Sécurité de l'information

Profils des certificats, OCSP, LCR
Chaine de confiance de l'IGC de la Banque de France
Environnement de Production

Date	***:***	17 Août 2023	***Version***	***:***	1.3
Rédacteur	***:***	RSI	***Nombre de pages***	***:***	**54**
Classification	***:***	Public			

Suivi des versions

Version	Date	Rédacteur	Modification
1.0	16/06/2020	RT - RSI	Version Initiale
1.1	18/08/2020	RT - RSI	Mise à jour mineure
1.2	20/02/2022	RT - RSI	Mise à jour : - Profil de certificat Authentification Forte Machine DC - Durée de validité des certificats émis par l'AC « Banque de France AC v3 ID Forte »
1.3	17/08/2023	RSI	Mise à jour mineure

Validation du document

Validé par le Comité d'approbation des politiques de certification de la Banque de France.

Documents de référence

Document	Version	OID
Politique de Certification de l'AC « Banque de France AC v3 Racine »	1.0	**1.2.250.1.115.200.3.1.1.1.1**
Politique de Certification de l'AC « Banque de France AC v3 ID »	1.2	**1.2.250.1.115.200.3.1.1.2.1**
Politique de Certification de l'AC « Banque de France AC v3 ID Forte »	1.2	**1.2.250.1.115.200.3.1.1.4.1**
Politique de Certification de l'AC « Banque de France AC v3 Chiffrement »	1.2	**1.2.250.1.115.200.3.1.1.3.1**

Table des matières

1 Introduction

Ce document présente les différents profils de certificats délivrés par les Autorités de Certification de l'IGC de la Banque de France (Environnement de production) en fonction des niveaux de sécurité et des usages. Il présente également les profils OCSP et LCR.

Le schéma suivant décrit la hiérarchie des autorités de certification pour l'environnement de production.

2 Profils des certificats

2.1 Profils des certificats des Autorités de Certifications

2.1.1 Autorité de Certification Racine de l'IGC de la Banque de France

Certificat de l'Autorité de Certification racine de l'IGC de la Banque de France.

Cette AC est une AC auto-signée délivrant des certificats exclusivement à destination d'Autorité de Certification de la Banque de France dites :

- **Intermédiaires** : AC émettant des certificats pour des AC Émettrices
- Et **Émettrices** : AC émettant des certificats pour des utilisateurs finaux (personnes physiques, personnes morales, et services applicatifs).

Le champ *Organizationidentifier (2.5.4.97)*, reprend la nomenclature de l'ANSSI (**NTRFR**) suivi du numéro de SIREN de la Banque de France : **NTRFR-572104891**

Le champ *OrganizationUnitName*, reprend les exigences du RGSv2 en spécifiant l'identifiant ICD pour la France (0002) avant le SIREN de la Banque de France : **0002 572104891**

La valeur de ces deux champs est la même pour l'AC Racine ainsi que des AC intermédiaires / émettrices

La colonne « C » indique si le champ est critique (O) ou non (N).

Banque de France AC v3 Racine		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		20 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 20 ans
SubjectPublicKeyInfo		La clé publique avec une longueur de 4096 bits (RSA)
Issuer		
OrganizationIdentifier		NTRFR-572104891

Banque de France AC v3 Racine		
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 Racine
OrganizationUnitName		0002 572104891
OrganizationName		Banque de France
CountryName		FR
Extensions		
KeyUsage	***O***	
keyCertSign		Set
crlSigning		Set
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique de l'AC
BasicConstraints	***O***	
CA		Vraie
pathLenConstraint		None

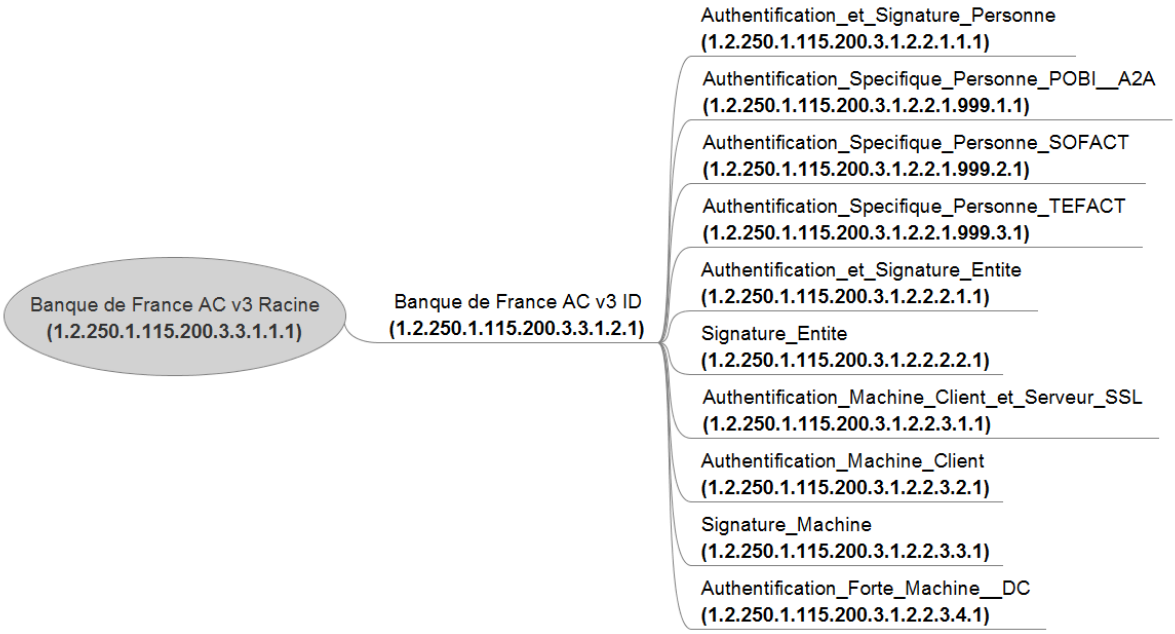
2.1.2 Banque de France AC v3 ID

Autorité de certification délivrant des certificats logiciels d'Authentification et de Signature. Elle est signée par l'AC Banque de France AC v3 Racine.

Banque de France AC v3 ID		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		20 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		NotAfter de l'AC Banque de France AC v3 Racine
SubjectPublicKeyInfo		La clé publique avec une longueur de 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		
KeyUsage	***O***	

Banque de France AC v3 ID		
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		Empreinte SHA-1 de la clé de l'AC Banque de France AC v3 Racine
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique de l'AC Banque de France AC v3 ID.
BasicConstraints	***O***	
CA		Vraie
pathLenConstraint		0

Ci-dessous un schéma qui décrit les profils de certificats de cette AC.



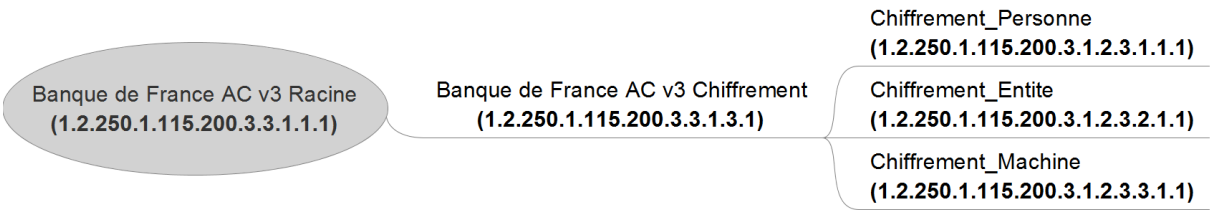
2.1.3 Banque de France AC v3 Chiffrement

Autorité de certification délivrant des certificats logiciels de Chiffrement. Elle est signée par l'AC Banque de France AC v3 Racine

Banque de France AC v3 Chiffrement		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		20 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		NotAfter de l'AC Banque de France AC v3 Racine
SubjectPublicKeyInfo		La clé publique avec une longueur de 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 Chirffrement
OrganizationUnitName		0002 572104891
OrganizationName		Banque de France
CountryName		FR
Extensions		
KeyUsage	***O***	
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 caIssuer • http://cert.igcv3.certificats.banque-france.fr/racine-1.2.250.1.115.200.3.3.1.1.1.cer
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé de l'AC Banque de France AC v3 Racine
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique de l'AC Banque de France AC v3 Chiffrement
BasicConstraints	***O***	
CA		Vraie
pathLenConstraint		0

Ci-dessous un schéma qui décrit les profils de certificats de cette AC.



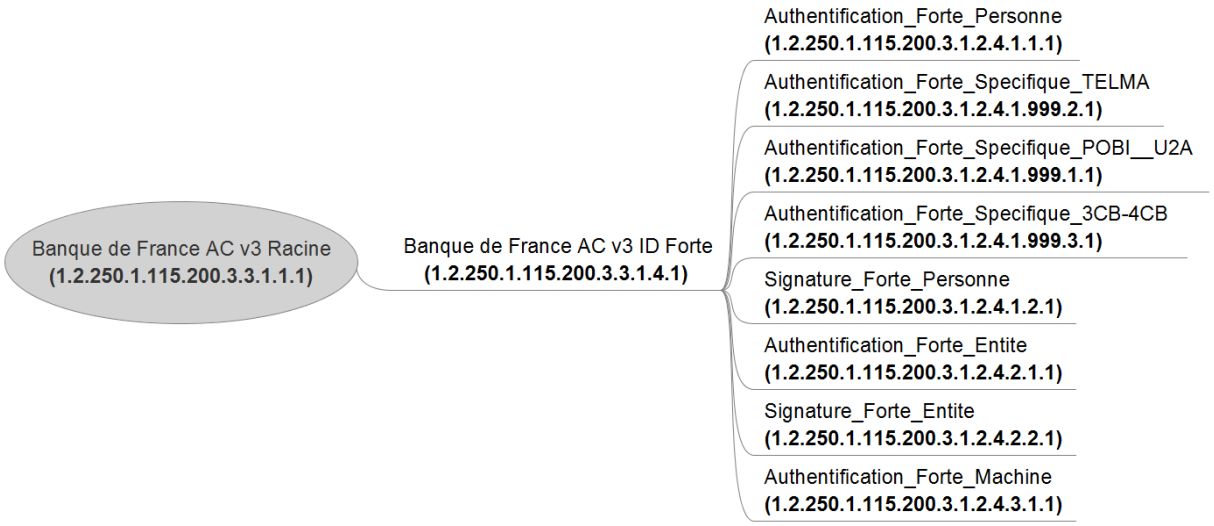
2.1.4 Banque de France AC v3 ID Forte

Autorité de certification délivrant des certificats matériels d'Authentification ou de Signature. Elle est signée par l'AC Banque de France AC v3 Racine.

Banque de France AC v3 ID Forte		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		20 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		NotAfter de l'AC Banque de France AC v3 Racine
SubjectPublicKeyInfo		La clé publique avec une longueur de 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	***O***	
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

Banque de France AC v3 ID Forte		
		• 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		Empreinte SHA-1 de la clé de l'AC Banque de France AC v3 Racine
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique de l'AC Banque de France AC v3 ID Forte.
BasicConstraints	***O***	
CA		Vraie
pathLenConstraint		0

Ci-dessous un schéma qui décrit les profils de certificats de cette AC.



2.2 Profils des certificats émis par l'AC Banque de France AC v3 ID.

Ce chapitre décrit l'ensemble des profils de certificats émis par l'AC Banque de France AC v3 ID.

Ce chapitre est divisé en 3 sous parties :

- Profils de certificats liés à une Personne Physique ;
- Profils de certificats liés à un service applicatif de type Entité ;
- Profils de certificats liés à un service applicatif de type Machine.

2.2.1 Profils de certificats liés à une Personne Physique

2.2.1.1 Authentification et Signature Personne

Certificat logiciel d'authentification et de signature.

LCP		
Champ	**C**	**Valeur**
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
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		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4
		En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
serialNumber		Élément complémentaire permettant de distinguer les homonymes : Empreinte SHA-1 du matricule unique du porteur au sein de l'IGC.
commonName		Le nom complet du porteur tel qu'il devrait être affiché par les applications. Le prénom d'usage du porteur, suivi d'un espace, suivi du nom de l'état civil ou du nom d'usage du porteur.
organizationUnitName		Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - l'ICD est sur 4 caractères ; (0002 pour la France) - l'identification de l'organisation sur 35 caractères - le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Nom officiel complet du de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays de résidence du demandeur
Validity		3 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**

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,OU=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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice (Banque de France AC v3 ID)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant 'User Principal Name' du Porteur
rfc822Name		Adresse Email du Porteur

2.2.1.2 Authentification Spécifique Personne POBI (A2A)

Certificat logiciel d'authentification, avec des champs spécifiques utilisés par une application spécifique Banque de France.

LCP		
Champ	C	Valeur
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
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		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Le nom complet du porteur tel qu'il devrait être affiché par les applications : Numéro de compte dans l'application
organizationUnitName		Identification de l'entité dont dépend le porteur.
organizationName		Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays de résidence du demandeur
Validity		**3 ans**
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice (Banque de France AC v3 ID)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant 'User Principal Name' du Porteur
rfc822Name		Adresse Email du Porteur

2.2.1.3 Authentification Spécifique Personne SOFACT

Certificat logiciel d'authentification, avec des champs spécifiques utilisés par une application spécifique Banque de France.

LCP		
Champ	C	Valeur
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
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		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Le nom complet du porteur tel qu'il devrait être affiché par les applications : Numéro de compte dans l'application
organizationUnitName		Identification de l'entité dont dépend le porteur.
organizationName		Nom officiel complet du de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays de résidence du demandeur
Validity		**3 ans**
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
PublicKeyAlgorithm		rsaEncryption

SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice (Banque de France AC v3 ID)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant 'User Principal Name' du Porteur
rfc822Name		Adresse Email du Porteur

2.2.1.4 Authentification Spécifique Personne TEFACT

Certificat logiciel d'authentification, avec des champs spécifiques utilisés par une application spécifique Banque de France

LCP		
Champ	C	Valeur
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
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		Numéro de compte dans l'application
organizationIdentifier		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Numéro de compte dans l'application
organizationUnitName		Identification de l'entité dont dépend le porteur.
organizationName		Nom officiel complet du de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays de résidence du demandeur
Validity		3 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice (Banque de France AC v3 ID)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant User Principal Name du Porteur
rfc822Name		Adresse Email du Porteur

2.2.2 Profils de certificats liés à un service applicatif de type Entité

2.2.2.1 Authentification et Signature Entité

Certificat logiciel d'authentification et de signature pour une entité.

LCP		
Champ	C	Valeur
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
Key Size		2048 bits (RSA)
Issuer		DN de l'AC émettrice
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		

organizationIdentifier		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4
		En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Nom significatif du service mettant en œuvre le certificat Entité
organizationUnitName2		Nom de l'Entité
organizationUnitName		Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur :
		- l'ICD est sur 4 caractères ; (0002 pour la France)
		- l'identification de l'organisation sur 35 caractères
		- le séparateur entre les deux chaînes est un espace.
		Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays où est établie l'entité responsable du certificat
Validity		3 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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		1.2.250.1.115.200.3.1.2.2.2.1.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	***N***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant 'User Principal Name' de l'Entité
rfc822Name		Adresse Email de l'Entité

2.2.2.2 Signature Entité

Certificat logiciel de signature pour une entité.

LCP		
Champ	C	Valeur
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
Key Size		2048 bits (RSA)
Issuer		DN de l'AC émettrice
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.

commonName		Nom significatif du service mettant en œuvre le certificat Entité
organizationUnitName2		Nom de l'Entité
organizationUnitName		Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - L'ICD est sur 4 caractères ; (0002 pour la France) - L'identification de l'organisation sur 35 caractères - Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays où est établie l'entité responsable du certificat
Validity		**3 ans**
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
		Extensions Standard
KeyUsage	***O***	nonRepudiation
ExtendedKeyUsage	***N***	emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies	***N***	
PolicyIdentifier		1.2.250.1.115.200.3.1.2.2.2.2.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	***N***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**

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		Empreinte SHA-1 de la clé publique de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant 'User Principal Name' de l'Entité
rfc822Name		Adresse Email de l'Entité

2.2.3 Profils de certificat liés à un service applicatif de type Machine

2.2.3.1 Authentification Machine Client et Serveur SSL

Certificat d'authentification SSL serveur.

DVCP		
Champ	C	Valeur
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
Key Size		2048 bits (RSA)
Issuer		DN de l'AC émettrice
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Nom Commun de la machine / serveur.
organizationUnitName2		Nom de l'application rattachée au certificat
organizationUnitName		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4],

		ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - L'ICD est sur 4 caractères ; (0002 pour la France) - L'identification de l'organisation sur 35 caractères - Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays dans lequel est établi ou réside le demandeur
Validity		**3 ans**
NotBefore		Date de la génération du certificat
NotAfter		Date de la génération du certificat + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice (Banque de France AC v3 ID)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name (SAN)	***N***	
otherName (UPN)		(Optionnel) Le FQDN du serveur
dNSName		Un ou plusieurs noms de domaine contrôlés par le responsable du certificat. Ce champ est obligatoire
iPAddress		(Optionnel) Un ou plusieurs adresses IP contrôlés par le responsable du certificat.

2.2.3.2 Authentification Machine Client

Certificat d'authentification SSL client.

DVCP		
Champ	C	Valeur
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
Key Size		2048 bits (RSA)
Issuer		DN de l'AC émettrice
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4
		En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Nom Commun de la machine / serveur.
organizationUnitName2		Nom de l'application rattachée au certificat
organizationUnitName		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce

		champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - L'ICD est sur 4 caractères ; (0002 pour la France), - L'identification de l'organisation sur 35 caractères, - Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays dans lequel est établi ou réside le demandeur
Validity		**3 ans**
NotBefore		Date de la génération du certificat
NotAfter		Date de la génération du certificat + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name (SAN)	***N***	
otherName (UPN)		(Optionnel) Le FQDN de la machine/serveur
rfc822Name		(Optionnel) Adresse Email Principale
rfc822Name		(Optionnel) Adresse Email Secondaire

2.2.3.3 Signature Machine

Certificat de signature pour une machine.

Champ	C	Valeur
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
Key Size		2048 bits (RSA)
Issuer		DN de l'AC émettrice
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Nom Commun de la machine / serveur.
organizationUnitName2		Nom de l'application rattachée au certificat
organizationUnitName		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - L'ICD est sur 4 caractères ; (0002 pour la France)

		- L'identification de l'organisation sur 35 caractères - Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays dans lequel est établi ou réside le demandeur
Validity		3 ans
NotBefore		Date de la génération du certificat
NotAfter		Date de la génération du certificat + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name (SAN)	***N***	
otherName (UPN)		(Optionnel) Le FQDN de la machine/serveur
rfc822Name		(Optionnel) Adresse Email Principale
rfc822Name		(Optionnel) Adresse Email Secondaire

2.3 Profils des certificats émis par l'AC Banque de France AC v3 ID Forte.

Ce chapitre décrit l'ensemble des profils de certificats émis par l'AC Banque de France AC v3 ID Forte.

Ce chapitre est divisé en 3 sous parties :

- Profils de certificats liés à une Personne Physique ;
- Profils de certificats liés à un service applicatif de type Entité ;
- Profils de certificats liés à un service applicatif de type Machine.

2.3.1 Profils des certificats liés à une Personne Physique.

2.3.1.1 Authentification Forte Personne

Certificat matériel d'authentification. Ces certificats se présentent sur un module cryptographique (NCP+).

NCP+		
Champ	**C**	**Valeur**
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
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		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
serialNumber		Élément complémentaire permettant de distinguer les homonymes : Empreinte SHA-1 du matricule unique du porteur au sein de l'IGC.
organizationUnitName		Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - L'ICD est sur 4 caractères ; (0002 pour la France) - L'identification de l'organisation sur 35 caractères - Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes

commonName		Le nom complet du porteur tel qu'il devrait être affiché par les applications. Le prénom d'usage du porteur, suivi d'un espace, suivi du nom de l'état civil ou du nom d'usage du porteur.
countryName		Pays de résidence du demandeur
Validity		**< 3 ans**
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + max 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice (Banque de France AC v3 ID Forte)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat

BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant 'User Principal Name' du Porteur
rfc822Name		Adresse Email du Porteur

2.3.1.2 Authentification Forte Personne TELMA

Authentification forte avec des champs spécifiques pour une application spécifique Banque de France. Ces certificats se présentent sur un module cryptographique (NCP+).

NCP+		
Champ	**C**	**Valeur**
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
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		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Le nom complet du porteur tel qu'il devrait être affiché par les applications : Numéro de compte dans l'application
organizationUnitName		Identification de l'entité dont dépend le porteur.
organizationName		Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays de résidence du demandeur
Validity		**3 ans**
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice (Banque de France AC v3 ID Forte)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant 'User Principal Name' du Porteur
rfc822Name		Adresse Email du Porteur

2.3.1.3 Authentification Forte Spécifique POBI (U2A)

Authentification forte avec des champs spécifiques pour une application spécifique Banque de France. Ces certificats se présentent sur un module cryptographique (NCP+).

NCP+		
Champ	**C**	**Valeur**
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
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		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Le nom complet du porteur tel qu'il devrait être affiché par les applications : Numéro de compte dans l'application
organizationUnitName		Identification de l'entité dont dépend le porteur.
organizationName		Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays de résidence du demandeur
Validity		**3 ans**
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
		Extensions Standard
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**

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		Empreinte SHA-1 de la clé publique de l'AC émettrice (Banque de France AC v3 ID Forte)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant 'User Principal Name' du Porteur
rfc822Name		Adresse Email du Porteur

2.3.1.4 Authentification Forte Spécifique 3CB-4CB

Authentification forte avec des champs spécifiques pour une application spécifique Banque de France. Ces certificats se présentent sur un module cryptographique (NCP+).

Ces certificats sont uniquement à usage interne.

NCP+		
Champ	**C**	**Valeur**
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
Key Size		2048 bits (RSA)
Issuer		
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID Forte
organizationUnitName		0002 572104891
organizationName		Banque de Frances
countryName		FR
Subject		
E (Email)		Adresse Email Fixe Interne à la Banque de France
serialNumber		Elément complémentaire permettant de distinguer les homonymes : Empreinte SHA-1 du matricule unique du porteur au sein de l'IGC.
organizationIdentifier		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.

commonName		Le nom complet du porteur tel qu'il devrait être affiché par les applications : Le prénom d'usage du porteur, suivi d'un espace, suivi du nom de l'état civil ou du nom d'usage du porteur.
organizationUnitName		Identification de l'entité dont dépend le porteur.
organizationName		Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays de résidence du demandeur
Validity		**3 ans**
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice (Banque de France AC v3 ID Forte)
SubjectKeyIdentifier	***N***	

KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant 'User Principal Name' du Porteur
rfc822Name		Adresse Email du Porteur

2.3.1.5 Signature Forte Personne

Certificat de signature sur support matériel. Ces certificats se présentent sur un module cryptographique (NCP+).

NCP+		
Champ	**C**	**Valeur**
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
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		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
serialNumber		Elément complémentaire permettant de distinguer les homonymes : Empreinte SHA-1 du matricule unique du porteur au sein de l'IGC.
commonName		Le nom complet du porteur tel qu'il devrait être affiché par les applications. Le prénom d'usage du porteur, suivi d'un espace, suivi du nom de l'état civil ou du nom d'usage du porteur.
organizationUnitName		Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - L'ICD est sur 4 caractères ; (0002 pour la France) - L'identification de l'organisation sur 35 caractères - Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes

countryName		Pays de résidence du demandeur
Validity		**< 3 ans**
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + max 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice (Banque de France AC v3 ID Forte)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant 'User Principal Name' du Porteur
rfc822Name		Adresse Email du Porteur

2.3.2 Profils des certificats liés à un service applicatif de type Entité

2.3.2.1 Authentification Forte Entité

Certificat matériel d'authentification pour une entité. Ces certificats se présentent sur un module cryptographique (NCP+).

NCP+		
Champ	**C**	**Valeur**
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
Key Size		2048 bits (RSA)
Issuer		DN de l'AC émettrice
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID Forte
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Nom significatif du service mettant en œuvre le certificat Entité
organizationUnitName2		Nom de l'Entité
organizationUnitName		Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - L'ICD est sur 4 caractères ; (0002 pour la France) - L'identification de l'organisation sur 35 caractères - Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays où est établie l'entité responsable du certificat
Validity		**3 ans**
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)

Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant 'User Principal Name' de l'Entité
rfc822Name		Adresse Email de l'Entité

2.3.2.2 Signature Forte Entité

Certificat matériel de signature pour une entité. Ces certificats se présentent sur un module cryptographique (NCP+).

NCP+		
Champ	**C**	**Valeur**
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
Key Size		2048 bits (RSA)
Issuer		DN de l'AC émettrice
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID Forte
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Nom significatif du service mettant en œuvre le certificat Entité
organizationUnitName2		Nom de l'Entité
organizationUnitName		Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - L'ICD est sur 4 caractères ; (0002 pour la France) - L'identification de l'organisation sur 35 caractères - Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays où est établie l'entité responsable du certificat
Validity		**3 ans**
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant 'User Principal Name' de l'Entité
rfc822Name		Adresse Email de l'Entité

2.3.3 Profils des certificats liés à un service applicatif de type Machine

2.3.3.1 Authentification Forte Machine

Profils de certificats conformes à la norme ETSI EN 319 411-1. Ces certificats se présentent sur un support cryptographique de type SSCD.

Champ	C	Valeur
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
Key Size		2048 bits (RSA)
Issuer		**DN de l'AC émettrice**

organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID Forte
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Nom Commun de la machine / serveur.
organizationUnitName2		Nom de l'application rattachée au certificat
organizationUnitName		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - L'ICD est sur 4 caractères ; (0002 pour la France) - L'identification de l'organisation sur 35 caractères - Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays dans lequel est établi ou réside le demandeur
Validity		**3 ans**
NotBefore		Date de la génération du certificat
NotAfter		Date de la génération du certificat + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name (SAN)	***N***	
otherName (UPN)		(Optionnel) Le FQDN du serveur
rfc822Name		(Optionnel) Adresse Email Principale
rfc822Name		(Optionnel) Adresse Email Secondaire

2.3.3.2 Authentification Forte Machine (DC)

Authentification forte pour Contrôleur de domaine.

DVCP		
Champ	C	Valeur
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
Key Size		2048 bits (RSA)
Issuer		DN de l'AC émettrice

organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 ID Forte
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Nom Commun de la machine / serveur.
organizationUnitName2		Nom de l'application rattachée au certificat
organizationUnitName		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - L'ICD est sur 4 caractères ; (0002 pour la France) - L'identification de l'organisation sur 35 caractères - Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays dans lequel est établi ou réside le demandeur
Validity		**3 ans**
NotBefore		Date de la génération du certificat
NotAfter		Date de la génération du certificat + 3 ans
PublicKeyAlgorithm		rsaEncryption
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Extensions Standard		
KeyUsage	***O***	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		1.2.250.1.115.200.3.1.2.4.3.2.1
policyQualifierId		CPS

Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	***N***	**URL(s) de distribution de la CRL de l'AC**
CRLDP1		http://crl.igcv3.certificats.banque-france.fr/id-forte-1.2.250.1.115.200.3.1.2.4.3.2.1.crl
CRLDP2		http://crl.igcv3.certificats.banque-france.org/id-forte-1.2.250.1.115.200.3.1.2.4.3.2.1.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.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
Authority Information Access	***N***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name (SAN)	***N***	
otherName (UPN)		(Optionnel) Le FQDN de la machine/serveur
dNSName		Un ou plusieurs noms de domaine contrôlés par le responsable du certificat. Ce champ est obligatoire
iPAddress		(Optionnel) Un ou plusieurs adresses IP contrôlés par le responsable du certificat.

2.4 Profils des certificats émis par l'AC Banque de France AC v3 Chiffrement.

Ce chapitre décrit l'ensemble des profils de certificats émis par l'AC Banque de France AC v3 Chiffrement.

Ce chapitre est divisé en 3 sous parties :

- Profils de certificats liés à une Personne Physique ;
- Profils de certificats liés à un service applicatif de type Entité ;
- Profils de certificats liés à un service applicatif de type Machine.

2.4.1 Profils des certificats liés à une Personne Physique.

2.4.1.1 Chiffrement Personne

Certificat logiciel de chiffrement (clés doivent être séquestrées).

Champ	C	Valeur
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
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		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
serialNumber		Élément complémentaire permettant de distinguer les homonymes : Empreinte SHA-1 du matricule unique du porteur au sein de l'IGC.
commonName		Le nom complet du porteur tel qu'il devrait être affiché par les applications : Le prénom d'usage du porteur, suivi d'un espace, suivi du nom de l'état civil ou du nom d'usage du porteur.
organizationUnitName		Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - L'ICD est sur 4 caractères ; (0002 pour la France) - L'identification de l'organisation sur 35 caractères - Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Nom officiel complet du de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays de résidence du demandeur
Validity		**3 ans**
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
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***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice (Banque de France AC v3 Chiffrement)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Adresse Email du Porteur
rfc822Name		Adresse Email du Porteur

2.4.2 Profils des certificats liés à un service applicatif de type Entité

2.4.2.1 Chiffrement Entité

Certificat logiciel de chiffrement pour une entité (clés doivent être séquestrées)

Champ	C	Valeur
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
Key Size		2048 bits (RSA)
Issuer		**DN de l'AC émettrice**
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 Chiffrement
organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Nom significatif du service mettant en œuvre le certificat Entité
organizationUnitName2		Nom de l'Entité
organizationUnitName		Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - L'ICD est sur 4 caractères ; (0002 pour la France), - L'identification de l'organisation sur 35 caractères, - Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays où est établie l'entité responsable du certificat
Validity		3 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
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		1.2.250.1.115.200.3.1.2.3.2.1.1
policyQualifierId		CPS

Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	***N***	**URL(s) de distribution de la CRL de l'AC**
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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name	***N***	
otherName (UPN)		Identifiant 'User Principal Name' de l'Entité
rfc822Name		Adresse Email de l'Entité

2.4.3 Profils des certificats liés à une Machine

2.4.3.1 Chiffrement Machine

Certificat de chiffrement pour une machine. (Clés doivent être séquestrées)

Champ	C	Valeur
Version		2=(version 3)
SerialNumber		Unique pour chaque certificat généré par l'IGC
Key Size		2048 bits (RSA)
Issuer		DN de l'AC émettrice
organizationIdentifier		NTRFR-572104891
commonName		Banque de France AC v3 Chiffrement

organizationUnitName		0002 572104891
organizationName		Banque de France
countryName		FR
Subject		
organizationIdentifier		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
commonName		Nom Commun de la machine / serveur.
organizationUnitName2		Nom de l'application rattachée au certificat
organizationUnitName		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - L'ICD est sur 4 caractères ; (0002 pour la France) - L'identification de l'organisation sur 35 caractères - Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
organizationName		Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
countryName		Pays dans lequel est établi ou réside le demandeur
Validity		**3 ans**
NotBefore		Date de la génération du certificat
NotAfter		Date de la génération du certificat + 3 ans
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		1.2.250.1.115.200.3.1.2.3.3.1.1
policyQualifierId		CPS
Qualifier		http://pc.igcv3.certificats.banque-france.fr
CRL Distribution Point	***N***	**URL(s) de distribution de la CRL de l'AC**

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***	**URL(s) du service OCSP de l'AC**
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		Empreinte SHA-1 de la clé publique de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		FAUX
Subject Alternative Name (SAN)	***N***	
otherName (UPN)		(Optionnel) Le FQDN de la machine/serveur
rfc822Name		(Optionnel) Adresse Email Principale
rfc822Name		(Optionnel) Adresse Email Secondaire

3 Profil des LCR et LAR

3.1 Champs des LCR et LAR

Champs de base	Valeur
Version	Version 2
Signature	Sha256WithRSAEncryption (2.16.840.1.101.3.4.2.1)
Hash	sha256
Issuer DN	Selon l'émetteur de chaque AC décrite plus haut
This Update	Au plus tôt à la date de début de vie de l'AC
Next Update	Prochaine date à laquelle la CRL sera mise à jour, soit 6 jours après la date de génération de la présente CRL.
Revoked Certificates	N° de série des certificats révoqués. Exemple : « 0C0062 »
Revocation Date	Date à laquelle un Certificat donné a été révoqué.

3.2 Extensions des LCR et LAR

Champ	O	C	Valeur
Authority Key Identifier	TRUE	FALSE	ID de la clé=voir la clé de chaque AC décrite plus haut
CRL Number	TRUE	FALSE	N° de série de la CRL Exemple : « 0115 »
ExpiredCertsOnCRL	TRUE	FALSE	Date à partir de laquelle les certificats expirés sont conservés dans la CRL. La Banque de France conserve l'ensemble des certificats expirés dans la CRL. La date fixe correspond à une journée après la création des AC de l'IGC de la Banque de France, soit le 29 juin 2019 (20190629000000Z).

4 Protocole de vérification de certificat en ligne (OCSP)

Bien que les exigences complémentaires n'imposent pas la mise en place d'un répondeur OCSP, la version 2 du RGS l'impose. C'est aussi une obligation du CA/B Forum.

Les réponses OCSP doivent se conformer à la RFC6960 et / ou RFC5019. Ainsi, il y a deux possibilités :

1. Être signé par l'AC qui a délivré les certificats dont le statut de révocation est vérifié, ou
2. Être signé par un répondeur OCSP dont le certificat est signé par l'AC qui a délivré le certificat dont l'état de révocation est vérifié.

Dans ce dernier cas, le certificat de signature OCSP doit contenir une extension de type **id-pkix-ocsp-nocheck**, comme défini par RFC6960.

La Banque de France met en œuvre la solution 2, et chaque répondeur OCSP dispose par conséquent d'un certificat propre, émis par l'AC pour laquelle le répondeur OCSP est déployé.

Les AC intermédiaires / émettrices ne signent donc pas les réponses OCSP et par conséquent ne contiennent pas le keyUsage digitalSignature comme préconisé par le RGS qui reprend les préconisations du CAB Forum.

4.1 Les champs communs aux certificats de signature OCSP

Chaque AC intermédiaire / émettrice possède son propre serveur OCSP. Les bi-clés des répondeurs OCSP ont une durée de validité de 3 ans.

Certificat OCSP		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC
KeySize		2048 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 3 ans
SubjectPublicKeyInfo		La clé publique avec une longueur de 2048 bits (RSA)
Issuer		
OrganizationIdentifier		NTRFR-572104891
CommonName		Chaque AC intermédiaire signe le certificat de son propre serveur/certificat OCSP : • 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		Empreinte SHA-1 de la date de création du certificat OCSP
CommonName		Chaque AC intermédiaire possède son propre serveur/certificat OCSP : • OCSP Banque de France AC v3 ID • OCSP Banque de France AC v3 Chiffrement

Certificat OCSP		
		• OCSP Banque de France AC v3 ID Forte
OrganizationUnitName		0002 572104891
OrganizationName		Banque de France
CountryName		FR
Extensions		
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique de l'AC
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte SHA-1 de la clé publique du certificat OCSP

4.2 Les profils des certificats OCSP

Champ	C	IGCv3 Intermediaire
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	***O***	digitalSignature
Extended Key Usage	***N***	OCSP Signing with no-check