Sécurité de l'information

Politique de certification
Banque de France AC v3 Racine

(OID : 1.2.250.1.115.200.3.1.1.1.1)

Date	***:***	28 Mai 2020	***Version***	***:***	1.0
Rédacteur	***:***	RSI	***Nombre de pages***	***:***	49
Classification	***:***	Publique			

FICHE DE CONTRÔLE DU DOCUMENT

Suivi des versions

Version	Date	Rédacteur	Modification
1.0	28/05/2020	DM - RSI	Version Initiale

Validation du document : Validé par le Comité d'approbation des politiques de certification de la Banque de France.

TABLE DES MATIÈRES

1. INTRODUCTION 5
1.1. PRÉSENTATION GÉNÉRALE 5
1.2. IDENTIFICATION DU DOCUMENT 6
1.3. DÉFINITIONS ET ACRONYMES 6
1.4. ENTITÉS INTERVENANT DANS L'INFRASTRUCTURE DE GESTION DE CLEFS 8
1.5. USAGE DES CERTIFICATS 11
1.6. GESTION DES POLITIQUES DE CERTIFICATION 11
2. RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIÉES 13
2.1. ENTITÉS CHARGÉES DE LA MISE À DISPOSITION DES INFORMATIONS 13
2.2. INFORMATIONS PUBLIÉES 13
2.3. DÉLAIS ET FRÉQUENCE DE PUBLICATION 13
2.4. CONTRÔLE D'ACCÈS AUX INFORMATIONS PUBLIÉES 13
3. IDENTIFICATION ET AUTHENTIFICATION 14
3.1. NOMMAGE 14
3.2. VALIDATION INITIALE DE L'IDENTITÉ 15
3.3. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLEFS 16
3.4. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RÉVOCATION 16
4. EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DE CERTIFICATS 17
4.1. DEMANDE DE CERTIFICAT 17
4.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT 17
4.3. DÉLIVRANCE DU CERTIFICAT 17
4.4. ACCEPTATION DU CERTIFICAT 17
4.5. USAGES DU BI-CLEF ET DU CERTIFICAT 18
4.6. RENOUVELLEMENT (AU SENS RFC 3647) D'UN CERTIFICAT 18
4.7. DÉLIVRANCE D'UN NOUVEAU CERTIFICAT SUITE À UN CHANGEMENT DE BI-CLEF 18
4.8. MODIFICATION D'UN CERTIFICAT 19
4.9. RÉVOCATION ET SUSPENSION DES CERTIFICATS 19
4.10. FONCTION D'INFORMATION SUR L'ÉTAT DES CERTIFICATS 22
4.11. FIN DE LA RELATION ENTRE L'AC INTERMÉDIAIRE/EMETTRICE ET L'AC RACINE 22
4.12. SÉQUESTRE DE CLEF ET RECOUVREMENT 22
5. MESURES DE SÉCURITÉ NON TECHNIQUES 23
5.1. MESURES DE SÉCURITÉ PHYSIQUE 23
5.2. MESURES DE SÉCURITÉ PROCÉDURALES 24
5.3. MESURES DE SÉCURITÉ VIS-À-VIS DU PERSONNEL 25
5.4. PROCÉDURES DE CONSTITUTION DES DONNÉES D'AUDIT 26
5.5. ARCHIVAGE DES DONNÉES 28
5.6. CHANGEMENT DE CLEF D'AC 29
5.7. REPRISE SUITE À COMPROMISSION OU SINISTRE 29
5.8. FIN DE VIE DE L'IGC 30
6. MESURES DE SÉCURITÉ TECHNIQUES 32
6.1. GÉNÉRATION ET INSTALLATION DE BI-CLEFS 32
6.2. MESURES DE SÉCURITÉ POUR LA PROTECTION DES CLEFS PRIVÉES ET POUR LES MODULES CRYPTOGRAPHIQUES 33

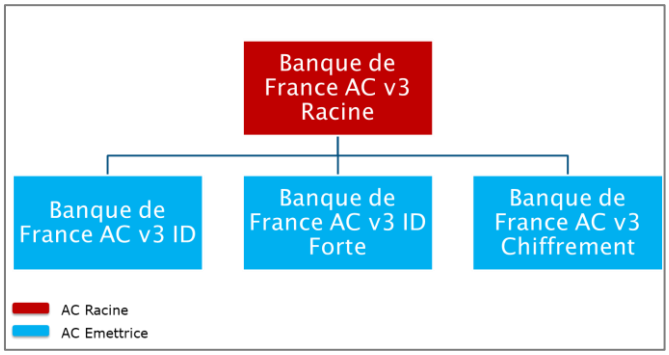
6.3. AUTRES ASPECTS DE LA GESTION DES BI-CLEFS 35
6.4. DONNÉES D'ACTIVATION 35
6.5. MESURES DE SÉCURITÉ DES SYSTÈMES INFORMATIQUES 35
6.6. MESURE DE SÉCURITÉ DES SYSTÈMES DURANT LEUR CYCLE DE VIE. 36
6.7. MESURES DE SÉCURITÉ RÉSEAU 36
6.8. HORODATAGE / SYSTÈME DE DATATION 37
7. PROFILS DES CERTIFICATS ET DES LCR / LAR 38
8. AUDITS DE CONFORMITÉ ET AUTRES ÉVALUATIONS 39
8.1. FRÉQUENCE ET CIRCONSTANCES DES ÉVALUATIONS 39
8.2. IDENTITÉ ET QUALIFICATION DES ÉVALUATEURS 39
8.3. RELATIONS ENTRE ÉVALUATEURS ET ENTITÉS ÉVALUÉES 39
8.4. SUJETS COUVERTS PAR LES ÉVALUATIONS 39
8.5. ACTIONS PRISES SUITE AUX CONCLUSIONS DES ÉVALUATIONS 39
8.6. COMMUNICATION DES RÉSULTATS 39
9. AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES 40
9.1. TARIFS 40
9.2. RESPONSABILITÉ FINANCIÈRE 40
9.3. CONFIDENTIALITÉ DES DONNÉES PROFESSIONNELLES 40
9.4. PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL 41
9.5. DROITS SUR LA PROPRIÉTÉ INTELLECTUELLE ET INDUSTRIELLE 42
9.6. INTERPRÉTATIONS CONTRACTUELLES ET GARANTIES 42
9.7. EXCLUSIONS ET LIMITATIONS DE GARANTIE 43
9.8. EXCLUSIONS ET LIMITATIONS DE RESPONSABILITÉS 43
9.9. INDEMNITÉS 44
9.10. DURÉE ET FIN ANTICIPÉE DE VALIDITÉ DE LA PC 44
9.11. NOTIFICATIONS INDIVIDUELLES ET COMMUNICATION ENTRE LES PARTICIPANTS 44
9.12. AMENDEMENTS DE LA PC 44
9.13. DISPOSITIONS CONCERNANT LA RÉSOLUTION DE CONFLITS 44
9.14. JURIDICTIONS COMPÉTENTES 45
9.15. CONFORMITÉ AUX LÉGISLATIONS ET RÉGLEMENTATIONS 45
9.16. DISPOSITIONS DIVERSES 46
9.17. AUTRES DISPOSITIONS 46
10. ANNEXE 1 : DOCUMENTS CITÉS EN RÉFÉRENCE 47
10.1. RÈGLEMENTATION 47
10.2. DOCUMENTS TECHNIQUES 47
11. ANNEXE 2 : EXIGENCES DE SÉCURITÉ DU MODULE CRYPTOGRAPHIQUE DE L'AC ... 49
11.1. EXIGENCES SUR LES OBJECTIFS DE SÉCURITÉ 49
11.2. EXIGENCES SUR LA CERTIFICATION 49

1. Introduction

1.1. Présentation générale

La Banque de France a mis en œuvre sa propre Infrastructure de Gestion de Clefs nommée IGCv3 afin de sécuriser son système d'information et les échanges entre ses différents métiers.

L'IGC de la Banque de France s'appuie sur une hiérarchie de certification illustrée sur le schéma ci-dessous :



Pour des raisons de confidentialité, ce schéma illustre exclusivement les AC publiques dédiées aux utilisateurs finaux.

Le présent document constitue la politique de certification (PC) de l'autorité de certification « Banque de France AC v3 Racine » de la Banque de France et contient les informations publiques de la Déclaration des Pratiques de Certification (DPC) associée.

L'autorité de certification (AC) « Banque de France AC v3 Racine » est une AC Racine auto-signée délivrant des certificats exclusivement à destination d'autorités de certification de la Banque de France dites :

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

La structure du présent document est basée sur les préconisations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)) relatives à l'application du Référentiel de sécurité (RGS) pris en application du décret n°2010-112 du 2 février 2010 (décret RGS) lui-même pris en application des dispositions des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives et de la RFC 3647.

Cette offre de certificats et sa politique de certification (PC) sont structurées sur la base des exigences du document ETSI EN 319 411-1 relatif aux autorités de certification délivrant des certificats.

Cette politique de certification a vocation à être consultée et examinée par les organismes ou les personnes qui utiliseront ces certificats pour les aider à apprécier le degré de confiance qu'ils peuvent placer dans ces certificats.

Cette politique de certification a le statut de document « public » sur l'échelle de classification de la Banque de France et est mise à disposition du public sous différentes formes, notamment sous format électronique, sur le site web institutionnel de la Banque de France.

1.2. Identification du document

La présente PC porte le titre suivant :

Politique de certification
Banque de France AC v3 Racine

Cette PC est identifiée par l'OID 1.2.250.1.115.200.3.1.1.1.1 et couvre les offres de certificats identifiés par les OID suivants :

Usage du certificat	OID de la PC
Autorité de Certification Intermédiaire ou Emettrice	1.2.250.1.115.200.3.1.2.1.1

La présente PC est associée à la Déclaration des Pratiques de Certification (DPC) contenant les informations des pratiques de l'AC, considérées comme confidentielles par la Banque de France, et identifiée par un OID.

1.3. Définitions et acronymes

1.3.1. Acronymes

Les acronymes utilisés dans ce document sont présentés dans le tableau suivant.

AC	Autorité de certification
AE	Autorité d'enregistrement
AED	Autorité d'Enregistrement Déléguée
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ARL	Authority Revocation List, ou LAR
CAPC	Comité d'approbation des politiques de certification (cf. chapitre 1.6.1)
CN	Common Name
CRL	Certificate Revocation List, ou LCR
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IGC	Infrastructure de gestion de clefs, ou PKI en anglais
ITU	International Telecommunication Union
LAR	Liste des certificats d'AC révoqués, ou ARL
LCR	Liste des certificats révoqués, ou CRL
LDAP	Light Directory Access Protocol
MC	Mandataire de certification
O	Organization
OC	Opérateur de certification
OCSP	Online Certificate Status Protocol
OI	Organization Identifier
OID	Object Identifier
OU	Organizational Unit

PC	Politique de certification
PDS	PKI Disclosure Statement (Déclaration des informations de l'IGC)
PIN	Personal Identification Number
PP	Profil de protection
PKI	Public Key Infrastructure, ou IGC en français
PSCE	Prestataire de services de certification électronique
PUK	PIN Unlock Key
QSCD	Qualified Signature Creation Device (Dispositif de création de signature qualifié)
RC	Responsable de Certificat
RCAS	Responsable de Certificat d'Authentification du Serveur
RFC	Request for Comments
RGPD	Règlement Général sur la Protection des Données
RSA	Rivest Shamir Adelman
SAN	Subject Alternative Name
SHA256	Secure Hash Algorithm 256
SP	Service de publication
SSI	Sécurité des systèmes d'information
UPN	User Principal Name
URL	Uniform Resource Locator

Tableau 1 – Liste des acronymes

1.3.2. Définitions

Les termes utilisés dans ce document sont présentés dans le tableau suivant.

Entrée	Définition
Algorithme RSA	Inventé en 1978 par Ronald L. Rivest, Adi Shamir et Leonard M. Adleman. Il peut être utilisé pour chiffrer des informations et/ou pour les signer (signature numérique).
Autorité de certification (AC)	Entité, composante de base de l'IGC, qui délivre des certificats à une population de porteurs ou à d'autres composants d'infrastructure.
Autorité de certification émettrice	Autorité de certification dont le certificat est signé par l'autorité de certification racine. Une autorité de certification émettrice signe les certificats des porteurs.
Autorité de certification racine	Autorité de certification dont le certificat est auto-signé. L'autorité de certification racine signe les certificats des autorités de certification émettrices.
Autorité d'enregistrement (AE)	Cf. paragraphe 1.4.2.
Bi-clef	Ensemble constitué d'une clef publique et d'une clef privée, formant une paire indissociable utilisée par un algorithme cryptographique asymétrique.
Comité d'approbation des politiques de certification (CAPC)	Entité de la Banque de France en charge de la validation des politiques de certification. À date de rédaction de ce document, le CAPC est le Comité de pilotage de l'IGC. Fonction interne à la Banque de France

Entrée	Définition
Certificat de clef publique	Message structuré (ex. X. 509 v3) créé et signé par une autorité de certification reconnue, laquelle garantit l'authenticité de la clef publique qu'il contient. Un certificat contient au minimum un identifiant du porteur et la clef publique du porteur. L'autorité de certification signe les certificats à l'aide de sa propre clef privée.
Clef privée	Composant confidentiel d'une bi-clef, connu uniquement de son propriétaire et utilisé par lui seul pour déchiffrer une donnée dont il est destinataire ou pour signer des données dont il est l'auteur.
Clef publique	Composant non confidentiel d'une bi-clef, pouvant être communiqué à tous les membres d'une population. Une clef publique permet de chiffrer des données à destination du porteur de la bi-clef. Elle permet également de vérifier une signature apposée par le porteur.
Composante	Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC.
Liste des certificats révoqués	Certificate Revocation List ou Liste de Certificats Révoqué (LCR) Liste des numéros de certificats non expirés ayant fait l'objet d'une révocation. La CRL est signée par l'autorité de certification pour assurer son intégrité et son authenticité.
Déclaration des pratiques de certification (DPC)	Ensemble des pratiques à mettre en œuvre pour satisfaire aux exigences de la PC.
Gestionnaire local de la sécurité (GLS)	Dans chaque unité où la sécurité de l'information nécessite la mise en œuvre et le suivi de procédures locales, un GLS est désigné. Il assiste le responsable de l'unité dans tous les domaines relevant de la sécurité de l'information. Fonction interne à la Banque de France
Infrastructure de gestion de clefs	Ensemble de composants, fonctions et procédures dédiés à la gestion de bi-clefs et de certificats.
Mandataire de certification	Personne physique assurant le rôle d'autorité d'enregistrement par délégation.
Entité ou Organisme	Entité responsable d'une AC Intermédiaire ou Emettrice.
Object Identifier (OID)	Identifiant unique permettant de référencer la PC auprès d'un organisme tiers.
Politique de certification (PC)	Ensemble de règles qui indique les conditions d'applicabilité d'un certificat pour une communauté donnée ou pour des applications ayant des besoins de sécurité communs.
Portail Utilisateur	Interface utilisée par tout utilisateur standard de l'IGC (*porteurs et RC*) pour la demande et la gestion de ses certificats en mode self-service
Portail de gestion	Interface utilisée par les Opérateurs et des MC pour la gestion des certificats durant leur cycle de vie
PKCS (*Public Key Cryptographic Standards*)	Ensemble de standards de chiffrement relatifs aux clefs publiques.
Responsable de la sécurité de l'information (RSI)	Propriétaire de l'Infrastructure de gestion de clefs de la Banque de France Fonction interne à la Banque de France

Tableau 2 – Définitions

1.4. Entités intervenant dans l'infrastructure de gestion de clefs

Ce paragraphe présente les entités intervenant dans l'infrastructure de gestion de clefs (IGC), ainsi que les obligations auxquelles elles sont soumises.

Les obligations suivantes sont communes à toutes les entités de l'IGC :

- documenter et respecter les accords, conventions ou contrats qui lient la Banque de France aux autres entités ;
- mettre en œuvre les moyens techniques et humains nécessaires à la réalisation des prestations auxquelles l'entité s'engage dans les conditions garantissant qualité et sécurité.

1.4.1. Autorités de certification

L'infrastructure de gestion de clefs (IGC) mise en place par la Banque de France permet l'émission de plusieurs types de certificats électroniques.

Ces certificats appartiennent à des offres établies suivant des critères divers, en particulier :

- leurs usages ;
- leur niveau de sécurité.

La Banque de France a choisi un modèle de confiance (présenté ci-dessous) dans lequel on trouve une AC « racine », plusieurs AC « Emettrices » et AC « Intermédiaires ».

Le certificat de l'AC « racine » est auto-signé et ne dépend pas d'autres autorités de certification. Les certificats des AC « Emettrices » et des AC « Intermédiaires » sont signés par l'AC « racine ».

Les autorités de certification sont représentées par le Responsable de la sécurité de l'information (RSI) de la Banque de France.

La notion d'autorité de certification (AC) telle qu'utilisée dans la présente PC est définie au chapitre 1.3.2 ci-dessus.

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation, ...) et s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clefs (IGC).

Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clefs et des certificats.

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'European Telecommunications Standards Institute (ETSI) dans le domaine (cf. ETSI EN 319 411-1), la décomposition *fonctionnelle* d'une IGC qui est retenue dans la présente PC est la suivante :

- **Autorité d'enregistrement (AE)** (aussi appelée « service d'enregistrement ») - Cette fonction vérifie les informations d'identification de la future Autorité de Certification Intermédiaire ou Emettrice pour laquelle le certificat est émis, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. L'AE a également en charge, lorsque cela est nécessaire, la re vérification des informations de l'AC Intermédiaire ou Emettrice lors du renouvellement du certificat de celle-ci.
- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clef privée de l'AC) les certificats de l'AC Racine, des AC Intermédiaires et des AC Emettrices à partir des informations transmises par l'autorité d'enregistrement.
- **Fonction de génération des éléments secrets** - Cette fonction génère les éléments secrets à destination de l'AC Racine, des AC Intermédiaires et des AC Emettrices.
- **Fonction de remise** - Cette fonction remet à l'AC Intermédiaire ou Emettrice au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif cryptographique, clef privée, codes d'activation,…).
- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées, les politiques et pratiques publiées par l'AC Racine, les certificats d'AC et toute autre information pertinente destinée aux AC Intermédiaires et AC Emettrices et/ou aux utilisateurs de certificats, hors informations d'état des certificats.
- **Fonction de gestion des révocations** - Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
- **Fonction d'information sur l'état des certificats** - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) et éventuellement également selon un mode requête-réponse temps réel (OCSP).

Dans le cadre de ses fonctions opérationnelles, l'AC veille au respect des exigences suivantes en tant que responsable de l'ensemble de l'IGC :

- Être une entité légale au sens de la loi française.
- Être en relation par voie contractuelle ou hiérarchique ou réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats des services applicatifs de cette entité. L'AC peut aussi, le cas échéant, être en relation contractuelle ou hiérarchique ou réglementaire avec le ou les mandataires de certification choisis par l'entité.

- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux porteurs, aux utilisateurs de certificats, ceux qui mettent en œuvre ses certificats.

- S'assurer que les exigences de la PC et les procédures de la déclaration des pratiques de certification (DPC) sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.

- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions obligatoires de la présente PC, notamment en matière de génération des certificats, de remise des certificats, de gestion des révocations et d'information sur l'état des certificats.

- Élaborer, mettre en œuvre, contrôler et maintenir les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels. L'AC mène une analyse de risques permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse.

- Mettre en œuvre ce qui est nécessaire pour respecter les engagements définis dans sa PC, notamment en termes de fiabilité, de qualité et de sécurité. À ce titre, elle doit posséder un ou des systèmes de gestion de la qualité et de la sécurité de l'information adaptés aux services de certification qu'elle assure.

- Générer, et renouveler lorsque nécessaire, ses bi-clefs et les certificats correspondants (signature de certificats, de LCR et de réponses OCSP), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux porteurs et utilisateurs de certificats.

- Suivre les demandes en capacité et réaliser des projections concernant les futurs besoins en capacité afin de garantir la disponibilité du service, notamment en matière de capacités de traitement et de stockage.

1.4.2. Autorité d'enregistrement

L'AE a pour rôle de vérifier et de valider les informations de la future AC Intermédiaire ou AC Emettrice . Pour cela, l'AE assure les tâches suivantes :

- La prise en compte et la vérification des informations de la future AC Intermédiaire ou AC Emettrice ;
- L'établissement et la transmission des demandes afférentes à un certificat à la fonction adéquate de l'IGC ;
- L'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;

Dans tous les cas, l'archivage des pièces du dossier d'enregistrement (sous forme électronique et/ou papier) est de la responsabilité de l'AE (cf. chapitre 5.5).

1.4.3. Autorité de Certification Intermédiaire ou Emettrice

Un certificat d'AC Intermédiaire ou d'AC Emettrice ne peut être délivré qu'à la Banque de France ou à une de ses filiales.

La Politique de Certification et la Déclaration des Pratiques de Certification de l'AC Intermédiaire ou de l'AC Emettrice doivent être fournies à l'AC Racine pour valider que les exigences sont cohérentes avec celles de la présente PC.

1.4.4. Utilisateurs de certificats

Sont appelés utilisateurs, les personnes physiques ou automates qui s'appuient sur les certificats d'AC délivrés par l'AC Racine pour vérifier l'origine et la validité des certificats d'utilisateurs finaux délivrés pour leurs propres besoins.

Les utilisateurs des AC Intermédiaires et Emettrices sont précisés dans leurs PC respectives.

1.4.5. Autres participants

1.4.5.1. Composantes de l'IGC

La décomposition en fonctions de l'IGC est présentée au chapitre 1.4.1 ci-dessus.

1.4.5.2. Mandataires de certification

Le Mandataire de Certification (MC) est une personne physique dûment identifiée, nommée par le demandeur et habilité à demander un certificat d'AC Intermédiaire ou Emettrice pour le compte du demandeur.

1.4.5.3. Opérateur de certification

La Banque de France s'appuie sur un acteur externe pour la mise à disposition et l'exploitation de son IGC. Cet acteur endosse le rôle d'Opérateur de Certification (OC) et dispose de l'expertise nécessaire pour prendre en charge les services permettant d'assurer la génération et la révocation des certificats.

L'OC est en charge du bon fonctionnement de l'IGC, de la sécurité des moyens techniques ainsi que de la sécurité des personnels et des locaux.

1.5. Usage des certificats

1.5.1. Domaines d'utilisation applicables

1.5.1.1. Bi-clefs et certificats des AC Intermédiaires et Emettrices

L'autorité de certification « Banque de France AC v3 Racine » délivre exclusivement des certificats d'AC Intermédiaires et Emettrices à la Banque de France ou à ses filiales.

La bi-clef d'une AC Intermédiaire ou Emettrice est utilisée uniquement pour :

- Signer les certificats qu'elle émet ;
- Signer les listes des AC révoquées (LAR) qu'elle émet (cas d'une AC Intermédiaire) ;
- Signer les listes des certificats révoquées (LCR) qu'elle émet (cas d'une AC Emettrice) ;
- Signer les certificats des répondeurs OCSP qu'elle émet.

1.5.1.2. Bi-clefs et certificats d'AC et de ses composantes

La bi-clef de l'autorité de certification « Banque de France AC v3 Racine » est utilisée uniquement pour :

- signer les certificats d'AC Emettrices qu'elle émet ;
- signer les listes des AC révoqués (LAR) qu'elle émet ;
- signer les certificats des répondeurs OCSP qu'elle émet.

1.5.2. Domaines d'utilisation interdits

La Banque de France décline toute responsabilité dans l'usage fait d'un certificat dans un cadre autre que l'usage prévu aux paragraphes 1.5.1.1 et 4.5.

1.6. Gestion des politiques de certification

1.6.1. Entité gérant les politiques de certification

La PC de l'autorité de certification « Banque de France AC v3 Racine » est élaborée et mise à jour par le Responsable de la sécurité de l'information de la Banque de France.

Cette PC est soumise à l'approbation du Comité d'approbation des politiques de certification (CAPC – cf. chapitre 1.6.2) notamment pour :

- valider les usages et restrictions d'usage des certificats émis par cette AC ;
- vérifier sa conformité aux évolutions technologiques et aux exigences fonctionnelles ou légales et réglementaires.

Un tableau indiquant les différentes versions de la PC, les dates de révisions et les principales modifications apportées par rapport à sa version antérieure est présenté en page 2 du présent document.

1.6.2. Point de contact de la politique de certification

Les coordonnées de la personne et du CAPC en charge de l'élaboration de la PC sont les suivantes.

Responsable de la sécurité de l'information	RSI Banque de France 39 rue croix des petits champs 75001 Paris email : 1206-crypto-ut@banque-france.fr
Comité d'approbation des politiques de certification, présidé par le RSI	RSI Banque de France 39 rue croix des petits champs 75001 Paris email : 1206-crypto-ut@banque-france.fr

1.6.3. Entité gérant la conformité de la DPC avec les PC

L'entité gérant la conformité de la DPC avec la présente politique de certification est le RSI de la Banque de France.

1.6.4. Procédures d'approbation de la conformité de la DPC

L'entité approuvant la conformité de la DPC avec les PC Banque de France est le Comité d'approbation des politiques de certification (CAPC – cf. chapitre 1.6.2).

2. Responsabilités concernant la mise à disposition des informations devant être publiées

2.1. Entités chargées de la mise à disposition des informations

Le RSI de la Banque de France est responsable de la mise à disposition des informations publiées.

2.2. Informations publiées

L'AC publie les informations suivantes à destination des porteurs et des utilisateurs de certificats :

Information publiée	Emplacement de publication
PC de l'AC « *Banque de France AC v3 Racine* »	• http://pc.igcv3.certificats.banque-france.fr
Certificats de chaine de confiance	Les certificats de la chaine de confiance sont publiés sur le site de publication : • http://pc.igcv3.certificats.banque-france.fr Le certificat de l'AC « *Banque de France AC v3 Racine* » y est publié. Pour permettre aux utilisateurs de s'assurer de l'origine des certificats, leurs empreintes sont également publiées sur le site de publication : • Empreinte du certificat de l'AC « *Banque de France AC v3 Racine* » : 1f2cb835935ab103922f3a96c0c03fa2764f2a46
LAR de l'AC « *Banque de France AC v3 Racine* »	• 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
Répondeur OCSP de l'AC « *Banque de France AC v3 Racine* »	• http://ocsp.igcv3.certificats.banque-france.org/racine-1.2.250.1.115.200.3.5.1.1.1 • http://ocsp.igcv3.certificats.banque-france.fr/racine-1.2.250.1.115.200.3.5.1.1.1

Tableau 3 – Liste des informations publiées

L'intégrité des données publiées est assurée par la publication des empreintes numériques de ces données.

2.3. Délais et fréquence de publication

Les informations documentaires publiées (*PC, …*) sont mises à jour dès que nécessaire afin que soit assurée la cohérence entre les informations publiées et les engagements et pratiques effectifs de l'AC.

Le certificat d'AC Racine est diffusé préalablement à toute diffusion de certificats et/ou de LCR/LAR correspondantes. Les délais et la fréquence de mise à jour des LCR sont détaillés aux chapitres 4.9.7 et 4.9.8.

Les systèmes publiant ces informations sont disponibles 7j/7 et 24h/24.

2.4. Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est en accès libre et gratuit. Le personnel chargé des ajouts, modifications, suppressions des données publiées est spécifiquement habilité à réaliser l'opération et accède aux systèmes de publication des informations au travers d'un contrôle d'accès fort (*authentification au moins à 2 facteurs*).

3. Identification et authentification

L'authentification a pour objet de vérifier l'identité dont une entité (personne ou machine) se prévaut. Elle est précédée par une identification de l'entité qui permet à cette dernière de se faire reconnaitre du système

3.1. Nommage

3.1.1. Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500.

Dans chaque certificat, l'AC Racine et l'AC Intermédiaire ou Emettrice sont identifiées par un « Distinguished Name » (*au sens de la norme X.501*). Les données d'identification de l'AC Intermédiaire ou Emettrice figurent dans le champ « Objet » (*« Subject » en anglais*) du certificat ; les données d'identification de l'AC Racine figurent dans le champ « Émetteur » (*« Issuer » en anglais*).

3.1.2. Nécessité d'utilisation de noms explicites

Les noms choisis sont explicites.

3.1.2.1. Identité de l'AC Racine

L'identification de l'AC Racine se fait en utilisant le DN dont la composition est décrite ci-dessous :

Attribut du DN	**Valeur**
Country (C)	Pays de résidence de l'entité responsable de l'AC Racine
OrganizationName (O)	Nom officiel complet de l'entité responsable de l'AC Racine
OrganizationIdentifier (OI)	Numéro d'immatriculation officiel de l'entité responsable de l'AC Racine 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.
OrganizationalUnitName (OU)	Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité responsable de l'AC Racine : 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.
CommonName (CN)	Nom significatif de l'AC Racine

3.1.2.2. Identité de l'AC Intermédiaire ou Emettrice

L'identification des AC Intermédiaires et Emettrices se fait en utilisant le DN dont la composition est décrite ci-dessous :

Attribut du DN	Valeur
Country (C)	Pays de résidence de l'entité responsable de l'AC Intermédiaire ou Emettrice
OrganizationName (O)	Nom officiel complet de l'entité responsable de l'AC Intermédiaire ou Emettrice
OrganizationIdentifier (OI)	Numéro d'immatriculation officiel de l'entité responsable de l'AC Intermédiaire ou Emettrice 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.
OrganizationalUnitName (OU)	Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité responsable de l'AC Intermédiaire ou Emettrice : 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.
CommonName (CN)	Nom significatif de l'AC Intermédiaire ou Emettrice

3.1.2.3. Certificats de test

Sans objet.

3.1.3. Anonymisation ou pseudonymisation des services applicatifs

L'anonymisation ou l'utilisation des pseudonymes dans les certificats émis n'est pas autorisée par l'AC.

3.1.4. Règles d'interprétation des différentes formes de noms

Tous les caractères sont au format UTF8String ou PrintableString.

3.1.5. Unicité des noms

Le champ DN Subject identifie une AC Intermédiaire ou Emettrice de façon unique au sein du domaine de l'IGCv3.

3.1.6. Identification, authentification et rôle des marques déposées

L'AC ne peut voir sa responsabilité engagée en cas d'utilisation illicite des marques déposées, des marques notoires et des signes distinctifs.

3.2. Validation initiale de l'identité

3.2.1. Méthode pour prouver la possession de la clef privée

Pour un certificat d'AC Intermédiaire et Emettrice, la bi-clef est générée sous le contrôle de l'OC. Le demandeur prouve la possession de la clef privée en transmettant à l'AC Racine une requête signée avec la clef privée générée.

3.2.2. Validation de l'identité d'un organisme

Les certificats des AC Intermédiaires et Emettrices sont délivrés exclusivement à la Banque de France ou à ses filiales.

L'AE vérifie toutefois l'identification de l'organisme, de son représentant légal et de toutes personnes désignées par ce dernier, directement ou indirectement, pour le représenter vis-à-vis de l'AC Racine ou de l'AE.

Le cas échéant, les informations d'enregistrement sont archivées par l'AC Racine ou par l'AE.

3.2.3. Validation de l'identité d'un individu

Sans objet.

3.2.4. Informations non vérifiées

Sans objet.

3.2.5. Validation de l'autorité du demandeur

Une demande de certificat d'AC Intermédiaire ou Emettrice ne peut être réalisée que par un personnel habilité, de Banque de France ou d'une de ses filiales, à demander un certificat d'AC Intermédiaire ou Emettrice sur l'IGCv3 pour le compte du demandeur.

3.2.6. Critères d'interopérabilité, certification croisée d'AC

Les demandes d'accords et les accords de reconnaissance avec des AC extérieures sont étudiés par le RSI et soumis pour approbation au CAPC.

3.3. Identification et validation d'une demande de renouvellement des clefs

Le renouvellement de la bi-clef d'une AC Intermédiaire ou Emettrice entraîne automatiquement la génération et la fourniture d'un nouveau certificat.

Un nouveau certificat ne peut pas être fourni à une AC Intermédiaire ou Emettrice sans renouvellement de la bi-clef correspondante (cf. chapitre 4.6).

3.3.1. Identification et validation pour un renouvellement courant

La procédure d'identification et de validation de toute demande de renouvellement est identique à la procédure d'enregistrement initiale.

3.3.2. Identification et validation pour un renouvellement des clefs après révocation

Suite à la révocation définitive d'un certificat d'AC Intermédiaire ou Emettrice, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initiale.

3.4. Identification et validation d'une demande de révocation

Pour des raisons précisées au chapitre 4.9.1, les certificats des AC Intermédiaires et Emettrices peuvent être révoqués.

La demande de révocation ne peut être effectuée que par l'entité ayant demandé initialement le certificat (*par l'intermédiaire du responsable de l'AC concernée*) auprès de l'AE de l'AC Racine.

4. Exigences opérationnelles sur le cycle de vie de certificats

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

Une demande de certificat d'AC Intermédiaire ou Emettrice ne peut être effectuée que par un représentant légal de la Banque de France ou toute personne habilitée et désignée par celui-ci (un MC) pour le compte de la Banque de France ou une de ses filiales.

4.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat

Une demande de certificat d'AC Intermédiaire ou Emettrice est établie par le représentant légal de l'entité responsable de l'AC ou par la personne désignée par celui-ci.

La demande est spécifiée auprès de l'AC Racine qui sera en charge d'établir un document de cérémonie des clefs décrivant les conditions de génération et d'émission du certificat d'AC Intermédiaire ou Emettrice.

4.2. Traitement d'une demande de certificat

4.2.1. Exécution des processus d'identification et de validation de la demande

L'AE contrôle l'identité et le pouvoir de la personne désignée par le représentant légal de l'entité responsable de l'AC.

4.2.2. Acceptation ou rejet de la demande

Une demande de certificat d'AC Intermédiaire ou Emettrice est acceptée ou rejetée par l'AE.

En cas de rejet de la demande, l'AE en informe le MC en indiquant les raisons du rejet.

En cas d'acceptation de la demande, une cérémonie des clefs est organisée pour l'émission du certificat d'AC Intermédiaire ou Emettrice.

4.2.3. Durée d'établissement du certificat

Le certificat d'une AC Intermédiaire ou Emettrice est émis durant la cérémonie des clefs.

4.3. Délivrance du certificat

Lorsque la demande est validée par l'AE, une cérémonie des clefs est organisée et planifiée pour générer le certificat de l'AC Intermédiaire ou Emettrice.

4.3.1. Actions de l'AC concernant la délivrance du certificat

Pour toute demande de certificat d'AC Intermédiaire ou Emettrice, l'AC Racine effectue les opérations suivantes :

- Vérification de la conformité entre les informations de l'AC Intermédiaire ou Emettrice du futur certificat et le document de cérémonie des clefs ;
- Signature du certificat de l'AC Intermédiaire ou Emettrice ;
- Vérification du contenu du certificat généré ;

4.3.2. Notification par l'AC de la délivrance du certificat

Le certificat de l'AC Intermédiaire ou Emettrice est remis à son représentant (*MC ou représentant légal*) au cours de la cérémonie des clefs. La signature du procès-verbal (PV) de cérémonie des clefs atteste de la remise du certificat.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

La signature du PV de cérémonie des clefs vaut acceptation du certificat.

4.4.2. Publication du certificat

Les certificats des AC Intermédiaire et Emettrice de la Banque de France et de ses filiales sont publiés (*tels que définis au paragraphe 2.2*).

4.4.3. Notification par l'AC aux autres entités de la délivrance du certificat

Sans objet.

4.5. Usages de la bi-clef et du certificat

4.5.1. Utilisation de la clef privée et du certificat par l'AC Intermédiaire/Emettrice

L'utilisation de la clef privée et du certificat associé est décrite au chapitre 1.5.1, de façon limitative. Dans le cas contraire, leur responsabilité pourrait être engagée, et le certificat associé pourrait être révoqué.

L'usage autorisé de la clef privée et du certificat associé est par ailleurs indiqué dans le certificat lui-même, dans les extensions concernant les usages des clefs et limités :

- à « *keyCertSign* » et « *cRLsign* » pour la signature de certificats et de LCR,

4.5.2. Utilisation de la clef publique et du certificat par l'utilisateur du certificat

Les utilisateurs de certificats ne doivent les utiliser que dans les domaines d'utilisation spécifiés au chapitre 1.5.1. Les utilisateurs s'engagent à respecter strictement ces domaines d'utilisation. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé du certificat est indiqué dans le certificat dans les extensions concernant les usages des clefs.

4.6. Renouvellement (au sens RFC 3647) d'un certificat

Les certificats seuls ne sont jamais renouvelés au sens de la RFC 3647 (*on entend par renouvellement au sens RFC 3647 la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations étant identiques au certificat précédent, y compris la clef publique de l'AC Intermédiaire ou Emettrice*). La génération d'une nouvelle bi-clef est systématique pour toute délivrance d'un certificat.

4.7. Délivrance d'un nouveau certificat suite à un changement de bi-clef

4.7.1. Causes possibles de changement d'une bi-clef

Les bi-clefs des AC Intermédiaire et Emettrice ainsi que les certificats correspondants sont renouvelées au minimum tous les 17 ans.

Par ailleurs, une bi-clef et un certificat peuvent être renouvelés :

- par anticipation (*ex : pour minimiser les possibilités d'attaques cryptographiques*),
- ou suite à la révocation du certificat d'une AC Intermédiaire ou Emettrice (*cf. chapitre 4.9*).

Nota – Dans la suite du présent chapitre, le terme « fourniture d'un nouveau certificat » couvre également la fourniture d'un nouveau bi-clef à l'AC Intermédiaire ou Emettrice.

4.7.2. Origine d'une demande d'un nouveau certificat

Le traitement d'un nouveau certificat est identique à celui d'une demande initiale (*cf. chapitre 4.1.1*).

4.7.3. Procédure de traitement d'une demande d'un nouveau certificat

La procédure de traitement d'une demande d'un nouveau certificat est identique à la procédure d'une demande initiale (*cf. chapitre 4.2*).

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont régies par les dispositions du chapitre 4.3.1.

4.7.4. Notification de l'établissement du nouveau certificat

Cf. chapitre 4.3.2.

4.7.5. Démarche d'acceptation du nouveau certificat

Cf. chapitre 4.4.1.

4.7.6. Publication du nouveau certificat

Cf. chapitre 4.4.2.

4.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Cf. chapitre 4.4.3.

4.8. Modification d'un certificat

On entend par *modification d'un certificat* des modifications d'informations sans changement de la clef publique (cf. chapitre 4.7) et autres qu'uniquement la modification des dates de validité (cf. chapitre 4.6), comme défini dans la RFC 3647.

La modification de certificat n'est pas autorisée. Toute demande de modification se traduit par une demande de nouveau certificat, détaillée au chapitre 4.2.

4.9. Révocation et suspension des certificats

4.9.1. Causes possibles d'une révocation

Lorsque l'une des circonstances ci-dessous se réalise et que l'AC en a connaissance (*elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment*), le certificat concerné est révoqué et son numéro de série placé dans la Liste de certificats révoqués (LCR).

Toute demande de révocation peut être motivée par l'un des cas prévus à l'article 4.9.1.1 (*le cas échéant, cette cause n'est pas publiée, cf. chapitre 4.9.3.1*).

4.9.1.1. Certificats d'AC Intermédiaire/Emettrice

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'une AC Intermédiaire ou Emettrice :

- Les informations figurant dans le certificat ne sont pas ou plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- L'AC Intermédiaire ou Emettrice n'a pas respecté les modalités applicables d'utilisation du certificat ;
- L'AC Intermédiaire ou Emettrice n'a pas respecté ses obligations découlant de la PC dont le certificat dépend ;
- Une erreur (*intentionnelle ou non*) a été détectée dans le dossier de l'AC Intermédiaire ou Emettrice ;
- La clef privée associée au certificat de l'AC Intermédiaire ou Emettrice est suspectée de compromission, est compromise, est perdue ou volée (*éventuellement les données d'activation associées*) ;
- Le représentant légal de l'AC Intermédiaire ou Emettrice ou le MC le cas échéant demande la révocation du certificat ;
- La cessation d'activité de l'entité l'AC Intermédiaire ou Emettrice.

Dès lors qu'une des circonstances ci-dessus se réalise et que l'AC Racine en a connaissance, le certificat doit être révoqué.

4.9.1.2. Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (*y compris un certificat d'AC pour la génération de certificats, de LCR et LAR, de réponses OCSP*) :

- suspicion de compromission, compromission, perte ou vol de la clef privée de la composante ;
- décision de changement de composante de l'IGC suite à une détection de non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (*par exemple suite à un audit de qualification ou de conformité négatif*) ;
- cessation d'activité de l'entité opérant la composante ;
- migration de la composante sur une autre solution technique incompatible avec la première.

4.9.2. Origine d'une demande de révocation

4.9.2.1. Certificats d'AC Intermédiaire/Emettrice

Les personnes et entités habilitées à demander une révocation de certificat sont :

- Un représentant légal (RL) ou un MC de l'entité responsable de l'AC Intermédiaire ou Emettrice,
- L'AC Racine,
- L'AE rattachée à l'AC Racine.

4.9.2.2. Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC (le RSI), ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

4.9.3. Procédure de traitement d'une demande de révocation

4.9.3.1. Certificats d'AC Intermédiaire/Emettrice

À la réception d'une demande de révocation, l'AE vérifie l'identité du demandeur et la validité de la demande, selon les exigences décrites au paragraphe 3.3.2.

La demande de révocation doit au moins comporter les informations suivantes :

- l'identité de l'AC Intermédiaire ou Emettrice figurant dans le certificat ;
- le nom de l'entité responsable de l'AC Intermédiaire ou Emettrice ;
- le nom du demandeur de la révocation (représentant légal ou MC) ;
- une information permettant de retrouver rapidement et sans erreur le certificat à révoquer (*par défaut le n° de série*).

Si la demande est recevable, l'AC Racine organise une cérémonie des clefs pour :

- Signer une nouvelle LAR contenant le numéro de série du certificat de l'AC Intermédiaire ou Emettrice révoquée,
- Détruire les clefs de l'AC Intermédiaire ou Emettrice révoquée.

Si la demande n'est pas recevable, le demandeur en est informé.

L'opération de révocation est enregistrée dans les journaux d'événements de l'AC « Banque de France AC v3 Racine ». Les demandes de révocation sont enregistrées et archivées.

Les causes de révocation définitive des certificats ne sont pas publiées.

4.9.3.2. Certificats d'une composante de l'IGC

En cas de révocation du certificat de l'AC « Banque de France AC v3 Racine » appartenant à la chaîne de confiance d'un certificat, les actions suivantes sont à réaliser :

- Informer l'ensemble des AC Intermédiaires et Emettrices concernées dans les plus brefs délais que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide ;
- Informer tous les organismes référençant une des offres émises par l'AC ;
- Informer le point de contact identifié de l'ANSSI.

4.9.4. Délai accordé à l'AC Intermédiaire/Emettrice pour formuler la demande de révocation

Dès que le MC (*ou une personne autorisée*) a connaissance de la survenance d'une des causes possibles de révocation, de son ressort, il (elle) doit formuler sa demande de révocation sans délai.

4.9.5. Délai de traitement par l'AC d'une demande de révocation

4.9.5.1. Certificats d'AC Intermédiaire/Emettrice

Dès lors qu'une demande de révocation d'AC Intermédiaire ou Emettrice est authentifiée et validée, l'AC Racine met tous les moyens en œuvre pour organiser une cérémonie des clefs dans les meilleurs délais.

4.9.5.2. Certificats d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un événement constituant une cause de révocation possible pour ce type de certificat. La révocation du certificat est effective lorsque le

numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat, et que cette liste est accessible au téléchargement.

La révocation d'un certificat de signature de l'AC (*signature de certificats, de LCR / LAR, de réponses OCSP*) est effectuée immédiatement, particulièrement s'il s'agit d'un cas de compromission de clef.

4.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

La Banque de France met à disposition des utilisateurs de certificats un répondeur OCSP, des listes de certificats révoqués (LCR) et des listes d'autorités révoquées (LAR) tous précisés au chapitre 2.2.

L'utilisateur d'un certificat est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. Le choix de la méthode utilisée (LCR, OCSP) est à l'appréciation de l'utilisateur.

4.9.7. Fréquence d'établissement des LCR

Les LAR sont générées au maximum toutes les 24 heures.

4.9.8. Délai maximum de publication d'une LCR

La LAR est publiée dans un délai maximum de 30 min suivant sa génération.

4.9.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Un service de vérification en ligne du statut des certificats (OCSP) est mis à disposition des utilisateurs par la Banque de France. Ses caractéristiques en termes d'intégrité, de disponibilité et de délai de publication sont les mêmes que celles du service de publication de LCR.

En cas d'indisponibilité du service OCSP, les utilisateurs peuvent consulter le statut des certificats à partir des points de distribution de la LAR.

4.9.10. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Cf. chapitre 4.9.6.

4.9.11. Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12. Exigences spécifiques en cas de compromission de la clef privée

En cas de compromission de clef privée, les actions suivantes sont entreprises :

Cas des certificats d'AC Intermédiaire ou Emettrice

Les entités (cf. chapitre 4.9.2) autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clef privée.

Cas des certificats d'AC

Outre les actions énumérées au chapitre 4.9.3.2, la révocation suite à une compromission de la clef privée fait l'objet d'une information clairement diffusée sur le site http://pc.igcv3.certificats.banque-france.fr et éventuellement relayée (*en liaison avec la Direction de la communication de la Banque de France*) par d'autres moyens, par exemple, communiqué de presse, publication sur le site institutionnel de la Banque de France.

Une information est diffusée auprès du point de contact identifié de l'ANSSI.

4.9.13. Causes possibles d'une suspension

Sans objet. La suspension de certificat n'est pas prévue pour les AC de la Banque de France.

4.9.14. Origine d'une demande de suspension

Sans objet. La suspension de certificat n'est pas prévue pour les AC de la Banque de France.

4.9.15. Procédure de traitement d'une demande de suspension

. Sans objet. La suspension de certificat n'est pas prévue pour les AC de la Banque de France.

4.9.16. Limites de la période de suspension d'un certificat

Sans objet. La suspension de certificat n'est pas prévue pour les AC de la Banque de France.

4.10. Fonction d'information sur l'état des certificats

4.10.1. Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats a pour but de permettre aux utilisateurs de vérifier le statut d'un certificat et de sa chaîne de certification, c'est à dire vérifier également les signatures des certificats de la chaîne et les signatures garantissant l'origine et l'intégrité des LCR / LAR.

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs un mécanisme de consultation libre de LCR et LAR. Ces LCR et LAR sont au format LCRv2, publiées électroniquement aux URL définies au paragraphe 2.2. Ces adresses figurent également dans le champ « Point de Distribution des LCR » de chaque certificat.

4.10.2. Disponibilité de la fonction

Le tableau suivant présente les engagements en termes de disponibilité de la fonction d'information sur l'état des certificats.

Disponibilité du service	24h/24h, 7j/7j
Durée maximale d'indisponibilité par interruption de service	4h
Durée maximale total d'indisponibilité par mois	8h
Temps de réponse maximal à une requête OCSP	6s

Tableau4 – Disponibilité de la fonction d'information sur l'état des certificats

4.10.3. Dispositifs optionnels

Sans objet.

4.11. Fin de la relation entre l'AC Intermédiaire/Emettrice et l'AC Racine

En cas de fin de relation contractuelle entre l'AC Racine et l'AC Intermédiaire ou Emettrice, le certificat de ce dernier est révoqué.

4.12. Séquestre de clef et recouvrement

Sans objet. Le séquestre n'est pas permis par l'AC.

4.12.1. Politiques et pratiques de recouvrement par séquestre des clefs

Sans objet.

4.12.2. .Politiques et pratiques de recouvrement par encapsulation des clefs de session

Sans objet.

5. Mesures de sécurité non techniques

Les différentes mesures et contrôles décrits dans ce chapitre visent à assurer un niveau de confiance fort dans le fonctionnement de l'IGC.

5.1. Mesures de sécurité physique

Les mesures de sécurité physique sont dictées par le respect des règles et normes documentées au sein des services informatiques de la Banque de France (Politiques locales de sécurité internes à la Banque de France).

Les Politiques locales de sécurité sont citées dans la DPC.

Par ailleurs, pour les services que l'OC exploite, ce dernier a conduit une analyse de risques ayant permis d'identifier les mesures de sécurité décrites dans le présent chapitre.

5.1.1. Situation géographique et construction des sites

La construction des sites respecte les règlements et normes en vigueur.

5.1.2. Accès physiques

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'AC, les accès aux locaux des différentes composantes de l'IGC sont contrôlés. En outre, toute personne entrant dans ces zones physiquement sécurisées reste accompagnée par une personne autorisée.

Pour les fonctions de génération des certificats, de génération des éléments secrets de l'AC Intermédiaire ou Emettrice et de gestion des révocations, l'accès est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux, et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, les composantes concernées de l'IGC définissent un périmètre de sécurité physique où sont installées ces machines. La mise en œuvre de ce périmètre permet de respecter la séparation des rôles de confiance telle que prévue dans cette PC. Notamment, tout local utilisé en commun avec d'autres fonctions que les fonctions rendues par la composante concernée se situe en dehors de ce périmètre de sécurité.

Nota – On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisés pour la mise en œuvre de ces fonctions.

5.1.3. Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'IGC, et les engagements en matière de disponibilité des différentes fonctions de l'AC, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.4. Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences de la présente PC, et les engagements en matière de disponibilité des différentes fonctions de l'AC, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.5. Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences de la présente PC, et les engagements en matière de disponibilité des différentes fonctions de l'AC, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.6. Conservation des supports

Les différentes informations intervenant dans les activités de l'IGC sont identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité). L'AC maintient un inventaire de ces informations. L'AC met en place des mesures pour éviter la compromission et le vol de ces informations. Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils sont manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés. Des procédures de gestion protègent ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

5.1.7. Mise hors service des supports

En fin de vie, les supports sont, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes. Les procédures et moyens de destruction et de réinitialisation sont conformes à ce niveau de confidentialité.

5.1.8. Sauvegardes hors site

En complément de sauvegardes sur sites, les composantes de l'IGC mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes sont organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conforme aux exigences et engagements de la présente PC. Les informations sauvegardées hors site respectent les exigences de la présente PC en matière de protection en confidentialité et en intégrité de ces informations.

Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats mettent en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.). Les fonctions de sauvegarde et de restauration sont effectuées par les rôles de confiance appropriés et conformément aux mesures de sécurité procédurales.

5.2. Mesures de sécurité procédurales

Ces mesures permettent d'assurer que les tâches liées aux fonctions essentielles de l'IGC sont réparties entre plusieurs personnes.

Des contrôles de procédures sont mis en place pour chacune des entités de l'IGC. Elles sont détaillées dans la DPC et couvrent les thèmes suivants :

- rôles de confiance ;
- nombre de personnes requises par tâches ;
- identification et authentification pour chaque rôle ;
- rôles exigeant une séparation des attributions.

5.2.1. Rôles de confiance

L'AC distingue au moins les cinq rôles fonctionnels de confiance suivants :

- **Responsable de sécurité :** Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est responsable des opérations de génération et de révocation des certificats.
- **Responsable d'application :** Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'I.G.C. au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
- **Ingénieur système :** Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
- **Opérateur :** Un opérateur au sein d'une composante de l'I.G.C. réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
- **Contrôleur :** Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'I.G.C. et aux politiques de sécurité de la composante.

En plus de ces rôles de confiance, l'AC a défini le rôle de **Porteur de part de secret**. Le Porteur de part de secret a la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité de la part qui lui a été confiée.

5.2.2. Nombre de personnes requises par tâches

Suivant le type d'opération/tâche à effectuer, la présence d'une ou de plusieurs personnes disposant de rôles spécifiques est nécessaire.

Le nombre et la qualité des personnes requis par tâche sont précisés dans la DPC.

5.2.3. Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC fait vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants. Notamment, elle fait vérifier :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle,
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes,
- le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes,
- éventuellement, que des clefs cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.

Ces contrôles sont conformes à la politique de sécurité de la composante.

5.2.4. Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul sont respectées. Les attributions associées à chaque rôle sont conformes à la politique de sécurité de la composante concernée.

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et responsable d'exploitation / opérateur,
- contrôleur et tout autre rôle,
- ingénieur système et opérateur.

5.3. Mesures de sécurité vis-à-vis du personnel

Des contrôles effectués sur le personnel intervenant sur l'IGC sont mis en place pour chacune des entités de l'IGC. Elles sont détaillées dans la DPC et couvrent les aspects suivants :

- qualifications, compétences et habilitations requises ;
- procédures de vérification des antécédents ;
- exigences en matière de formation initiale ;
- exigences et fréquence en matière de formation continue ;
- fréquence et séquence de rotation entre différentes attributions ;
- sanctions en cas d'actions non autorisées ;
- exigences vis-à-vis du personnel des prestataires externes ;
- documentation fournie au personnel.

De plus, les individus contribuant aux tâches de l'AC ou de l'AE doivent être libres de tout conflit d'intérêt vis-à-vis de l'AC.

Les éventuels conflits d'intérêt sont traités pour les agents de la Banque de France selon les règles internes.

Les éventuels conflits d'intérêt pour les personnes extérieures à la Banque de France et intervenant dans les rôles de confiance de l'IGC sont traités, par le correspondant métier, selon les bonnes pratiques du domaine.

5.3.1. Qualifications, compétences et habilitations requises

Toute personne amenée à travailler au sein de l'IGC est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles.

Toute personne intervenant au sein de l'AC est informée de ses responsabilités relatives aux services de l'IGC et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2. Procédures de vérification des antécédents

L'AC et chaque composante de l'IGC mettent en œuvre les moyens légaux pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de l'IGC ou d'une de ses composantes.

La vérification d'antécédents est réalisée préalablement à l'affectation d'un rôle de confiance à un personnel. Elle porte notamment sur le bulletin n°3 du casier judiciaire du personnel qui doit être fourni à l'employeur avant l'attribution du rôle.

Les personnes ayant un rôle de confiance ne souffrent d'aucun conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

5.3.3. Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité correspondants à la composante au sein de laquelle il opère.

5.3.4. Exigences et fréquence en matière de formation continue

En fonction de la nature des évolutions (*liées au systèmes, aux procédures, à l'organisation,* …), le personnel concerné reçoit une formation appropriée préalablement à toute évolution.

5.3.5. Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6. Sanctions en cas d'actions non autorisées

Des sanctions en cas d'actions non autorisées par la PC/DPC de l'AC et les procédures établies ainsi que les processus et procédures internes à l'IGC, soit par négligence, soit par malveillance, sont prévues.

5.3.7. Exigences vis-à-vis du personnel des prestataires

Le personnel des prestataires intervenant sur les composantes de l'IGC respecte les exigences de l'AC. Ces exigences sont traduites en clauses adéquates dans les contrats avec ces prestataires.

5.3.8. Documentation fournie au personnel

Le personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques (*notamment la PC*) et pratiques générales (*notamment la DPC et les procédures opérationnelles*) de la composante au sein de laquelle il travaille.

5.4. Procédures de constitution des données d'audit

Des journaux d'événements sont constitués pour rendre possibles la traçabilité et l'imputabilité des opérations effectuées. Ces journaux sont protégés en authenticité et en intégrité, et font l'objet de règles strictes d'exploitation décrites dans la DPC qui couvrent notamment les points suivants :

- types d'événements à enregistrer ;
- fréquence de traitement des journaux d'événements ;
- période de conservation des journaux d'événements ;
- protection des journaux d'événements ;
- procédure de sauvegarde des journaux d'événements ;
- système de collecte des journaux d'événements ;
- notification de l'enregistrement d'un événement au responsable de l'événement ;
- évaluation des vulnérabilités.

5.4.1. Type d'évènements à enregistrer

Chaque entité opérant une composante de l'IGC journalise, au minimum, les événements tels que décrit ci-dessous sous forme électronique. La journalisation est automatique depuis le démarrage du système et sans interruption jusqu'à son arrêt.

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.),
- démarrage et arrêt des systèmes informatiques et des applications,
- traces d'activité (logs) des pare-feux et des routeurs,
- événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à la défaillance de la fonction de journalisation, pannes logicielles et matérielles,
- connexion / déconnexion des Utilisateurs ayant des rôles de confiance, et des tentatives non réussies correspondantes,

5.4.1.1. Informations enregistrées pour chaque évènement

Chaque enregistrement d'un événement dans un journal contient les champs suivants :

- type de l'événement,
- nom de l'exécutant ou référence du système déclenchant l'événement,

- date et heure de l'événement,
- résultat de l'événement (échec ou réussite).

5.4.1.2. Evènements enregistrés par l'AE

Les évènements enregistrés par l'AE sont les suivants :

- réception d'une demande de certificat (initiale et renouvellement),
- validation / rejet d'une demande de certificat,
- réception d'une demande de révocation,
- validation / rejet d'une demande de révocation,
- transmission du certificat à l'entité responsable de l'AC Intermédiaire ou Emettrice,
- accusé de réception de l'entité responsable de l'AC Intermédiaire ou Emettrice
- acceptation ou rejet explicite par l'entité responsable de l'AC Intermédiaire ou Emettrice,

5.4.1.3. Evènements enregistrés par l'AC

Les évènements enregistrés par l'AC sont les suivants :

- événements liés aux clefs de signature et aux certificats d'AC (génération, sauvegarde / récupération, destruction, …),
- génération des bi-clefs d'AC Intermédiaire ou Emettrice,
- génération des certificats d'AC Intermédiaire ou Emettrice,
- personnalisation des supports et génération des codes d'activation,
- publication et mise à jour des informations liées aux AC (*PC/DPC, certificats d'AC, …*)
- génération puis publication des LAR,
- requêtes et réponses OCSP.

5.4.1.4. Evènements divers

D'autres évènements sont également recueillis. Il s'agit d'évènements concernant la sécurité qui ne sont pas produits automatiquement par les systèmes mis en œuvre :

- les accès physiques,
- les actions de maintenance et de changements de la configuration des systèmes,
- les changements apportés au personnel ayant des rôles de confiance,
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clefs*, données d'activation, mots de passe, …*).

5.4.1.5. Imputabilité

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'événements.

Suivant le type d'événement concerné, les champs suivants peuvent être enregistrés :

- destinataire de l'opération,
- nom ou identifiant du demandeur de l'opération ou référence du système effectuant la demande,
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes),
- cause de l'événement,
- toute information caractérisant l'événement (par exemple pour la génération d'un certificat, son numéro de série).

Les opérations de journalisation sont effectuées au cours du processus concerné. En cas de saisie manuelle, l'écriture s'effectue, sauf exception, le même jour ouvré que l'événement.

5.4.2. Fréquence de traitement des journaux d'évènements

Les journaux d'événements sont contrôlés et analysés suivant la fréquence définie au chapitre 5.4.8.

5.4.3. Période de conservation des journaux d'évènements

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.

5.4.4. Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements sont protégés en disponibilité (*contre la perte et la destruction partielle ou totale, volontaire ou non*).

Les systèmes générant les journaux d'événements sont synchronisés sur une source fiable de temps détaillée au chapitre 6.8.

5.4.5. Procédure de sauvegarde des journaux d'évènements

Les procédures de sauvegarde des journaux sont détaillées dans la DPC.

Les journaux d'évènements sont protégés en disponibilité (*contre la perte et la destruction partielle ou totale, volontaire ou non*).

Les systèmes générant les journaux d'événements sont synchronisés sur une source fiable de temps détaillée au chapitre 6.8.

5.4.6. Système de collecte des journaux d'évènements

Le système de collecte garantie le niveau de sécurité relatif à l'intégrité, la disponibilité et la confidentialité des journaux d'évènements.

5.4.7. Notification de l'enregistrement d'un évènement au responsable de l'évènement

Sans objet.

5.4.8. Évaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements sont contrôlés au moins 1 fois par jour, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité 1 fois par semaine et dès la détection d'une anomalie. Cette analyse donne lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.

Un rapprochement entre les différents journaux d'évènements de l'AE et de l'AC est effectué au moins 1 fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

5.5. Archivage des données

L'archivage est réalisé par l'autorité d'enregistrement et les AC dans le but d'assurer la continuité de service, l'auditabilité et la non-répudiation des opérations, la pérennité des journaux constitués par les différentes composantes de l'IGC, la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les mesures nécessaires sont mises en place par l'AE et l'AC afin que ces archives soient disponibles, ré-exploitables, protégées en intégrité et qu'elles fassent l'objet de règles strictes d'exploitation et de protection contre la destruction.

5.5.1. Types de données à archiver

Sont notamment archivés :

- les PC et les DPC successives,
- les LCR / LAR,
- les certificats ,
- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques,
- les accords contractuels avec d'autres AC,
- les récépissés ou notifications (à titre informatif),
- les justificatifs d'identité du représentant légal ou du MC et, le cas échéant, de leur entité de rattachement,
- les journaux d'événements des différentes entités de l'IGC.

Les données archivées sous forme électronique sont notamment dupliquées et stockées sur deux sites distincts.

5.5.2. Période de conservation des archives

Pour les dossiers de demande de certificat :

- les dossiers et les pièces justificatives sont archivés pour une durée de vingt ans à compter de la date d'acceptation du certificat.
- A l'expiration de la durée d'archivage, le dossier et les pièces justificatives font l'objet d'une destruction.

Pour les certificats et LAR émis par l'AC :

- les certificats et les LAR émis par l'AC sont conservés pendant une durée de vingt ans à compter de leur génération.
- A l'expiration de la durée d'archivage, les LAR font l'objet d'une destruction.

Pour les réponses OCSP :

- les réponses OCSP sont conservées pendant au moins trois mois à compter de leur date d'expiration.
- A l'expiration de la durée d'archivage, les réponses OCSP font l'objet d'une destruction.

Pour les journaux d'évènements :

- les journaux d'évènements sont conservés pendant vingt ans à compter de leur date de génération.
- A l'expiration de la durée d'archivage, les journaux d'événements font l'objet d'une destruction.

5.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives :

- sont protégées en intégrité,
- sont accessibles aux seules personnes autorisées,
- peuvent être relues ou exploitées,
- lisibles et exploitables sur l'ensemble de leur cycle de vie.

5.5.4. Procédure de sauvegarde des archives

Sans objet.

5.5.5. Exigences d'horodatage des données

Le chapitre 6.8 précise les exigences en matière de datation et d'horodatage.

5.5.6. Système de collecte des archives

Sans objet.

5.5.7. Procédures de récupération et de vérification des archives

Les archives papier ou électronique doivent pouvoir être récupérées par l'AC dans un délai de 2 jours ouvrés.

5.6. Changement de clef d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité des certificats signés par une AC se termine avant celle du certificat de cette AC.

En cas de changement de clef de l'AC, les procédures à appliquer sont décrites dans la DPC.

En cas de génération d'un nouveau bi-clef, seule la nouvelle clef privée est utilisée pour signer des certificats. Le certificat d'AC précédent reste utilisable pour valider les certificats émis précédemment, au moins jusqu'à expiration de tous les certificats signés avec la clef privée correspondante.

5.7. Reprise suite à compromission ou sinistre

Les procédures de récupération des composantes de l'IGC en cas de sinistre ou de compromission sont décrites dans la DPC.

5.7.1. Procédures de remontée et de traitement des incidents et des compromissions

Chaque entité agissant pour le compte de l'IGC met en œuvre des procédures de remontée d'incident et de traitement des incidents. Ceci est réalisé au travers de la sensibilisation et la formation des personnels et au travers de l'analyse des journaux d'événements.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clef privée de l'AC, l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui en informe immédiatement l'AC. Le cas de l'incident majeur est impérativement traité dès réception et la publication de l'information de révocation du certificat, s'il y a lieu, est faite dans la plus grande urgence, voire immédiatement, par tout moyen utile ou disponible.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses systèmes devient insuffisant pour son utilisation prévue restante, alors l'AC informe toutes les AC Intermédiaires/Emettrices et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords. De plus tous les certificats concernés sont révoqués.

Conformément aux obligations réglementaires, l'organe de contrôle national (l'ANSSI) est informé de tout incident de sécurité touchant l'AC et ses services dans les 24 (vingt-quatre) heures.

5.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Chaque composante de l'IGC dispose d'un plan de continuité d'activité et de service qui permet de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC/DPC, des engagements de l'AC.

5.7.3. Procédures de reprise en cas de compromission de la clef privée d'une composante

Chaque composante de l'IGC dispose d'un plan de continuité.

Dans le cas de compromission d'une clef d'AC, le certificat correspondant est immédiatement révoqué comme précisé au chapitre 4.9. De plus, l'AC respecte les engagements suivants :

- arrêter immédiatement l'utilisation de la clef de la composante compromise,
- informer sans délai: toutes les AC Intermédiaires et Emettrices et les tiers utilisateurs,
- indiquer sans délai que les certificats et les informations de statut de révocation délivrés en utilisant cette clef d'AC peuvent ne plus être valables.
- prévenir l'ANSSI de la compromission dans les 24 heures,
- le cas échéant procéder à un dépôt de plainte auprès des autorités compétentes selon leurs modalités.

5.7.4. Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC/DPC (cf. chapitre 5.7.2).

5.8. Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

5.8.1. Transfert d'activité ou cessation d'activité affectant une composante de l'IGC autre que l'AC

Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AC :

- a mis en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (*notamment, archivage des certificats des services applicatifs et des informations relatives aux certificats*) ;

- assure la continuité de la fonction de révocation (prise en compte d'une demande de révocation et publication des LAR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC.

L'AC prévient l'ensemble des entités de l'IGC, par note expresse, trois mois avant la date effective de cessation ou de transfert de d'activité.

L'AC prévient toutes les AC Intermédiaires et Emettrices par un moyen à sa discrétion avec un préavis de trois mois.

L'AC communique au point de contact de l'ANSSI :

- les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité, notamment les dispositifs mis en place en matière d'archivage (clefs et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC ;
- les modalités des changements survenus, l'inventaire et la mesure des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet événement ;
- un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les AC Intermédiaires et Emettrices ainsi qu'aux utilisateurs de certificats ;
- le cas échéant, les obstacles ou délais supplémentaires rencontrés dans le déroulement du processus.

Au terme des trois mois de préavis, si l'AC est en cessation d'activité, tous les certificats émis par cette AC seront révoqués.

Dans tous les cas, les procédures mises en œuvre pour l'archivage de l'AC sont décrites dans la DPC.

5.8.2. Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle. La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux 3 points ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LAR conformément aux engagements pris dans sa PC.

L'AC stipule dans ses pratiques les dispositions prises en cas de cessation de service ; elles incluent :

- la notification des entités affectées ;
- le transfert de ses obligations à d'autres parties ;
- la gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, une procédure permet de :

- s'interdire de transmettre la clef privée lui ayant permis d'émettre des certificats ;
- prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- révoquer le certificat de l'AC ;
- révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- informer toutes les AC Intermédiaires et Emettrices dont le certificat est révoqué ou à révoquer.

6. Mesures de sécurité techniques

6.1. Génération et installation de bi-clefs

6.1.1. Génération des bi-clefs

6.1.1.1. Clefs d'AC

Les bi-clefs d'AC sont générées sur des HSM (*Hardware Security Module : modules cryptographiques matériels sécurisés*) selon une procédure formelle appelée « *Key Ceremony* » ou « cérémonie de clefs ».

L'initialisation de l'IGC et/ou la génération des clefs de signature d'AC s'accompagne de la génération de secrets d'IGC.

Ces parts de secrets sont générées suivant un schéma à seuil de Shamir (*n parties parmi m sont nécessaires et suffisantes pour reconstituer le secret*) permettant de déclencher le chargement sécurisé, dans un nouveau module cryptographique, de la clef privée de l'AC Racine sauvegardée lors de la cérémonie de clefs.

Suite à leur génération, les parts de secrets sont remis à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC Racine. Chaque part de secrets est mise en œuvre par son porteur.

Les cérémonies de clefs se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins deux sont externes à l'AC et sont impartiaux. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. Dans la mesure du possible, un des témoins est un officier public (huissier ou notaire). L'environnement utilisé garantit la confidentialité et l'intégrité des clefs privées d'AC.

6.1.1.2. Clefs d'AC Intermédiaire/Emettrice générées par l'AC Racine

Les bi-clefs d'AC Intermédiaire et Emettrice sont générées sur des HSM (*Hardware Security Module : modules cryptographiques matériels sécurisés*) selon une procédure formelle appelée « *Key Ceremony* » ou « cérémonie de clefs ».

6.1.1.3. Clefs d'AC Intermédiaire/Emettrice générées au niveau du serveur de l'AC Intermédiaire/Emettrice

La génération de la bi-clef d'une AC Intermédiaire ou Emettrice doit être réalisée dans un dispositif cryptographique répondant aux exigences du chapitre 11 dans le cas où le bi-clef est généré au niveau du serveur.

6.1.2. Transmission de la clef privée à son propriétaire

Dans le cas où la clef privée est générée au niveau du serveur de l'AC Intermédiaire ou Emettrice, celle-ci est transmise à l'entité responsable de manière sécurisée suivant les modalités décrites dans le document de cérémonie des clefs.

6.1.3. Transmission de la clef publique à l'AC

Les clefs publiques des AC Intermédiaire ou Emettrice sont transmises à l'AC Racine, aux fins de signature, dans des conditions qui garantissent leur intégrité et leur origine (*sous forme d'une requête PKCS10*).

6.1.4. Transmission de la clef publique de l'AC aux utilisateurs de certificat

La clef publique de l'AC Racine est transmise aux utilisateurs sous forme de certificat.

Par ailleurs, l'empreinte numérique de l'AC Racine figure :

- dans son certificat et dans tout autre certificat d'AC signé par l'AC Racine ;
- sur le site http://pc.igcv3.certificats.banque-france.fr ;
- et peut également être consultée auprès du point de contact identifié au chapitre 1.6.2.

6.1.5. Taille des clefs

L'AC racine dispose d'une clef RSA de 4096 bits.

Les AC Intermédiaires et Emettrices disposent d'une clef RSA de 4096 bits.

Ces exigences sont revues à mesure de l'évolution de l'état de l'art technique et/ou de la législation.

6.1.6. Vérification de la génération des paramètres des bi-clefs et de leur qualité

L'équipement de génération des bi-clefs utilise des paramètres respectant les normes de sécurité propres à l'algorithme RSA. Le détail est fourni dans la DPC.

La bi-clef d'une AC Intermédiaire ou Emettrice est générée en utilisant des paramètres respectant les normes de sécurité propres à l'algorithme RSA. Les paramètres et les algorithmes de signature sont documentés au chapitre 7.

La bi-clef d'une AC Intermédiaire ou Emettrice est générée et protégée par un module cryptographique matériel répondant aux exigences du chapitre 11 pour le niveau de sécurité considéré.

La bi-clef de l'AC Racine est générée et protégée par un module cryptographique matériel répondant aux exigences du chapitre 11 pour le niveau de sécurité considéré.

6.1.7. Objectifs d'usage de la clef

L'utilisation de la clef privée de l'AC Racine et du certificat associé est strictement limitée à la signature de certificats et de LAR.

L'utilisation de la clef privée d'une AC Intermédiaire ou Emettrice est strictement limitée à la signature de certificats et de LCR / LAR.

6.2. Mesures de sécurité pour la protection des clefs privées et pour les modules cryptographiques

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1. Modules cryptographiques de l'AC

Pour la génération et la mise en œuvre de ses clefs de signature, l'AC « Banque de France AC v3 Racine » utilise un module cryptographique répondant aux critères communs au niveau EAL4+ et qualifié au niveau renforcé répondant ainsi aux exigences du chapitre 11.

6.2.1.2. Modules cryptographiques de l'AC Intermédiaire/Emettrice

Dans le cas d'une génération par l'AC Racine, la bi-clef d'une AC Intermédiaire ou Emettrice est générée et mise en œuvre dans un module cryptographique répondant aux critères communs au niveau EAL4+ et qualifié au niveau renforcé répondant ainsi aux exigences du chapitre 11.

Dans le cas d'une génération au niveau du serveur de l'AC Intermédiaire ou Emettrice, l'AC Racine s'assure de la conformité du dispositif cryptographique mis en œuvre, au travers d'un engagement contractuel clair et explicite de l'entité responsable de l'AC Intermédiaire ou Emettrice.

6.2.2. Contrôles de la clef privée par plusieurs personnes

Le contrôle des clefs privées de l'AC Racine est assuré par un dispositif mettant en œuvre le partage de secrets (nécessité de réunir au moins 3 porteurs de secrets parmi 5).

Le rôle de conservateur de secrets est assuré par du personnel de confiance. Les conservateurs de secrets sont responsables des secrets qui leur sont remis. Ils en assurent la conservation afin de garantir leur confidentialité, disponibilité, intégrité et traçabilité. Des précisions sont apportées dans la DPC.

6.2.3. Séquestre de la clef privée

Les clefs privées de l'AC Racine ne sont pas séquestrées.

Les clefs privées des AC Intermédiaires et Emettrices ne sont pas séquestrées.

6.2.4. Copies de secours de la clef privée

La clef privée de l'AC Racine fait l'objet d'une copie de secours bénéficiant du même niveau de sécurité que les clefs initiale.

Les opérations de copie sont conformes aux exigences du chapitre 11 permettant ainsi d'assurer les opérations cryptographiques à l'intérieur du module cryptographique.

Les clefs privées des AC Intermédiaires et Emettrices peuvent être sauvegardées par leur propre entité responsable. Le cas échéant, les clefs sauvegardées doivent être enregistrées sous forme chiffrée et avec un mécanisme de contrôle d'intégrité.

6.2.5. Archivage de la clef privée

La clef privée de l'AC Racine n'est pas archivée.

Les clefs privées des AC Intermédiaires et Emettrices ne sont pas archivées.

6.2.6. Transfert de la clef privée vers/depuis le module cryptographique

La clef privée d'une AC Intermédiaire ou Emettrice est générée dans un dispositif cryptographique et tout transfert est réalisée sous forme chiffrée.

Le transfert de la clef privée de l'AC Racine vers et depuis le module cryptographique est soumis à un dispositif mettant en œuvre le partage de secrets. Les moyens de transfert utilisés permettent d'assurer la confidentialité et l'intégrité de la clef privée.

6.2.7. Stockage de la clef privée dans un module cryptographique

La clef privée de l'AC Racine est stockée dans un module cryptographique répondant aux exigences du chapitre 11 (*cf. chapitre 6.2.1.1*) pour le niveau de sécurité considéré.

Les clefs des AC Intermédiaires ou Emettrices sont générées dans un dispositif cryptographique répondant aux exigences du chapitre 11 (*cf. chapitre 6.2.1.2*) pour le niveau de sécurité considéré.

6.2.8. Méthode d'activation de la clef privée

6.2.8.1. Clef privée d'AC

L'activation de la clef privée de l'AC Racine dans le module cryptographique est contrôlée via des données d'activation et nécessite l'intervention d'au moins deux porteurs de secrets (*personnes disposant d'un rôle de confiance, cf. chapitre 5.2*) permettant de répondre aux exigences du chapitre 11 pour le niveau de sécurité considéré.

6.2.8.2. Clefs privées des AC Intermédiaires/Emettrices

L'activation de la clef privée d'une AC Intermédiaire ou Emettrice dans le module cryptographique est contrôlée via des données d'activation et nécessite l'intervention d'au moins deux porteurs de secrets (*personnes disposant d'un rôle de confiance, cf. chapitre 5.2*) permettant de répondre aux exigences du chapitre 11 pour le niveau de sécurité considéré.

6.2.9. Méthode de désactivation de la clef privée

6.2.9.1. Clef privée d'AC

La désactivation de la clef privée de l'AC Racine dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

Les conditions de désactivation permettent de répondre aux exigences du chapitre 11 pour le niveau de sécurité considéré.

6.2.9.2. Clefs privées des AC Intermédiaires/Emettrices

La désactivation de la clef privée d'une AC Intermédiaire ou Emettrice dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

Les conditions de désactivation permettent de répondre aux exigences du chapitre 11 pour le niveau de sécurité considéré.

6.2.10. Méthode de destruction de la clef privée

6.2.10.1. Clef privée d'AC

En fin de vie de la clef privée de l'AC Racine, normale ou anticipée (révocation), celle-ci sera détruite à partir du module cryptographique, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.10.2. Clefs privées des AC Intermédiaires/Emettrices

En fin de vie d'une clef privée d'AC Intermédiaire ou Emettrice, normale ou anticipée (révocation), celle-ci sera détruite à partir du module cryptographique, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.11. Niveau d'évaluation sécurité des modules cryptographiques

Le niveau d'évaluation du module cryptographique de l'AC Racine est précisé au chapitre 6.2.1.

Pour les AC Intermédiaires et Emettrices, les modules cryptographiques sont évalués au niveau correspondant à l'usage visé.

6.3. Autres aspects de la gestion des bi-clefs

6.3.1. Archivage des clefs publiques

Les clefs publiques sont archivées dans le cadre de l'archivage des certificats correspondants.

6.3.2. Durée de vie des bi-clefs et des certificats

Les certificats et bi-clefs des AC Intermédiaires et Emettrices ont la même durée de vie.

Cette durée de vie est :

- Inférieure ou égale à 20 ans pour les certificats d'AC Intermédiaires et Emettrices ;

La fin de vie du certificat de l'AC Racine ayant émis le certificat de l'AC Intermédiaires ou Emettrice est postérieure à la fin de vie des certificats qu'elle émet.

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

6.4.1.1. Génération et installation des données d'activation correspondant à la clef privée de l'AC

La génération et l'installation des données d'activation des modules cryptographiques de l'IGC sont réalisées lors de la phase d'initialisation et de personnalisation de ces modules. Les données d'activation sont transmises à leur responsable de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués.

6.4.1.2. Génération et installation des données d'activation correspondant à la clef privée des AC Intermédiaires/Emettrices

La génération et l'installation des données d'activation des modules cryptographiques de l'IGC sont réalisées lors de la phase d'initialisation et de personnalisation de ces modules. Les données d'activation sont transmises à leur responsable de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués.

6.4.2. Protection des données d'activation

6.4.2.1. Protection des données d'activation correspondant à la clef privée de l'AC

Les données d'activation sont protégées en intégrité et en confidentialité jusqu'à leur remise à leur destinataire (*porteur de secret*). Le destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.4.2.2. Protection des données d'activation correspondant à la clef privée des AC Intermédiaires/Emettrices

Les données d'activation sont protégées en intégrité et en confidentialité jusqu'à leur remise à leur destinataire (*porteur de secret*). Le destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.4.3. Autres aspects liés aux données d'activation

Sans objet.

6.5. Mesures de sécurité des systèmes informatiques

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Les systèmes informatiques de l'IGC offrent un niveau de sécurité décrit précisément dans la DPC qui couvre notamment les points suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) ;
- gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) ;
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;

- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non autorisés et mises à jour des logiciels ;
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- protection du réseau contre toute intrusion d'une personne non autorisée ;
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- éventuellement, gestion des reprises sur erreur.

La protection en confidentialité et en intégrité des clefs privées ou secrètes d'infrastructure et de contrôle (cf. chapitre 1.4.1.2) fait l'objet de mesures particulières, définies suite à l'analyse de risques.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) sont en place lorsque nécessaire.

6.5.2. Niveau d'évaluation sécurité des systèmes informatiques

Le détail est fourni dans la DPC.

Les règles suivantes sont appliquées sur les systèmes de l'IGC BDF afin d'assurer un niveau de sécurité optimum :

- tous les ingénieurs système sont des agents de la Banque de France ou d'un prestataire garantissant un niveau de sécurité identique ;
- Aucun compte utilisateur autre que celui des ingénieurs système ou administrateurs de base de données n'est créé ;
- le compte d'un ingénieur est suspendu en cas de départ ou d'absence prolongée ;
- tous les comptes sont individuels et traçables ;
- les systèmes d'audit permettant l'imputabilité des actions de chacun sont mis en place ;
- les fichiers systèmes sensibles sont surveillés quotidiennement afin d'en vérifier l'intégrité ;
- le serveur Pare-feu est surveillé quotidiennement, les éventuelles attaques sont analysées et enregistrées afin de déterminer la stratégie utilisée par les attaquants ;
- l'ensemble du système d'information est protégé par des anti-virus ;
- tous les serveurs sont sauvegardés selon un plan de sauvegarde associé à un plan de reprise en cas de désastre ;
- un dispositif de contrôle d'intégrité assure que les fichiers présents sur chaque machine ne sont pas altérés.

6.6. Mesure de sécurité des systèmes durant leur cycle de vie

Les objectifs de sécurité sont définis dès les phases de spécification et de conception.

L'AC utilise des systèmes et des produits fiables qui sont protégés contre une modification illégitime.

6.6.1. Mesures de sécurités liées au développement des systèmes

La Banque de France s'engage à ce que les programmes et systèmes de l'AE soient développés et implémentés dans le strict respect de la politique de sécurité de la Banque de France.

Toute évolution significative d'un système d'une composante de l'IGC doit être signalée à l'AC pour validation. Elle doit être documentée et doit apparaître dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

6.6.2. Mesures liées à la gestion de la sécurité

L'AC s'engage à ce que toute évolution des systèmes soit enregistrée.

6.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

6.7. Mesures de sécurité réseau

L'interconnexion entre les systèmes de l'IGC et les réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au bon fonctionnement de l'IGC.

Les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées.

6.8. Horodatage / Système de datation

Pour dater les évènements, les différentes composantes de l'IGC s'appuient sur l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près.

Cette précision de synchronisation par rapport au temps UTC n'est pas requise pour les opérations faites hors ligne (ex : administration de l'AC Racine).

La synchronisation par rapport au temps UTC se réfère à un système comprenant au moins deux sources indépendantes de temps.

7. Profils des certificats et des LCR / LAR

Le document annexe [IGC-BDF-v3_Profils] détaille les profils des certificats, les listes de révocation (LCR/LAR) et le service OCSP mis en œuvre dans le cadre de la présente PC.

Le document est disponible sur le site de publication de l'IGCv3 à l'adresse suivante : http://pc.igcv3.certificats.banque-france.fr.

8. Audits de conformité et autres évaluations

La Banque de France a la responsabilité du bon fonctionnement des composantes de l'IGC conformément aux dispositions énoncées dans le présent document.

Pour ce faire, deux types de contrôle sont identifiés : la maîtrise de l'activité de l'IGC et le contrôle de conformité par rapport aux documents constitutifs de l'IGC (PC, DPC). La maîtrise de l'activité de l'IGC est assurée par :

- des contrôles opérationnels : vérification de l'exécution des procédures par les gestionnaires, qui en rendent compte aux responsables de l'IGC ;
- des contrôles hiérarchiques sur les gestionnaires ;
- des contrôles menés par les services d'audit de la Banque de France.

8.1. Fréquence et circonstances des évaluations

Une évaluation est réalisée tous les deux ans ou de façon exceptionnelle sur demande du Comité d'approbation des politiques de certification, typiquement après une première mise en service ou modification significative d'une composante de l'IGC.

De plus, sur demande expresse du Comité d'approbation des politiques de certification, une évaluation externe peut être réalisée par des contrôleurs faisant partie d'une entité d'audit externe à la Banque de France.

8.2. Identité et qualification des évaluateurs

Le contrôle d'une composante est assigné par l'AC à une équipe d'auditeurs compétents en matière de sécurité des systèmes d'information et dans le domaine d'activité de la composante concernée.

8.3. Relations entre évaluateurs et entités évaluées

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

8.4. Sujets couverts par les évaluations

Les évaluations portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5. Actions prises suite aux conclusions des évaluations

À l'issue d'une évaluation, un rapport est fourni à l'AC et au CAPC.

L'AC présente si nécessaire au CAPC un plan d'action permettant de prendre en compte les remarques des évaluateurs.

8.6. Communication des résultats

L'AC se réserve le droit de communiquer tout ou partie des résultats aux entités ayant le besoin d'en connaitre.

Dans tous les cas, les résultats des audits de conformité sont tenus à la disposition de l'organisme de qualification en charge de la qualification de l'AC.

9. Autres problématiques métiers et légales

9.1. Tarifs

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

Sans objet.

9.1.2. Tarifs pour accéder aux certificats

Sans objet.

9.1.3. Tarifs pour accéder aux informations d'état et de révocation de certificats

Les informations d'état et de révocation de certificats sont mises à disposition gratuitement.

9.1.4. Tarifs pour d'autres services

Sans objet.

9.1.5. Politique de remboursement

Sans objet.

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

Les risques susceptibles d'engager la responsabilité de l'AC sont couverts par un dispositif d'assurance approprié tel que décrit ci-après.

La Banque de France est son propre assureur et prend à sa charge les conséquences des sinistres mettant en jeu sa responsabilité civile dans la limite du montant défini aux conditions particulières de ses polices d'assurances. Au-delà de ce montant et dans la limite des plafonds définis, les assureurs se substituent aux obligations de la Banque de France.

Les prestataires de services de certification, fournisseurs d'infrastructure technique, et de dispositifs de création de signature intervenant dans l'IGC doivent pouvoir justifier être couverts indépendamment par une assurance responsabilité civile exploitation professionnelle.

9.2.2. Autres ressources

Ressources propres suffisantes au bon fonctionnement et à l'accomplissement des activités de l'AC.

9.2.3. Couverture et garantie concernant les entités utilisatrices

Pas d'exigence spécifique.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- la partie non publique de la DPC ;
- les clefs privées de l'AC Racine, des composantes et des certificats émis ;
- les données d'activation associées aux clefs privées de l'ACR et des certificats émis ;
- tous les secrets de l'IGC ;
- les journaux d'événements des composantes de l'IGC ;
- les dossiers d'enregistrement des entités clientes ;
- les causes de révocations, sauf accord explicite de publication.

9.3.2. Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3. Responsabilité en termes de protection des informations confidentielles

L'AC a mis en place et respecte des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme confidentielles au sens de l'article 9.3.1 ci-dessus.

L'AC respecte la législation et la réglementation en vigueur sur le territoire français. En particulier, il est précisé qu'elle peut devoir mettre à disposition les dossiers d'enregistrement des AC Intermédiaires/Emettrices à des tiers dans le cadre de procédures légales.

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

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,

En conformité avec les dispositions précitées, le traitement automatisé des données nominatives réalisé à partir de l'IGC de la Banque de France a fait l'objet d'une déclaration auprès du Correspondant informatique et libertés (CIL) de la Banque de France.

L'AC est le responsable du traitement des données.

9.4.2. Données personnelles

Les informations suivantes sont des données personnelles au sens de l'article 4 du règlement européen sur la protection des données ;

- données d'identification du mandataire de certification et du représentant légal de l'entité responsable de l'AC Intermédiaire/Emettrice ;
- données renseignées dans le dossier d'enregistrement pour la demande de certificat ;
- données renseignées dans la demande de révocation de certificat ;
- causes de révocation des certificats des AC Intermédiaires/Emettrices.

Les données personnelles sont collectées et traitées à seule fin de permettre la mise en œuvre de l'IGC de la Banque de France et pour l'utilisation définie dans le cadre de la PC. Elles sont détruites lorsque leur conservation n'est plus nécessaire à la certification et en particulier dans les cas suivants :

- rejet d'une demande de certification
- l'expiration de la période de conservation des archives précisée à l'article 5.5.2

9.4.3. Droit d'information des personnes concernées

L'AC informe les personnes concernées du traitement de leurs données personnelles au moment de la collecte des données.

9.4.4. Exercice des droits des personnes

L'AC gère les demandes des personnes concernées et répond aux demandes des personnes concernées dans les délais prévus par le règlement européen sur la protection des données.

9.4.5. Violations de données personnelles

L'AC notifie à la CNIL tout violation de données personnelles en lui communiquant au moins :

- la description de la nature de la violation de données personnelles, y compris les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données personnelles concernées ;
- le nom et les coordonnées du délégué à la protection des données;
- la description des conséquences probables de la violation de données personnelles ;

- la description des mesures prises ou proposées pour remédier à la violation de données personnelles, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

L'AC communique la violation de données à caractère personnel aux personnes concernées dans les conditions de l'article 34 du règlement européen sur la protection des données.

9.4.6. Registre des catégories d'activité de traitement

L'AC tient par écrit un registre de toutes les catégories d'activités de traitement effectuées conformément à l'article 30 du règlement relatif à la protection des données personnelles.

9.4.7. Données non personnelles

Sans objet.

9.4.8. Responsabilité en termes de protection des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 9.15).

9.4.9. Notification et consentement d'utilisation des données personnelles

Aucune des données personnelles ne peut être collectée et traitée par l'AC, pour une utilisation autre que celle définie dans le cadre de la PC, sans consentement exprès et préalable de la personne concernée.

Les données personnelles ne doivent ni être divulguées ni être transférées à un tiers sauf consentement préalable de la personne concernée, décision judiciaire ou autre autorisation légale.

9.4.10. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 9.15).

9.4.11. Autres circonstances de divulgation de données personnelles

Sans objet.

9.5. Droits de propriété intellectuelle et industrielle

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

9.6. Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clefs secrètes et/ou privées ;
- n'utiliser leurs clefs cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la présente PC et les documents qui en découlent ;
- respecter et appliquer la partie de la DPC leur incombant ;
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre 8) et l'organisme de qualification ;
- respecter les accords ou contrats qui les lient entre elles ou aux AC Intermédiaires/Emettrices ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1. Autorités de certification

L'AC Racine a pour obligation de :

- démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour une AC Intermédiaire/Emettrice et que le représentant légal de l'entité responsable de l'AC ou un MC a accepté le certificat, conformément aux exigences du chapitre 4.4 ;
- garantir et maintenir la cohérence de sa DPC avec sa PC ;
- prendre toutes les mesures pour s'assurer que le représentant légal ou le MC le cas échéant sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clefs, des certificats

ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre une AC Intermédiaire/Emettrice et l'AC Racine est formalisée par un lien contractuel ou hiérarchique ou réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC Racine assume toute conséquence directe dommageable qui résulterait du non-respect de sa propre PC, par elle-même ou l'une de ses composantes. Elle prévoit les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et possède la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique.

L'AC Racine engage sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelles qu'en soient la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des représentants légaux ou des MC à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

L'AC Racine reconnaît avoir à sa charge une obligation de garantir la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de l'AC.

9.6.2. Service d'enregistrement

Cf. obligations précisées au chapitre 9.6.1.

9.6.3. Mandataire de Certification

Le MC a l'obliqation de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- informer l'AC, sans délai, de toute modification concernant les informations contenues dans le certificat ;
- demander, sans délai, la révocation (cf. chapitres 3.4 et 4.9) du certificat en cas de compromission ou de suspicion de compromission de la clef privée ou des données d'activation.

9.6.4. Utilisateurs de certificats

Les utilisateurs de certificats doivent :

- respecter l'usage pour lequel un certificat a été émis ;
- pour chaque certificat de la chaîne de certification, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

9.6.5. Autres participants

Concernant l'OC :

En tant que prestataire de services, l'OC s'engage à respecter la DPC et le contrat de service établi avec l'AC.

9.7. Exclusions et limitations de garantie

Cf. chapitre 9.2.

9.8. Exclusions et limitations de responsabilités

Le régime de responsabilité est défini par l'article 33 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

L'AC Racine est responsable des exigences et des principes édictés dans la présente PC, ainsi que de tout dommage causé à une AC Intermédiaire/Emettrice ou utilisateur de certificat résultant d'un manquement aux procédures définies dans la PC et la DPC associée.

L'AC Racine 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 Racine 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 représentant légal, ou le MC le cas échéant, de l'entité responsable de l'AC Intermédiaire/Emettrice (cf. également chapitre 4.4.1).

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

9.9. Indemnités

Sans objet.

9.10. Durée et fin anticipée de validité de la PC

9.10.1. Durée de validité

Cette PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de la PC.

9.10.2. Fin anticipée de validité

En fonction de la nature et de l'importance des évolutions apportées à la PC, le délai de mise en conformité sera arrêté conformément aux modalités prévues par la réglementation en vigueur.

De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

9.10.3. Effets de la fin de validité et clauses restant applicables

Sans objet.

9.11. Notifications individuelles et communication entre les participants

En cas de changement de toute nature intervenant dans la composition technique de l'IGC, l'AC Racine s'engage à :

- au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et de ses différentes composantes ;
- au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

9.12. Amendements de la PC

9.12.1. Procédures d'amendement

Tout amendement de la PC devra être soumis au CAPC.

9.12.2. Mécanisme et période d'information sur les amendements

Sans objet.

9.12.3. Circonstances selon lesquelles l'OID doit être changé

Toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis peut se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

L'OID de la PC de l'AC Racine évoluera dès lors qu'un changement majeur (et qui sera signalé comme tel) interviendra dans les exigences de la présente PC.

9.13. Dispositions concernant la résolution de conflits

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.

9.14. Juridictions compétentes

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

9.15. Conformité aux législations et réglementations

La politique et les pratiques de l'AC sont non-discriminatoires.

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux présentés ci-dessous.

Document
Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles puis par ordonnance n°2018-1125 du 12 décembre 2018 .
Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.
Loi modifiée n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
Loi n° 90-1170 du 29 décembre 1990, modifiée sur la réglementation des télécommunications.
n°2002-688 du 2 mai 2002 modifiant le décret n°98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie, modifié par le décret n°2002-688 du 2 mai 2002.
Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie.
Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives modifiée par ordonnance n°2017-1426 du 4 octobre 2017 .
Décret n°2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005.
Décret nº 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique modifié par le décret n°2017-1416 du 28 septembre 2017 .
Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation .
Annexe de l'arrêté du 26 juillet 2004 - Spécifications techniques relatives aux prestataires de services de certification en vue de la reconnaissance de leur qualification.

Tableau – Textes législatifs et réglementaires applicables

9.16. Dispositions diverses

9.16.1. Accord global

Sans objet.

9.16.2. Transfert d'activités

Cf. chapitre 5.8.

9.16.3. Conséquences d'une clause non valide

Sans objet.

9.16.4. Application et renonciation

Sans objet.

9.16.5. Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par la jurisprudence des cours et tribunaux français, tout événement imprévisible, irrésistible et extérieur aux parties.

9.17. Autres dispositions

Sans objet.

10. Annexe 1 : Documents cités en référence

10.1. Règlementation

[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par *la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles puis par ordonnance n°2018-1125 du 12 décembre 2018*
[ORDONNANCE]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives *modifiée par ordonnance n°2017-1426 du 4 octobre 2017*
[DEC_EXEC_1506]	Décision d'exécution (UE) 2015/1506 de la Commission du 8 septembre 2015 établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public visés à l'article 27, paragraphe 5, et à l'article 37, paragraphe 5, du règlement [eIDAS].
[eIDAS]	Règlement n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n°1999/93/CE.
[DécretRGS]	Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005

10.2. Documents techniques

[RGS]	Référentiel Général de Sécurité – Version 2.0
[ETSI EN 319401]	General Policy Requirements for Trust Service Providers
[ETSI EN 319411-1]	Policy & Security Requirements for TSPs Issuing Certificates - Part 1: General requirements
[ETSI EN 319411-2]	Policy & Security Requirements for TSPs Issuing Certificates - Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETSI EN 319412-1]	Certificate Profiles - Part 1: Overview and common data structures
[ETSI EN 319412-2]	Certificate Profiles - Part 2: Certificate profile for certificates issued to natural persons
[ETSI EN 319412-3]	Certificate Profiles - Part 3: Certificate profile for certificates issued to legal persons
[ETSI EN 319412-4]	Certificate Profiles - Part 4: Certificate profile for web site certificates
[ETSI EN 319412-5]	Certificate Profiles - Part 5: QCStatements
[IGC-BDF-v3_Profils]	Profils des certificats, LCR/LAR et OCSP de l'IGCv3 de Banque de France
[PSCE_RGS_EIDAS]	Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet - Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS, version en vigueur.
[PSCO_QUALIF]	Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur.
[RFC_5280]	Internet Engineering Task Force (IETF) - Request for Comments : 5280 X.509 Internet Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile.
[RFC_6960]	Internet Engineering Task Force (IETF) - Request for Comments : 6960

	X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP.
[RFC_3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version d'août 2005 (complétée par les correctifs techniques Corrigendum 1 de janvier 2007et Corrigendum 2 de novembre 2008)
[TS_119_312]	ETSI TS 119 312 V1.1.1 (2014-11) : Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

11. Annexe 2 : Exigences de sécurité du module cryptographique de l'AC

11.1. Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clefs de signature (pour la génération des certificats électroniques, des LCR / LAR ou des réponses OCSP), ainsi que, le cas échéant, générer les bi-clefs des services applicatifs, doit répondre aux exigences de sécurité suivantes :

- Si les bi-clefs des services applicatifs sont générées par ce module, garantir que ces générations sont réalisées exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clefs générées ;
- Si les bi-clefs des services applicatifs sont générées par ce module, assurer la confidentialité des clefs privées et l'intégrité des clefs privées et publiques des service applicatifs lorsqu'elles sont sous la responsabilité de l'AC et pendant leur transfert vers le dispositif de protection des éléments secrets du service applicatif et assurer leur destruction sûre après ce transfert ;
- Assurer la confidentialité et l'intégrité des clefs privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- Être capable d'identifier et d'authentifier ses utilisateurs ;
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- Être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clefs privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clefs privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Si une fonction de sauvegarde et de restauration des clefs privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.
- Détecter les tentatives d'altérations physiques et entrer dans un état sûr quand une tentative d'altération est détectée.

11.2. Exigences sur la certification

Le module est certifié conformément aux exigences ci-dessus et a fait l'objet d'une qualification (EAL4+ avec une résistance élevée des mécanismes).