1. Objet du Document

Le présent document définit les conditions générales de l'Autorité de Certification « **Banque de France AC v3 Chiffrement** » de la Banque de France.
Il présente, en synthèse, la Politique de Certification « Banque de France AC v3 Chiffrement » référencée sous l'OID **1.2.250.1.115.200.3.1.1.3.1**.

2. Définitions et Acronymes

Le **Client** désigne l'entité personne morale du porteur qui acquiert un certificat auprès de l'AC « Banque de France AC v3 ID ».
Le **Porteur** désigne la personne physique pour laquelle un certificat est émis.
Le **RC/RCAS**, désigne la personne physique responsable de l'utilisation du certificat du service applicatif identifié dans le certificat, et de la clef privée correspondante.
Le **MC** désigne le Mandataire de Certification : personne physique habilité à demander des certificats auprès de l'Autorité d'Enregistrement.
Le **Portail Utilisateur** désigne l'interface utilisée par tout utilisateur de l'IGC (Porteurs et RC) pour la demande et la gestion de ses certificats.

AC	Autorité de Certification
AE	Autorité d'Enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CAPC	Comité d'approbation des politiques de certification
CRL	Certificate Revocation List, ou LCR
LAR	Liste des certificats d'AC révoqués, ou ARL
LDAP	Light Directory Access Protocol
MC	Mandataire de certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification
PDS	PKI Disclosure Statement
QSCD	Qualified Signature Creation Device
RC	Responsable de Certificat
RCAS	Responsable de Certificat d'Authentification Serveur

3. Contact de l'Autorité de Certification

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

4. Type de Certificats émis

Les certificats émis par l'AC « **Banque de France AC v3 Chiffrement** » sont des certificats

- De chiffrement pour les agents et les prestataires de la Banque de France et pour des membres d'une entreprise ou d'un organisme en relation avec un des métiers de la Banque de France.
- De chiffrement pour les services applicatifs (entité) de la Banque de France et des entreprises ou organismes en relation avec un des métiers de la Banque de France.
- De chiffrement pour les services applicatifs (machines) de la Banque de France

Les certificats émis par l'AC « Banque de France AC v3 Chiffrement » sont référencés sous les OID suivants :

Pour une Personne Physique :	
Chiffrement Personne	1.2.250.1.115.200.3.1.2.3.1.1.1

Pour un service applicatif de type Entité de la Banque de France	
Chiffrement Entité	1.2.250.1.115.200.3.1.2.3.2.1.1

Pour un service applicatif de type Machine de la Banque de France	
Chiffrement Machine	1.2.250.1.115.200.3.1.2.3.3.1.1

Les certificats sont émis conformément à la politique de certification publiée à l'adresse suivante : http://pc.igcv3.certificats.banque-france.fr .

Les certificats sont émis à travers la chaîne de certification suivante :

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

Les certificats de la chaîne de certification sont disponibles à l'adresse suivante : http://pc.igcv3.certificats.banque-france.fr
Toute application tierce souhaitant utiliser les certificats de la chaîne de certification doit en faire la demande préalable en écrivant au point de contact défini ci-dessus.

5. Objet des Certificats

Les certificats de chiffrement de personne physique émis par l'AC Banque de France AC v3 Chiffrement sont des certificats à destination de porteurs physiques :

- Agents et prestataires de la Banque de France,
- Membres d'une entreprise ou d'un organisme en relation avec un des métiers de la Banque de France.

Ces certificats sont générés et stockés par l'AC dans une archive logicielle protégée par un mot de passe et remis à chaque porteur. Dans le cadre du badge agent (exclusivement agents et prestataires de la Banque de France), ces certificats sont générés par l'AC et importés dans un dispositif de protection (le badge agent) remis à chaque porteur.
Les clefs privées générées font l'objet d'un séquestre par l'AC.
Les certificats de chiffrement de service applicatif émis par l'AC Banque de France AC v3 Chiffrement sont des certificats à destination :

- Des services applicatifs (entité et/ou machine) de la Banque de France,
- Des services applicatifs (entité) d'une entreprise ou d'un organisme en relation avec un des métiers de la Banque de France.

Ces certificats sont générés et stockés par l'AC dans une archive logicielle protégée par un mot de passe et remis à chaque RC.
Les clefs privées générées font l'objet d'un séquestre par l'AC.

6. Durée / Entrée en vigueur

Les présentes CGU sont opposables au Client et au Porteur dès sa signature et, à défaut de signature, dès la première utilisation du certificat.
Les CGU sont opposables pendant toute la durée de vie du certificat, d'une période de trois ans, sans préjudice de leurs éventuelles mises à jour.
L'AC s'engage à communiquer par tous moyens à sa disposition (courrier électronique, information en ligne, etc.) toute nouvelle version des CGU.
Toute utilisation du certificat après les modifications ou la mise à jour des CGU vaut acceptation des nouvelles CGU par le Client et le porteur.

7. Modalités d'obtention

7.1 Certificat de chiffrement pour une personne physique

1. Préparation et présentation de la demande de certificat

Pour une demande de certificat de chiffrement pour une personne physique, le futur porteur doit disposer d'un compte utilisateur sur le système de gestion des identités de la Banque de France. S'il ne dispose pas de compte utilisateur, celui-ci est créé lors de la demande de certificat.
Pour un agent ou un prestataire de la Banque de France, la demande de certificat ne nécessite pas la constitution d'un dossier d'enregistrement.
Pour un membre d'une entreprise ou d'un organisme en relation avec un des métiers de la Banque de France, la présentation d'une demande de certificat doit émaner d'un MC mandaté par le Client.
Le MC transmet à l'AE un dossier d'enregistrement contenant :

- Un formulaire de demande de certificat, daté de moins de 3 mois, co-signé par le futur porteur et par le MC, indiquant notamment :
  - L'identité du porteur,
  - L'adresse postale et l'adresse email permettant à l'AC de contacter le porteur,
  - Les conditions de séquestre de la clef privée,
  - L'acceptation des Conditions Générales d'Utilisation par le porteur
  - L'attestation que la vérification d'identité du porteur a été effectuée par le MC en face à face.
- Une copie de la pièce d'identité du porteur (en cours de validité, comportant une photographie d'identité, notamment carte nationale d'identité, passeport ou carte de séjour),

Le porteur est informé que l'utilisation de son compte utilisateur est nécessaire pour authentifier toute demande de certificat ou toute demande de révocation.
Le porteur est également informé des conditions de séquestre de la clef privée correspondante à son certificat.

2. Contrôle du dossier d'enregistrement

Dès réception de la demande, l'AE contrôle :

- La complétude de la demande pour un agent ou un prestataire de la Banque de France,
- La complétude du dossier d'enregistrement et notamment la cohérence des justificatifs fournis pour un membre d'une entreprise ou d'un organisme en relation avec un des métiers de la Banque de France.

3. Décision de validation ou de rejet de la demande

Après vérification de la complétude de la demande et du dossier d'enregistrement le cas échéant, l'AE prend la décision de rejeter ou d'accepter la demande :

- Cas du rejet : lorsque la demande est rejetée par l'AE, cette dernière informe le porteur et le MC le cas échéant.
- Cas de validation : lorsque la demande est validée par l'AE, cette dernière déclenche le processus de génération de certificat auprès de la fonction de génération de certificats de l'AC.

4. Transmission du certificat

Le certificat et la clef privée sont générés et stockés par l'AC dans une archive logicielle protégée par un mot de passe. L'archive logicielle est transmise par voie électronique au porteur à travers le Portail Utilisateur, accessible en accès-unique.
L'utilisation de la clef privée est protégée par la saisie de « données d'activation » (mot de passe) que le porteur récupère en s'authentifiant sur le Portail Utilisateur.

5. Acceptation du certificat par le porteur

La démarche d'acceptation est réalisée une fois que le porteur a récupéré successivement l'archive logicielle contenant le certificat et le mot de passe associé sur le Portail Utilisateur.
L'acceptation du certificat par le porteur est réalisée en ligne sur le Portail Utilisateur.
Le porteur dispose d'un délai de 21 jours pour accepter son certificat. Passé ce délai, l'AC prend des mesures allant jusqu'à la révocation du certificat.
Toutefois, le porteur est tenu d'avertir l'AE et son MC de toute inexactitude ou défaut du certificat ou de l'archive logicielle envoyée à la réception de son certificat. Le cas échéant, le certificat est révoqué. En cas de refus explicite du certificat par le porteur, le certificat est révoqué par l'AC.

7.2 Certificat d'Authentification, de Signature, ou d'Authentification et Signature pour un service applicatif de type entité ou machine

1. Préparation et présentation de la demande de certificat

Pour une demande de certificat pour un service applicatif à émettre, le futur RC doit disposer d'un compte utilisateur sur le système de gestion des identités de la Banque de France. S'il ne dispose pas de compte utilisateur, celui-ci est créé lors de la demande de certificat.
Pour une demande de certificat de chiffrement de service applicatif de type machine, le futur RC doit également être un agent de la Banque de France.
Pour une demande de certificat de chiffrement de service applicatif (entité et/ou machine) interne à la Banque de France, la constitution d'un dossier d'enregistrement n'est pas nécessaire.
Pour une demande de certificat de chiffrement de service applicatif (entité) externe à la Banque de France, la demande doit émaner d'un MC mandaté par le Client.
Le MC transmet à l'AE un dossier d'enregistrement contenant :

- Un formulaire de demande de certificat, daté de moins de 3 mois, co-signé par le futur RC et par le MC, indiquant notamment :
  - L'identité du RC,
  - L'adresse postale et l'adresse email permettant à l'AC de contacter le RC,
  - L'identité du service applicatif concerné,
  - Les conditions de séquestre de la clef privée
  - L'acceptation des Conditions Générales d'Utilisation par le RC
  - L'attestation que la vérification d'identité du RC a été effectuée par le MC en face à face.

- Une copie de la pièce d'identité du RC (en cours de validité, comportant une photographie d'identité, notamment une carte nationale d'identité, passeport ou carte de séjour).

Le RC est informé que l'utilisation de son compte utilisateur est nécessaire pour authentifier toute demande de certificat ou toute demande de révocation.
Le RC est également informé des conditions de séquestre de la clef privée correspondante au certificat émis pour le service applicatif dont il est responsable.

2. Contrôle du dossier d'enregistrement

Dès réception de la demande, l'AE contrôle :

- La complétude de la demande pour un service applicatif (entité et/ou machine) de la Banque de France,
- La complétude du dossier d'enregistrement et notamment la cohérence des justificatifs fournis pour service applicatif (entité) d'une entreprise ou d'un organisme en relation avec un des métiers de la Banque de France

3. Décision de validation ou de rejet de la demande

Après vérification de la demande, l'AE prend la décision de rejeter ou d'accepter la demande :

- Cas du rejet : lorsque la demande est rejetée par l'AE, cette dernière informe le RC.
- Cas de validation : lorsque la demande est validée par l'AE, cette dernière déclenche le processus de génération de certificat auprès de la fonction de génération de certificats de l'AC.

4. Transmission du certificat

Le certificat et la clef privée sont générés et stockés par l'AC dans une archive logicielle protégée par un mot de passe. L'archive logicielle est transmise par voie électronique au porteur à travers le Portail Utilisateur, accessible en accès-unique.
L'utilisation de la clef privée est protégée par la saisie de « données d'activation » (mot de passe) que le porteur récupère en s'authentifiant sur le Portail Utilisateur.

5. Acceptation du certificat par le RC

Pour un certificat de service applicatif de type entité, la démarche d'acceptation est réalisée une fois que le RC a récupéré successivement l'archive logicielle contenant le certificat et le mot de passe associé sur le Portail Utilisateur.
Pour un certificat de service applicatif de type machine, la démarche d'acceptation est réalisée une fois que le RC a récupéré le certificat sur le Portail Utilisateur.
L'acceptation du certificat par le RC est réalisée en ligne sur le Portail Utilisateur.
Le RC dispose d'un délai de 21 jours pour accepter le certificat. Passé ce délai, l'AC prend des mesures allant jusqu'à la révocation du certificat.
Toutefois, le RC est tenu d'avertir l'AE de toute inexactitude ou défaut du certificat ou de l'archive logicielle envoyée à la réception du certificat. Le cas échéant, le certificat est révoqué. En cas de refus explicite du certificat par le RC, le certificat est révoqué par l'AC.

7.3 Modalités d'enregistrement d'un nouveau RC pour un certificat de service applicatif de type entité ou machine déjà émis

Le changement de RC pour un certificat de service applicatif déjà émis n'est pas permis sans révocation du certificat.
Le RC est informé que l'utilisation de son compte utilisateur est nécessaire pour authentifier toute demande de certificat ou toute demande de révocation.

8. Modalités de renouvellement

Une notification est envoyée au porteur/RC à l'approche de la date d'expiration du certificat de façon à préparer la délivrance d'un nouveau certificat. Le déclenchement de la fourniture d'un nouveau certificat est à l'initiative du porteur/RC ou du MC qui lui est rattaché le cas échéant.
Les modalités de traitement d'une demande d'un nouveau certificat sont identiques à celles de la demande initiale.
Note : La génération d'un nouveau bi-clef est systématique pour toute délivrance d'un certificat.

9. Modalités de révocation

Une demande de révocation d'un certificat peut être faite :

- Pour une personne physique :
  - Par le porteur au nom duquel le certificat a été émis,
  - Par un MC de l'organisme du porteur,
  - Par un RL de l'organisme du porteur,
  - Par l'AC ayant délivré le certificat,
  - Et par l'AE rattachée à l'AC.
- Pour un service applicatif :
  - Par le RC pour le service applicatif (de type entité ou machine) considéré,
  - Par un RL de l'organisme du RC,
  - Par un MC de l'organisme du RC,
  - Par l'AC ayant délivré le certificat,
  - Et par l'AE rattachée à l'AC.

Les demandes de révocation peuvent être réalisées :

- En ligne , depuis le portail utilisateur, accessible l'adresse suivante: https://igcv3.certificats.banque-france.fr ,
- Par e-mail en écrivant directement à l'adresse 1206-crypto-ut@banque-france.fr ,
- Par courrier en écrivant à l'adresse suivante :

Banque de France
39 rue croix des petits champs
S1A-1206 Cellule R4F
75001 Paris

Si la demande est recevable, le certificat est révoqué par l'AE dans un délai de 24h maximum.
Dans tous les cas, à l'exception d'une révocation effectuée en ligne par le porteur/RC, la révocation est effectuée par l'Autorité d'Enregistrement, qui valide ainsi la demande.
Le demandeur, le porteur/RC et, via son MC, son entité sont informés par email de la prise en compte de la demande de révocation via accusé de réception émanant de l'AE.

10. Limites de responsabilité

Les certificats émis par l'AC « **Banque de France AC v3 Chiffrement** » pour des porteurs (personnes physiques) ne sont utilisables qu'à des fins de chiffrement.
Les certificats émis par l'AC « **Banque de France AC v3 Chiffrement** » pour des services applicatifs ne sont utilisables qu'à des fins de chiffrement.
Les certificats sont délivrés pour une durée de :

- 3 ans pour les certificats de personnes physiques (authentification, authentification et signature),
- 3 ans pour les certificats de services applicatifs (authentification, signature, et authentification de site internet).

L'AC « **Banque de France AC v3 Chiffrement** » conserve les données et les traces d'enregistrement pendant les délais prévus dans la Politique de Certification, à savoir :

- Les journaux d'évènements sont conservés sur site pendant au moins 1 mois. Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous 1 mois. Les journaux d'évènements sont conservés pendant au moins dix ans à compter de leur date de génération.
- Les dossiers et les pièces justificatives sont archivés pour une durée de dix ans à compter de la date d'acceptation du certificat par le porteur/RC.
- Les certificats et les LCR émis par l'AC sont conservés pendant au moins dix ans à compter de leur génération.
- Les réponses OCSP sont conservées pendant au moins trois mois à compter de leur date d'expiration.

11. Obligations des porteurs / RC

Le porteur/RC a l'obligation de :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat,
- Protéger sa clef privée/la clef privée du serveur dont il est responsable par des moyens appropriés à son environnement,
- Protéger les données d'activation et les mettre en œuvre uniquement lorsque nécessaire,
- Respecter les conditions d'utilisation de sa clef privée/la clef privée du serveur et du certificat correspondant,
- Informer l'AC de toute modification concernant les informations contenues dans le certificat,
- Demander, sans délai, la révocation du certificat en cas de compromission ou de suspicion de compromission de la clef privée ou des données d'activation.

12. Obligations de vérification des certificats par les utilisateurs

Les utilisateurs de certificats ont l'obligation de :

- Vérifier et respecter l'usage pour lequel un certificat a été émis,
- Vérifier que le certificat utilisé a bien été émis par l'AC « **Banque de France AC v3 Chiffrement** »,
- Vérifier que le certificat n'est pas présent dans les listes de révocation de l'AC « **Banque de France AC v3 Chiffrement** »,
- Vérifier la signature du certificat, et de la chaîne de certification, jusqu'à l'AC « **Banque de France AC v3 Racine** » et contrôler la validité des certificats.

Les certificats de la chaîne de certification sont disponibles à l'adresse suivante : http://pc.igcv3.certificats.banque-france.fr .

La liste de révocation des certificats émis par l'AC « **Banque de France AC v3 ID Chiffrement** » est disponible à l'adresse suivante :

- http://crl.igcv3.certificats.banque-france.fr/chiffrement-1.2.250.1.115.200.3.4.1.3.1.crl
- http://crl.igcv3.certificats.banque-france.org/chiffrement-1.2.250.1.115.200.3.4.1.3.1.crl
- ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20Chiffrement,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
- ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20Chiffrement,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

Les certificats révoqués restent présents dans la LCR même après leur date d'expiration d'origine.

À défaut de pouvoir consulter les LCR, un service de vérification en ligne du statut des certificats (OCSP) est mis à disposition des utilisateurs par la Banque de France.

Le répondeur OCSP est accessible aux adresses suivantes :

- 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

La fonction d'information sur l'état des certificats est disponible 24h/24 et 7j/7. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme à 4h et une durée maximale totale d'indisponibilité par mois conforme à 8h.

Le temps de réponse maximum du service OCSP à une requête reçue portant sur l'état d'un certificat est de 6 secondes à partir de la réception de la requête par le serveur.

13. Limite de garantie

L'AC décline toute responsabilité à l'égard de l'usage des certificats émis par elle ou des bi-clefs associés dans des conditions et à des fins autres que celles prévues dans la PC ainsi que dans tout autre document contractuel applicable associé.

L'AC décline toute responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, et quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication.

L'AC décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le porteur/RC ou le MC.

L'AC ne saurait être tenue responsable, et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'Article 1148 du Code civil.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, outre ceux habituellement retenus par la jurisprudence des cours et tribunaux français, la défaillance du réseau ou des installations ou réseaux de télécommunications externes.

L'AC n'est en aucun cas responsable des préjudices indirects subis par les entités utilisatrices.

14. Références documentaires

La Politique de Certification de « **Banque de France AC v3 Chiffrement** » est accessible à l'adresse suivante : http://pc.igcv3.certificats.banque-france.fr.

15. Politique de confidentialité

La collecte et l'usage de données personnelles par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (règlement général sur la protection des données – RGPD) et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

L'AC et le Client sont chacun responsable de traitement pour les données personnelles qu'il traite dans le cadre de la gestion des certificats et s'engagent à respecter les dispositions légales et réglementaires susvisées.

Les données personnelles recueillis par l'AC sont exclusivement réservées au traitement de l'IGC-BDF-V3, basé sur le respect d'une obligation légale, et dont la finalité est la gestion du cycle de vie des certificats numériques (vérification de l'identité, création du compte utilisateur, génération et gestion du certificat). Ces données sont destinées à l'administration de la Banque de France. Dans ce cadre, elle collecte des données personnelles nécessaires au traitement : données d'identification (Nom, Prénom), et coordonnées (adresse postale et électronique) des porteurs et mandataires de certification. Des données complémentaires sont également récoltées, afin d'effectuer les vérifications d'identités (copie de la pièce d'identité des Porteurs / Mandataires et Responsables Légaux).

Ces données sont conservées pendant 10 ans à compter de la date de génération du dernier certificat électronique délivré au porteur, et conformément à la Politique de Certification de l'AC.

Seuls les services internes de l'Autorité de Certification de la Banque de France, ainsi que les services de contrôle interne et d'audit, ont accès à ces données.

Vous disposez d'un droit d'accès et de rectification à vos données que vous pouvez exercer auprès de la Banque de France par email 1206-r4f-ut@banque-france.fr.

Vous avez la possibilité de déposer une réclamation auprès de la CNIL. Les coordonnées du Délégué à la Protection des Données sont : 1200-DPD-delegue-ut@banque-france.fr.

16. Conditions d'indemnisation

Sans Objet.

17. Loi applicable / résolution de conflits

Les présentes CGU et la Politique de Certification de l'AC « **Banque de France AC v3 Chiffrement** » sont soumises au droit français.

En cas de réclamation ou de contestation sur l'interprétation ou l'exécution du présent document ou du service de certification électronique, les parties en litige s'efforcent de régler le différend à l'amiable préalablement à toute instance judiciaire.

Application de la législation et de la réglementation en vigueur sur le territoire français.

18. Audits et références applicables

Les certificats émis par l'AC « Banque de France AC v3 Chiffrement » et la politique de certification sont structurées sur la base des exigences du document ETSI EN 319 411-1 relatif aux autorités de certification délivrant des certificats.

Un contrôle de conformité de la DPC à la PC pourra être effectué, sur demande du Comité d'approbation des politiques de certification (CAPC).

L'AC s'engage à effectuer ce contrôle au minimum une fois par an.

Par ailleurs, avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC fera également procéder à un contrôle de conformité de cette composante.

Signature du Porteur de Certificat / RC
Date: Nom : Prénom : Signature :