.3.3.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.4.1.2.1.crl

CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.5.1.2.1
		http://ocsp.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.5.1.2.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.3.1.2.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name (SAN)	N	
otherName (UPN)		(Optional) The machine/ server FQDN
rfc822Name		(Optional) Main email address
rfc822Name		(Optional) Secondary email address

2.2.3.4 Authentication Forte Machine (DC)

Strong Authentication for Domain Controller.

DVCP		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		DN of the Issuing CA
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		

organizationIdentifier		This field is mandatory if the requester is a legal entity, optional otherwise. Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Machine / Server common name
organizationUnitName2		Name of the application linked to the certificate
organizationUnitName		This field is mandatory if the requester is a legal entity, optional otherwise. In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - the ICD is on 4 characters; (0002 for France) - organization identification on 35 characters - the separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France.
organizationName		This field is mandatory if the requester is a legal entity, optional otherwise. Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence or country where the requester's is established
Validity		3 years
NotBefore		Date of certificate issuance
NotAfter		Date of certificate issuance + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	digitalSignature, keyEncipherment, keyAgreement
ExtendedKeyUsage	N	serverAuth (1.3.6.1.5.5.7.3.1) , clientAuth (1.3.6.1.5.5.7.3.2) , KDCAuth (1.3.6.1.5.2.3.5), SmartCardLogon (1.3.6.1.4.1.311.20.2.2)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.2.3.4.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.4.1.2.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.4.1.2.1.crl

CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NT RFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID,OU=0002%20572104891,O=Banque%20de%20France,OI=NT RFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.5.1.2.1
		http://ocsp.igcv3.certificats.banque-france.org/id-1.2.250.1.115.200.3.5.1.2.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-1.2.250.1.115.200.3.3.1.2.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name (SAN)	N	
otherName (UPN)		(Optional) The machine/ server FQDN
dNSName		One or more domain names managed by the person in charge of the certificate. This field is mandatory
iPAddress		(Optional) One or more IP addresses managed by the person in charge of the certificate.

2.3 Certificate profiles issued by the CA Banque de France AC v3 ID Forte.

This chapter describes all certificate profiles issued by the CA Banque de France AC v3 ID Forte.

This chapter is divided into 3 sub-sections:

- Certificate profiles related to a natural person,
- Certificate profiles related to an Entity-type application service,
- Certificate profiles related to an Machine-type application service.

2.3.1 Certificate profiles related to a natural person.

2.3.1.1 Authentication Forte Personne

Hardware certificate for authentication. These certificates are presented on a cryptographic module (NCP+).

NCP+		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID Forte
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
serialNumber		Complementary element to distinguish homonyms: SHA-1 hash value of the holder's unique number within the PKI
organizationUnitName		In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - the ICD is on 4 characters; (0002 for France) - organization identification on 35 characters - the separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France.
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
commonName		Full name of the holder as it should be displayed by applications. The holder's first name in use, followed by a

		space, followed by the holder's civil name or last name in use.
countryName		Requester's country of residence
Validity		3 years
NotBefore		Date of bi-key generation
NotAfter		Date of bi-key generation + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	digitalSignature
ExtendedKeyUsage	N	clientAuth (1.3.6.1.5.5.7.3.2) , SmartCardLogon (1.3.6.1.4.1.311.20.2.2)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.4.1.1.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.5.1.4.1 http://ocsp.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.5.1.4.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.3.1.4.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key (Banque de France AC v3 ID Forte)
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	

otherName (UPN)		Holder's identifier 'User Principal Name'
rfc822Name		Holder's email address

2.3.1.2 Authentication Forte Personne TELMA

Strong authentication with specific fields for a specific Banque de France application. These certificates are presented on a cryptographic module (NCP+).

NCP+		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID Forte
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Full name of the holder as it should be displayed by applications: Account number in the application
organizationUnitName		Identification of the entity to which the holder belongs
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence
Validity		3 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	DigitalSignature, KeyEncipherment, KeyAgreement
ExtendedKeyUsage	N	clientAuth (1.3.6.1.5.5.7.3.2) , SmartCardLogon (1.3.6.1.4.1.311.20.2.2)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.4.1.999.2.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL

CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.5.1.4.1
		http://ocsp.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.5.1.4.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.3.1.4.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key (Banque de France AC v3 ID Forte)
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	
otherName (UPN)		Holder's identifier 'User Principal Name'
rfc822Name		Holder's email address

2.3.1.3 Authentication Forte Spécifique POBI (U2A)

Strong authentication with specific fields for a specific Banque de France application. These certificates are presented on a cryptographic module (NCP+).

NCP+		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID Forte
organizationUnitName		0002 572104891

organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Full name of the holder as it should be displayed by applications : Account number in the application
organizationUnitName		Identification of the entity to which the holder belongs
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence
Validity		3 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	DigitalSignature, KeyEncipherment, KeyAgreement
ExtendedKeyUsage	N	clientAuth (1.3.6.1.5.5.7.3.2) , SmartCardLogon (1.3.6.1.4.1.311.20.2.2)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.4.1.999.1.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.5.1.4.1

		http://ocsp.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.5.1.4.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.3.1.4.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key (Banque de France AC v3 ID Forte)
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	
otherName (UPN)		Holder's identifier 'User Principal Name'
rfc822Name		Holder's email address

2.3.1.4 Authentification Forte Spécifique 3CB-4CB

Strong authentication with specific fields for a specific Banque de France application. These certificates are presented on a cryptographic module (NCP+).

These certificates are for internal use only.

NCP+		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID Forte
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
E (Email)		Internal fixed email address at The Banque de France
serialNumber		Complementary element to distinguish homonyms: SHA-1 hash value of the holder's unique number within the PKI
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix "NTRFR-" followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		The full name of the holder as it should be displayed by applications. The holder's first name in use, followed by a space, followed by the holder's civil name or last name in use.
organizationUnitName		Identification of the entity to which the holder belongs

organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence
Validity		3 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	DigitalSignature, KeyEncipherment, KeyAgreement
ExtendedKeyUsage	N	clientAuth (1.3.6.1.5.5.7.3.2) , SmartCardLogon (1.3.6.1.4.1.311.20.2.2)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.4.1.999.3.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.5.1.4.1
		http://ocsp.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.5.1.4.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.3.1.4.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key (Banque de France AC v3 ID Forte)
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	

otherName (UPN)	Holder's identifier 'User Principal Name'
rfc822Name	Holder's email address

2.3.1.5 *Signature Forte Personne*

Signature certificate on material support. These certificates are presented on a cryptographic module (NCP+).

NCP+		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID Forte
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix « NTRFR- » followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
serialNumber		Complementary element to distinguish homonyms: SHA-1 hash value of the holder's unique number within the PKI
commonName		The full name of the holder as it should be displayed by applications. The holder's first name in use, followed by a space, followed by the holder's civil name or last name in use.
organizationUnitName		In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - The ICD is on 4 characters; (0002 for France) - Organization identification on 35 characters - The separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France.
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence
Validity		3 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
PublicKeyAlgorithm		rsaEncryption

SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	nonRepudiation
ExtendedKeyUsage	N	emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.4.1.2.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.5.1.4.1
		http://ocsp.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.5.1.4.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.3.1.4.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key (Banque de France AC v3 ID Forte)
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	
otherName (UPN)		Holder's identifier 'User Principal Name'
rfc822Name		Holder's email address

2.3.2 Certificate profiles related to an entity-type application service

2.3.2.1 Authentication Forte Entité

Hardware authentication certificate for an entity. These certificates are presented on a cryptographic module (PCN+).

NCP+		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		DN of the Issuing CA
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID Forte
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix « NTRFR- » followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Significant name of the service implementing the certificate Entity
organizationUnitName2		Entity's name
organizationUnitName		In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - The ICD is on 4 characters; (0002 for France) - Organization identification on 35 characters - The separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France.
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Country where the entity responsible for the certificate is registered
Validity		3 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	digitalSignature
ExtendedKeyUsage	N	clientAuth (1.3.6.1.5.5.7.3.2), SmartCardLogon (1.3.6.1.4.1.311.20.2.2)

CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.4.2.1.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.5.1.4.1
		http://ocsp.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.5.1.4.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.3.1.4.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	
otherName (UPN)		Entity's identifier 'User Principal Name'
rfc822Name		Entity's email address

2.3.2.2 Signature Forte Entité

Hardware signature certificate for an entity. These certificates are presented on a cryptographic module (NCP+).

NCP+		
Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI

Key Size		2048 bits (RSA)
Issuer		DN of the Issuing CA
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID Forte
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix « NTRFR-» followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Significant name of the service implementing the certificate Entity
organizationUnitName2		Entity's name
organizationUnitName		In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - The ICD is on 4 characters; (0002 for France) - Organization identification on 35 characters - The separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France.
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Country where the entity responsible for the certificate is registered
Validity		3 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	nonRepudiation
ExtendedKeyUsage	N	emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.4.2.2.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL

CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.5.1.4.1 http://ocsp.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.5.1.4.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.3.1.4.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	
otherName (UPN)		Entity's identifier 'User Principal Name'
rfc822Name		Entity's email address

2.3.3 Certificate profiles related to a machine-type application service

2.3.3.1 Authentication Forte Machine

Certificate profiles complying with ETSI EN 319 411-1. These certificates are available on an SSCD cryptographic module.

Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		DN of the Issuing CA
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID Forte
organizationUnitName		0002 572104891

organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		This field is mandatory if the requester is a legal entity, optional otherwise. Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix « NTRFR- » followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Machine / Server common name.
organizationUnitName2		Name of the application linked to the certificate
organizationUnitName		This field is mandatory if the requester is a legal entity, optional otherwise. In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - The ICD is on 4 characters; (0002 for France) - L'identification de l'organisation sur 35 caractères - The separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France.
organizationName		This field is mandatory if the requester is a legal entity, optional otherwise. Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence or country where the requester's is established
Validity		3 years
NotBefore		Date of certificate issuance
NotAfter		Date of certificate issuance + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	digitalSignature
ExtendedKeyUsage	N	clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.4.3.1.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr

CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.4.1.4.1.crl
CRLDP3		ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
CRLDP4		ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20ID%20Forte,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		http://ocsp.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.5.1.4.1
		http://ocsp.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.5.1.4.1
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.3.1.4.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name (SAN)	N	
otherName (UPN)		(Optional) The server FQDN
rfc822Name		(Optional) Main email address
rfc822Name		(Optional) Secondary email address

2.4 Certificate profiles issued by the CA Banque de France AC v3 Chiffrement.

This chapter describes all certificate profiles issued by the CA Banque de France AC v3 Chiffrement.

This chapter is divided into 3 sub-sections:

- Certificate profiles related to a natural person,
- Certificate profiles related to an entity-type application service,
- Certificate profiles related to an machine-type application service.

2.4.1 Certificate profiles related to a natural person.

2.4.1.1 Chiffrement Personne

Encryption software certificate (keys should be escrowed).

Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 Chiffrement
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix « NTRFR- » followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
serialNumber		Complementary element to distinguish homonyms: SHA-1 hash value of the holder's unique number within the PKI
commonName		The full name of the holder as it should be displayed by applications. The holder's first name in use, followed by a space, followed by the holder's civil name or last name in use.
organizationUnitName		In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - The ICD is on 4 characters; (0002 for France) - Organization identification on 35 characters - The separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France.
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence
Validity		3 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	O	keyEncipherment

ExtendedKeyUsage	N	emailProtection (1.3.6.1.5.5.7.3.4), EncryptingFileSystem (1.3.6.1.4.1.311.10.3.4)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.3.1.1.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/chiffrement-1.2.250.1.115.200.3.4.1.3.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/chiffrement-1.2.250.1.115.200.3.4.1.3.1.crl
CRLDP3		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
CRLDP4		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
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		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
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/chiffrement-1.2.250.1.115.200.3.3.1.3.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key (Banque de France AC v3 Chiffrement)
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	
otherName (UPN)		Holder's email address
rfc822Name		Holder's email address

2.4.2 Certificate profile related to an Entity-type application service

2.4.2.1 Chiffrement Entité

Encryption software certificate (keys must be escrowed).

Field	C	Value
Version		2=(version 3)

SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		DN of the Issuing CA
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 Chiffrement
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix « NTRFR- » followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Significant name of the service implementing the certificate Entity
organizationUnitName2		Entity's name
organizationUnitName		In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - The ICD is on 4 characters; (0002 for France), - Organization identification on 35 characters, - The separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France.
organizationName		Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Country where the entity responsible for the certificate is registered
Validity		3 years
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	keyEncipherment
ExtendedKeyUsage	N	emailProtection (1.3.6.1.5.5.7.3.4), EncryptingFileSystem (1.3.6.1.4.1.311.10.3.4)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.3.2.1.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr

CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/chiffrement-1.2.250.1.115.200.3.4.1.3.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/chiffrement-1.2.250.1.115.200.3.4.1.3.1.crl
CRLDP3		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
CRLDP4		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
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		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
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/chiffrement-1.2.250.1.115.200.3.3.1.3.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FALSE
Subject Alternative Name	N	
otherName (UPN)		Entity's identifier 'User Principal Name'
rfc822Name		Entity's email address

2.4.3 Certificate profile related to a machine

2.4.3.1 Chiffrement Machine

Encryption certificate for a machine. (Keys must be escrowed)

Field	C	Value
Version		2=(version 3)
SerialNumber		Unique for each certificate issued by the PKI
Key Size		2048 bits (RSA)
Issuer		DN of the Issuing CA
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 Chiffrement
organizationUnitName		0002 572104891

organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		This field is mandatory if the requester is a legal entity, optional otherwise. Official registration number of the entity to which the holder belongs, in accordance with [EN_319_412-1] section 5.1.4. In France, this registration number may also be composed of the prefix « NTRFR- » followed by the SIREN or SIRET number. This prefix is adapted to the country in which the organisation is based.
commonName		Machine / Server common name.
organizationUnitName2		Application name linked to the certificate
organizationUnitName		This field is mandatory if the requester is a legal entity, optional otherwise. In accordance to Annex 2, section VII.1 de [RGS_v2_A4], this field must be present and contain the identification of the entity to which the holder belongs: - The ICD is on 4 characters; (0002 for France) - Organization identification on 35 characters - The separator between the two chains is a space. If the ICD number is equal to 0002, it must necessarily be followed by a SIREN or SIRET number since it refers to an organisation registered in France.
organizationName		This field is mandatory if the requester is a legal entity, optional otherwise. Full official name of the entity to which the holder belongs as registered by the competent authorities
countryName		Requester's country of residence or country where the requester's is established
Validity		3 years
NotBefore		Date of certificate issuance
NotAfter		Date of certificate issuance + 3 years
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	Y	keyEncipherment
ExtendedKeyUsage	N	emailProtection (1.3.6.1.5.5.7.3.4), EncryptingFileSystem (1.3.6.1.4.1.311.10.3.4)
CertificatePolicies	N	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.3.3.1.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr

CRL Distribution Point	N	Distribution URL(s) of the Certificate Authority CRL
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/chiffrement-1.2.250.1.115.200.3.4.1.3.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/chiffrement-1.2.250.1.115.200.3.4.1.3.1.crl
CRLDP3		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
CRLDP4		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
Authority Information Access	N	OCSP service URL(s) of the CA
AIA OCSP		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
AIA CAIssuer		http://cert.igcv3.certificats.banque-france.fr/chiffrement-1.2.250.1.115.200.3.3.1.3.1.cer
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the Issuing CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the public key contained in the certificate
BasicConstraints	N	
CA		FAUX
Subject Alternative Name (SAN)	N	
otherName (UPN)		(Optionnel) the machine / server FQDN
rfc822Name		(Optional) Main email address
rfc822Name		(Optional) Secondary email address

3 CRL and ARL profiles

3.1 CRL and ARL fields

Standard fields	Value
Version	Version 2
Signature	Sha256WithRSAEncryption (2.16.840.1.101.3.4.2.1)
Hash	sha256
Issuer DN	Depending on the issuer of each CA described above
This Update	At the earliest on the start date of the CA validity period
Next Update	Next date on which the CRL will be updated, i.e. 6 days after the generation date of this CRL.
Revoked Certificates	Serial number of revoked certificates
Revocation Date	The date on which a particular certificate was revoked.

3.2 CRL and ARL extensions

Fields	Y	C	Value
Authority Key Identifier	TRUE	FALSE	Key ID = see each CA key described above
CRL Number	TRUE	FALSE	CRL serial number
ExpiredCertsOnCRL	TRUE	FALSE	Date from which expired certificates are kept in the CRL. The Banque de France keeps all expired certificates in the CRL. The fixed date corresponds to one day after the Certification Authority certificate generation: June 29 2019 (20190629000000Z).

4 Online Certificate Status Protocol (OCSP)

Although the additional requirements do not require the installation of an OCSP responder, version 2 of the RGS does. It is also a requirement of the CA/B Forum.

OCSP responses must comply with RFC6960 and/or RFC5019. Thus, there are two possibilities:

1. They must be signed by the CA that issued the certificates whose revocation status is verified, or
2. They must be signed by an OCSP responder whose certificate is signed by the CA that issued the certificate whose revocation status is verified.

In the latter case, the OCSP signing certificate must contain an id-pkix-ocsp-nocheck extension as defined by RFC6960.

The Banque de France PKI implements solution 2, and each OCSP responder therefore has its own certificate, issued by the CA for which the OCSP responder is implemented.

Intermediate/issuing CAs do not sign OCSP responses and therefore do not contain the keyUsage digitalSignature as recommended by the RGS, which follows the CA/B Forum recommendations.

4.1 Common fields for OCSP signature certificate

Each intermediate / Issuing CA has its own OCSP server. The OCSP keys are valid for 3 years.

OCSP certificate		
Field	C	Value
Version		V3
SerialNumber		Issued by the CA
KeySize		2048 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Issued by the CA
Validity		
NotBefore		Date of keys generation
NotAfter		Date of keys generation + 3 years
SubjectPublicKeyInfo		Public key with a length of 2048 bits (RSA)
Issuer		
OrganizationIdentifier		NTRFR-572104891
CommonName		Each Intermediate CA signs the certificate for its own OCSP server/certificate : • Banque de France AC v3 ID • Banque de France AC v3 Chiffrement • Banque de France AC v3 ID Forte
OrganizationUnitName		0002 572104891
OrganizationName		Banque de France
CountryName		FR
Subject		
OrganizationIdentifier		NTRFR-572104891
SERIALNUMBER		SHA-1 hash value of the creation date of OCSP certificate
CommonName		Each Intermediate CA signs the certificate for its own OCSP server/certificate: • OCSP Banque de France AC v3 ID • OCSP Banque de France AC v3 Chiffrement

OCSP certificate		
		OCSP Banque de France AC v3 ID Forte
OrganizationUnitName		0002 572104891
OrganizationName		Banque de France
CountryName		FR
Extensions		
AuthorityKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the CA public key
SubjectKeyIdentifier	N	
KeyIdentifier		SHA-1 hash value of the OCSP certificate public key

4.2 OCSP certificates profiles

Field	C	IGCv3 Intermediate
Certificate Policies	N	
PolicyIdentifier		- Banque de France AC v3 ID 1.2.250.1.115.200.3.5.1.2.1 - Banque de France AC v3 Chiffrement 1.2.250.1.115.200.3.5.1.3.1 - Banque de France AC v3 ID Forte 1.2.250.1.115.200.3.5.1.4.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
Key usage	Y	digitalSignature
Extended Key Usage	N	OCSP Signing with no-check