Sécurité de l'information

Politique de certification
Banque de France AC v3 Chiffrement

(OID : 1.2.250.1.115.200.3.1.1.3.1)

Date	***:***	17 Août 2023	***Version***	***:***	1.2
Rédacteur	***:***	RSI	***Nombre de pages***	***:***	**67**
Classification	***:***	Public			

FICHE DE CONTRÔLE DU DOCUMENT

Suivi des versions

Version	Date	Rédacteur	Modification
1.0	28/05/2020	DM - RSI	Version Initiale
1.1	18/08/2020	RT - RSI	Mise à jour mineure
1.2	17/08/2023	RSI	Mise à jour : - Possibilité de délivrance des certificats pour des services applicatifs de type Entité, externes à la Banque de France. - Gestion des certificats émis par l'AC « Banque de France AC v3 Chiffrement », dans le cadre du badge agent Banque de France. - Mise à jour des informations liés à la gestion des données personnelles par l'AC Banque de France.

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

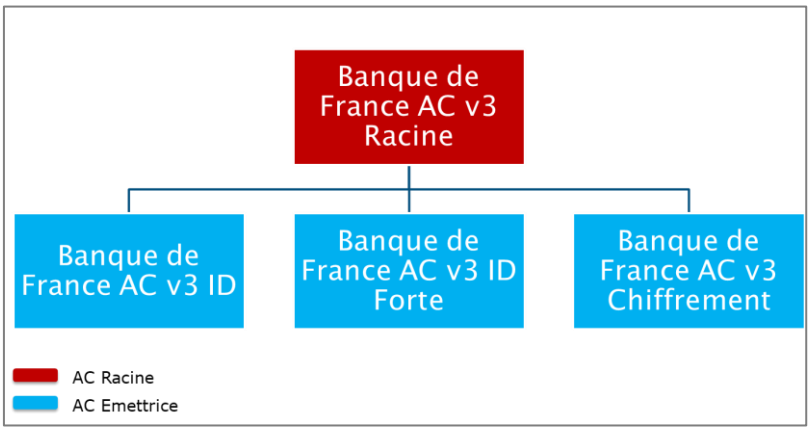
TABLE DES MATIÈRES

1. Introduction

1.1. Présentation générale

La Banque de France a mis en œuvre sa propre Infrastructure de Gestion de Clefs 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 :



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

L'Autorité de Certification « **Banque de France AC v3 Chiffremen**t » délivre des certificats d'une part aux membres du personnel de la Banque de France, et d'autres part à des membres des entreprises et administrations en relation avec un des métiers de la Banque de France.

Elle délivre notamment des certificats :

- Pour des personnes physiques :
  - Certificats de chiffrement au format logiciel,
- Pour des services applicatifs de type Entité (personne morale)
  - Certificats de chiffrement au format logiciel,
- Pour des services applicatifs de type Machine
  - Certificats de chiffrement au format logiciel

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.

Ces offres de certificats et la 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 Chiffrement

Cette PC est identifiée par l'OID **1.2.250.1.115.200.3.1.1.3.1** et couvre les offres de certificats identifiées par les OID suivants :

Usage du certificat	OID de la PC
Chiffrement Personne	1.2.250.1.115.200.3.1.2.3.1.1.1
Chiffrement Entité	1.2.250.1.115.200.3.1.2.3.2.1.1
Chiffrement Machine	1.2.250.1.115.200.3.1.2.3.3.1.1

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.

Entrée	Définition
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
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'un bi-clef, pouvant être communiqué à tous les membres d'une population. Une clef publique permet de chiffrer des données à destination du porteur du 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 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 de rattachement d'un porteur.
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 « émettrices » 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 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 du futur porteur d'un certificat, 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 du porteur lors du renouvellement du certificat de celui-ci.
- **Autorité d'enregistrement déléguée (AED)** – Cette fonction vérifie *a minima* les informations du dossier d'enregistrement du mandataire de certification avant transmission de celui-ci à l'AE.

  L'AED est désignée par le responsable de l'IGC.
- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clef privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clef publique du porteur provenant soit du porteur, soit de la fonction de génération des éléments secrets du porteur, si c'est cette dernière qui génère le bi-clef du porteur.
- **Fonction de génération des éléments secrets du porteur/service applicatif** - Cette fonction génère les éléments secrets à destination du porteur/RC, si l'AC a en charge une telle génération, et les prépare en vue de leur remise au porteur/RC (par exemple, personnalisation de la carte à puce destinée au porteur, courrier sécurisé avec le code d'activation, etc.). De tels éléments secrets peuvent être, par exemple, directement le bi-clef du porteur/service applicatif, les codes (activation, déblocage) liés au dispositif de stockage de la clef privée du porteur/service applicatif ou encore des codes ou clefs temporaires permettant au porteur/RC de mener à distance le processus de génération / récupération de son certificat.
- **Fonction de remise au porteur/RC** - Cette fonction remet au porteur/RC au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif du porteur/service applicatif, clef privée du porteur/service applicatif, codes d'activation,…).
- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées, les politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides de ses porteurs.
- **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).

- **Fonction de gestion des recouvrements** - Cette fonction traite les demandes de recouvrement de clefs privées des porteurs (notamment identification et authentification du demandeur) et détermine les actions à mener. Dans le cas d'une décision positive, le recouvrement est réalisé par la fonction de séquestre et recouvrement.
- **Fonction de séquestre et recouvrement** - Cette fonction fournit la capacité de séquestrer de manière sécurisée les clefs privées de confidentialité des porteurs/services applicatifs, puis de les recouvrer en cas de besoin, sur la base de demandes authentifiées et traitées par la fonction de gestion des recouvrements.

Un certain nombre d'entités et personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

- **Porteur** - La personne physique identifiée dans le certificat et qui est le détenteur de la clef privée correspondant à la clef publique qui est dans ce certificat.

- **Responsable du certificat du serveur ou de l'entité (RC)** – Personne en charge et responsable du certificat électronique du serveur ou de l'entité.

- **Mandataire de certification (MC)** - Le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des porteurs de cette entité.

- **Utilisateur de certificat** - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique ou une valeur d'authentification provenant du porteur du certificat ou chiffrer des données à destination du porteur du certificat.

- **Personne autorisée** - Il s'agit d'une personne autre que le porteur et le mandataire de certification et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.

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 porteurs 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 au porteur, 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 l'identité du futur porteur de certificat ou du futur RC et les informations liées au service applicatif. Pour cela, l'AE assure les tâches suivantes :

- La prise en compte et la vérification :
    - des informations du futur porteur et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
    - des informations du futur RC et du service applicatif (*entité ou machine*), ainsi que de leur entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- Le cas échéant, la prise en compte et la vérification des informations du futur MC (*cf. dernier paragraphe*) et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- 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) ;
- La conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du porteur ou, le cas échéant, du MC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (*notamment, elle respecte le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable depuis le 25 mai 2018*).

Elle est aussi chargée de la transmission sécurisée des données d'activation associées aux clefs privées.

Le cas échéant, l'AE s'appuie sur un mandataire de certification désigné et placé sous la responsabilité de l'entité cliente pour effectuer tout ou partie des opérations de vérification des informations (cf. chapitre 1.4.6.2 ci-dessous). L'AE s'assure que les demandes sont complètes et exactes et effectuées par un MC dûment autorisé pour les porteurs et RC externes.

Dans certain cas (*cas d'un MC d'une entité externe*), l'AE peut déléguer le contrôle de la complétude du dossier d'enregistrement du MC Externe à une AED.

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. Porteurs de certificats

Le porteur de certificat est une personne physique qui peut être :

- soit un agent de la Banque de France,
- soit un prestataire de la Banque de France,
- soit un membre d'une entreprise ou d'un organisme en relation avec un des métiers de la Banque de France (*personne externe à la Banque de France*). Cette personne utilise sa clef privée et le certificat correspondant dans le cadre de ses activités en relation avec l'entité identifiée dans le certificat et avec laquelle elle a un lien contractuel ou hiérarchique.

Dans le cas d'un prestataire de la Banque de France, l'ensemble des modalités de traitement décrites dans cette PC sont équivalentes à celles liées à un agent de la Banque de France. Par convention et pour simplifier la lecture, toutes les modalités de traitement évoquées dans la suite de cette PC sont applicables aux prestataires.

Les porteurs doivent respecter les conditions définies dans la présente politique de certification.

L'AC n'émet aucun certificat pour les particuliers.

1.4.4. Responsable de certificat (RC)

Dans le cadre de cette présente PC, un RC est une personne physique qui est responsable de l'utilisation du certificat du service applicatif (*entité ou machine*) identifié dans le certificat et de la clef privée correspondante.

Un certificat de type « entité » peut être délivré à un service applicatif interne Banque de France ou à une personne morale externe :

- En interne Banque de France : Tout agent de la Banque de France peut être un RC pour l'entité à laquelle il est rattaché.
- En externe Banque de France : Le RC est un membre d'une entreprise ou d'un organisme en relation avec un des métiers de la Banque de France.

Un certificat de service applicatif pour une machine ne peut être délivré qu'à un serveur informatique de la Banque de France. Dans ce cas, le RC est l'exploitant de la machine et est nécessairement un agent de la Banque de France et ne peut être en aucun cas un personnel externe.

Le RC respecte les conditions qui lui incombent définies dans la présente PC.

Il est à noter que même si le certificat identifie un service applicatif, celui-ci reste rattaché au RC. Par conséquent, en cas de départ du RC, le certificat du service applicatif est révoqué.

1.4.5. Utilisateurs de certificats

Sont appelés utilisateurs, les personnes physiques ou automates qui utilisent les certificats émis par la Banque de France.

Dans le cadre des certificats de chiffrement, un utilisateur peut être notamment :

- Un service en ligne qui utilise un dispositif de chiffrement pour chiffrer des données ou un message à destination du porteur du certificat ;
- Une personne physique qui émet un message chiffré à l'intention du porteur du certificat électronique.

Les domaines d'utilisation figurent dans la partie 1.5.1 de la présente politique de certification.

Les utilisateurs de certificats doivent respecter les conditions définies dans la présente politique de certification, en particulier les exigences du chapitre 9.6.4.

1.4.6. Autres participants

1.4.6.1. Composantes de l'IGC

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

1.4.6.2. Mandataires de certification

Les mandataires de certification (MC) sont des personnes physiques habilitées à demander des certificats auprès de l'autorité d'enregistrement.

Les mandataires de certification n'ont pas accès aux moyens qui leur permettraient d'activer et d'utiliser la clef privée associée à la clef publique contenue dans le certificat délivré au porteur et aux services applicatifs. Les engagements du MC à l'égard de l'AC sont précisés dans un contrat écrit avec l'entité de rattachement du MC. Le MC s'engage à :

- Effectuer en face à face, et de façon indépendante les contrôles d'identité des futurs porteurs/RC de l'entité pour laquelle il est MC ;
- Respecter les obligations définies dans la PC de l'AC qui lui incombent.

Pour les porteurs internes de la Banque de France :

Aucun mandataire de certification n'intervient dans le processus d'enregistrement d'un porteur interne de la Banque de France.

Pour les porteurs externes à la Banque de France :

Les porteurs externes sont authentifiés par un mandataire de certification. Une même entité peut s'appuyer sur un ou plusieurs mandataires de certification. Le mandataire de certification est formellement désigné auprès du correspondant métier de la Banque de France par un représentant légal de l'entité concernée. Le correspondant métier de la Banque de France, agissant en tant qu'AED, adresse à l'AE la liste des mandataires de certification habilités à faire des demandes pour un organisme.

L'entité doit signaler à l'AC, si possible préalablement mais au moins sans délai, le départ du MC de ses fonctions et, éventuellement, lui désigner un successeur.

Pour les services applicatifs (*de type entité et machine*) de la Banque de France :

Aucun mandataire de certification n'intervient dans le processus d'enregistrement d'un RC interne de la Banque de France.

Pour les services applicatifs (de type entité) appartenant à des personnes morales externes à la Banque de France :

Les RC externes sont authentifiés par un mandataire de certification formellement désigné auprès du correspondant métier de la Banque de France par un représentant légal de l'entité concernée. Une même entité peut s'appuyer sur un ou plusieurs mandataires de certification. Le correspondant métier de la

Banque de France, agissant en tant qu'AED, adresse à l'AE la liste des mandataires de certification habilités à faire des demandes pour un organisme.

L'entité doit signaler à l'AC, si possible préalablement mais au moins sans délai, le départ du MC de ses fonctions et, éventuellement, lui désigner un successeur.

1.4.6.3. 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 porteurs/services applicatifs

L'autorité de certification « Banque de France AC v3 Chiffrement » délivre exclusivement :

- Des certificats de chiffrement *pour personne physique*,
- Des certificats de chiffrement *pour une entité ou une machine*,

Certificat de chiffrement

Les porteurs de certificat de chiffrement peuvent utiliser leur certificat pour protéger en confidentialité des données (*documents, messages*) dans le cadre de leur activité professionnelle en relation avec un des métiers de la Banque de France.

Les certificats de chiffrement pour un service applicatif ont pour usage le chiffrement de données.

Les usages du certificat de chiffrement sont :

- Le déchiffrement : à l'aide de sa clef privée, un porteur déchiffre les données qui lui ont été transmises dans le cadre d'échanges dématérialisés, chiffrées à partir de sa clef publique,
- Le chiffrement : à l'aide de la clé publique du destinataire, une personne chiffre des données.

Certificat de TEST

Par ailleurs, l'AC « Banque de France AC v3 Chiffrement » délivre également des certificats à des fins de tests techniques clairement identifiés avec la mention « TEST » dans le DN du certificat émis.

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

Le bi-clef de l'autorité de certification « Banque de France AC v3 Chiffrement » est utilisé uniquement pour :

- signer les certificats de porteurs/services applicatifs qu'elle émet ;
- signer les listes de certificats révoqués (LCR) qu'elle émet ;
- signer les certificats des répondeurs OCSP.

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 Chiffrement » 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 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/RC et des utilisateurs de certificats :

Information publiée	Emplacement de publication
PC de l'AC « *Banque de France AC v3 Chiffrement* »	• 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 Les certificats des AC suivantes y sont publiés : • « *Banque de France AC v3 Racine* » • « *Banque de France AC v3 Chiffrement* » 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 • Empreinte du certificat de l'AC « *Banque de France AC v3 Chiffrement* » : 39742a74758ea3cca6fe82727471a3d74e744d79
Dossier d'enregistrement	Les documents constitutifs du dossier d'enregistrement sont disponibles sur le site de publication : • http://pc.igcv3.certificats.banque-france.fr
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
LCR de l'AC « *Banque de France AC v3 Chiffrement* »	• http://crl.igcv3.certificats.banque-france.fr/chiffrement-1.2.250.1.115.200.3.4.1.3.1.crl • http://crl.igcv3.certificats.banque-france.org/chiffrement-1.2.250.1.115.200.3.4.1.3.1.crl • ldap://ldap.igcv3.certificats.banque-france.fr/CN=Banque%20de%20France%20AC%20v3%20Chiffrement,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint • ldap://ldap.igcv3.certificats.banque-france.org/CN=Banque%20de%20France%20AC%20v3%20Chiffrement,OU=0002%20572104891,O=Banque%20de%20France,OI=NTRFR-572104891,C=FR?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
Répondeur OCSP de l'AC « *Banque de France AC v3 Chiffrement* »	• http://ocsp.igcv3.certificats.banque-france.org/chiffrement-1.2.250.1.115.200.3.5.1.3.1 • http://ocsp.igcv3.certificats.banque-france.fr/chiffrement-1.2.250.1.115.200.3.5.1.3.1

Conditions Générales d'Utilisation	Les Conditions Générales d'Utilisation (CGU) sont publiées sur le site de publication : • http://pc.igcv3.certificats.banque-france.fr

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, conditions générales d'utilisation, …*) 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.

Les certificats d'AC sont diffusés préalablement à toute diffusion de certificats de porteurs/services applicatifs 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 porteurs/RC et 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 de l'ITU.

Dans chaque certificat, le porteur/service applicatif et l'AC émettrice sont identifiés par un « Distinguished Name » (*au sens de la norme X.501 de l'ITU*). Les données d'identification du porteur figurent dans le champ « Objet » (*« Subject » en anglais*) du certificat ; les données d'identification de l'AC émettrice 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 des porteurs/services applicatifs

Identité des porteurs

L'identification des porteurs se fait en utilisant le DN dont la composition est décrite ci-dessous :

Attribut du DN	**Valeur**
Country (C)	Pays de résidence du demandeur
OrganizationName (O)	Nom officiel complet du de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
OrganizationIdentifier (OI)	Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
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 dont dépend le porteur : L'ICD est sur 4 caractères ; (0002 pour la France) L'identification de l'organisation sur 35 caractères Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
SerialNumber	Élément complémentaire permettant de distinguer les homonymes : Empreinte SHA-1 du matricule unique du porteur au sein de l'IGC.
CommonName (CN)	Le nom complet du porteur tel qu'il devrait être affiché par les applications: Le prénom d'usage du porteur, suivi d'un espace, suivi du nom de l'état civil ou du nom d'usage du porteur.

Identité des services applicatif (*entité*)

L'identification d'un service applicatif de type entité se fait en utilisant le DN dont la composition est décrite ci-dessous :

Attribut du DN	**Valeur**
Country (C)	Pays où est établie l'entité responsable du certificat
OrganizationName (O)	Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
OrganizationIdentifier (OI)	Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.
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 dont dépend le porteur : L'ICD est sur 4 caractères ; (0002 pour la France), L'identification de l'organisation sur 35 caractères, Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
OrganizationalUnitName (OU)	Nom de l'Entité
CommonName (CN)	Nom significatif du service mettant en œuvre le certificat Entité

Identité des services applicatifs (*machine*)

L'identification d'un service applicatif de type machine se fait en utilisant le DN dont la composition est décrite ci-dessous :

Attribut du DN	**Valeur**
Country (C)	Pays dans lequel est établi ou réside le demandeur
OrganizationName (O)	Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Nom officiel complet de l'entité dont dépend le porteur telle qu'enregistrée auprès des autorités compétentes
OrganizationIdentifier (OI)	Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation.

OrganizationalUnitName (OU)	Ce champ est obligatoire si le demandeur est une personne morale, optionnel sinon. Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : L'ICD est sur 4 caractères ; (0002 pour la France) L'identification de l'organisation sur 35 caractères Le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.
OrganizationalUnitName (OU)	Nom de l'application rattachée au certificat
CommonName (CN)	Nom Commun de la machine / serveur.

3.1.2.2. Certificats de test

Les certificats de porteur de test sont identifiables par le fait que l'attribut CN du DN contient le mot « TEST », précédant un prénom et un nom.

Les certificats de services applicatifs de test sont identifiables par le fait que l'attribut CN du DN contient le mot « TEST », précédant le nom significatif du service.

3.1.3. Anonymisation ou pseudonymisation des porteurs/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

Les règles suivantes sont appliquées par la Banque de France :

- Tous les caractères sont au format UTF8String ou PrintableString ;
- L'attribut CN du DN des certificats de chiffrement pour les porteurs comporte le premier prénom du porteur suivi d'un espace puis du nom du porteur (*pour les femmes mariées, le nom d'usage peut être inscrit à la suite du nom patronymique*) ;
- Les prénoms et noms composés, utilisent le tiret (trait d'union "-") comme élément séparateur ;
- L'attribut CN du DN des certificats de services applicatifs contient obligatoirement le nom significatif du service (*pour une entité*) ou du serveur (*pour une machine*) mettant en œuvre le certificat.

3.1.5. Unicité des noms

Le champ DN Subject identifie un porteur/service applicatif de façon unique au sein du domaine de l'AC « Banque de France AC v3 Chiffrement ».

Pour un certificat de chiffrement délivré à un porteur, l'unicité du DN sur le domaine de l'AC est assurée par l'attribut « *SerialNumber* » présent dans le DN et contenant :

- L'empreinte (SHA1) du numéro de matricule unique pour un porteur interne à Banque de France,
- L'empreinte (SHA1) de l'adresse email du porteur externe à Banque de France. L'adresse email est une donnée unique au sein du système de gestion des identités des utilisateurs de la Banque de France. Une adresse email ne peut être rattachée qu'à un seul utilisateur.

Pour un certificat de service applicatif, l'unicité du DN sur le domaine de l'AC est assurée par le couple d'attributs CN et O contenant respectivement le nom de service applicatif et le nom complet de l'entité responsable du certificat. Le nom du service applicatif rattaché à une entité ne peut être attribué à une autre entité.

3.1.6. Identification, authentification et rôle des marques déposées

L'AC ne peut voir sa responsabilité engagée en cas d'utilisation illicite par les porteurs/services applicatifs des marques déposées, des marques notoires et des signes distinctifs.

3.2. Validation initiale de l'identité

Un certificat établit un lien de confiance entre le porteur/service applicatif et la clef publique qui y figure. La validation initiale de l'identité d'un porteur, d'un RC le cas échéant, d'un mandataire de certification et d'un organisme fonde la confiance portée aux certificats émis par l'AC « Banque de France AC v3 Chiffrement ».

- Pour un certificat de porteur :
  - L'enregistrement d'un porteur interne de la Banque de France est réalisé sans MC.
  - L'enregistrement d'un porteur externe à la Banque de France est réalisé obligatoirement auprès d'un MC de l'entité du porteur.

- Pour un certificat de service applicatif pour une entité :
  - En interne Banque de France, l'enregistrement du service pour lequel le certificat doit être délivré se fait via l'enregistrement d'un RC interne de la Banque de France et sans MC
  - En externe Banque de France, l'enregistrement du service pour lequel le certificat doit être délivré se fait via l'enregistrement d'un RC externe de la Banque de France, qui est réalisé obligatoirement auprès d'un MC de l'entité du RC

- Pour un certificat de service applicatif pour une machine (*exclusivement au sein de la Banque de France*), l'enregistrement du serveur pour lequel le certificat doit être délivré se fait via l'enregistrement d'un RC interne de la Banque de France et sans MC.

Lorsque son intervention est nécessaire, le MC est préalablement enregistré par l'AE ou son enregistrement a lieu au moment du dépôt de la demande de certificat.

L'AC « Banque de France AC v3 Chiffrement » distingue donc plusieurs cas au cours desquels la validation initiale de l'identité d'une personne physique et/ou d'une entité a lieu :

- **Enregistrement d'un porteur sans MC :** enregistrement au cours duquel l'identité « personne physique » du futur porteur et son rattachement à l'entité sont vérifiés et validés directement par l'AE,

- **Enregistrement d'un RC sans MC pour un certificat de service applicatif à émettre ou d'un nouveau RC pour un certificat de service applicatif déjà émis :** enregistrement au cours duquel l'identité « personne physique » du futur RC, son habilitation à être RC pour le service applicatif considéré et l'entité considéré sont vérifiées et validées directement par l'AE,

- **Enregistrement d'un MC :** enregistrement au cours duquel l'identité « personne morale » de l'entité pour laquelle le MC interviendra, l'identité « personne physique » du futur MC et son rattachement à l'entité sont vérifiés et validés par l'AE,

- **Enregistrement d'un porteur via un MC :** enregistrement au cours duquel l'identité « personne physique » du futur porteur et son rattachement à l'entité pour laquelle le MC intervient sont vérifiés et validés par le MC,

- **Enregistrement d'un RC via un MC pour un certificat de service applicatif (entité) à émettre**: enregistrement au cours duquel l'identité « personne physique » du futur RC, son habilitation à être RC pour le service applicatif considéré et l'entité considérée, ainsi que son rattachement à l'entité pour laquelle le MC intervient sont vérifiés et validés par le MC.

Les différents cas d'enregistrement sont détaillés au chapitre 3.2.3.

3.2.1. Méthode pour prouver la possession de la clef privée

Un certificat établit un lien de confiance entre un porteur/service applicatif et une clef publique et donc une clef privée.

Pour un certificat de chiffrement de porteur/service applicatif, la bi-clef est générée par l'AC.

3.2.2. Validation de l'identité d'un organisme

Les porteurs de certificat de chiffrement utilisent leur certificat dans le cadre de leur activité en relation avec l'organisme dont ils dépendent et peuvent donc engager juridiquement cet organisme. Par conséquent, l'identité des organismes est vérifiée lors de la validation de l'identité du porteur.

Les certificats de chiffrement pour un porteur sont délivrés exclusivement :

- A des agents de la Banque de France (*cas des porteurs internes*),

- Ou à des personnels appartenant à des organismes en relation avec la Banque de France (*cas des porteurs externes*). En interne Banque de France, chaque métier est garant de la relation établie entre la Banque de France et les organismes.

Les certificats de chiffrement pour un service applicatif de type entité sont délivrés

sont délivrés exclusivement :

- A des services applicatifs de la Banque de France sous la responsabilité d'un RC appartenant à la Banque de France (*cas des RC internes*),
- Ou à des services applicatifs appartenant à des organismes en relation avec la Banque de France, et sous la responsabilité d'un RC appartenant à l'organisme (*cas des RC externes*)

Les certificats de chiffrement de service applicatif de type machine sont délivrés exclusivement à des serveurs de la Banque de France sous la responsabilité d'un RC appartenant à la Banque de France.

La validation de l'identité d'une entité :

- Est considérée comme réalisée pour les demandes de certificat pour des porteurs internes Banque de France et pour des services applicatifs (*entité et machine*) internes Banque de France,
- Est réalisée dans le cadre de l'enregistrement auprès de l'AE du Mandataire de Certification (MC) de cette entité pour les demandes de certificat à destination des porteurs externes à la Banque de France et pour des services applicatifs (entité) externes Banque de France. À cette occasion, un justificatif officiel de l'identité de l'entité doit être fourni.

Une AED peut être amenée à vérifier et transmettre cette pièce justificative à l'AE.

La validation de l'identité d'une entité est détaillée dans le chapitre 3.2.3.

3.2.3. Validation de l'identité d'un individu

Sont considérés comme individus les porteurs ou futurs porteurs, les RC le cas échéant, les mandataires de certification, et les représentants légaux d'organismes.

3.2.3.1. Enregistrement d'un MC

L'intervention d'un MC est obligatoire pour toute demande de certificat de porteur pour une personne externe à la Banque de France, ou pour une demande de certificat de service applicatif (entité) pour un service externe à la Banque de France.. Par conséquent, cette section concerne exclusivement l'enregistrement d'un MC d'une entité externe à la Banque de France.

Les MC sont enregistrés auprès de l'AE afin que celle-ci puisse vérifier leur habilitation à adresser des demandes.

Le dossier d'enregistrement d'un MC sert également de référence pour identifier formellement l'entité de rattachement des futurs porteurs externes à la Banque de France présentés par ce MC.

Éventuellement, un MC peut demander des certificats émis par l'AC « Banque de France AC v3 Chiffrement » pour son compte propre.

Le MC est nommé par un représentant légal de l'organisme auquel il appartient.

L'enregistrement d'un MC s'appuie sur la fourniture d'un dossier d'enregistrement comprenant :

- un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le MC. Ce mandat doit être signé par le MC pour acceptation ;

- un engagement signé, et daté de moins de 3 mois donné par le MC à l'AC d'effectuer correctement et de façon indépendante les contrôles des dossiers des demandeurs ;

- un engagement signé, et daté de moins de 3 mois, du MC de signaler à l'AE son départ de l'entité ;

- toute pièce, valide lors de la demande de certificat (*extrait Kbis, ou Certificat d'identification au Répertoire national des entreprises et de leurs établissements, ou inscription au répertoire des métiers, ...*), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce équivalente attestant de l'identification unique de l'entreprise qui figurera dans le certificat ;

- un document officiel d'identité en cours de validité du MC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie.

- un document officiel d'identité en cours de validité du représentant légal comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie.

- Un engagement signé, et daté de moins de 3 mois, du MC de ne valider des demandes de certificats qu'à des utilisateurs en relation avec un des métiers de la Banque de France (respecter les conditions d'utilisation décrites dans les PC).

Le cas échéant, l'AED vérifie, signe et transmet le dossier d'enregistrement complet d'un MC Externe à l'AE.

Un compte utilisateur sur le système de gestion des identités de la Banque de France est créé pour tout MC enregistré (*MC interne et MC externe*).

Le MC est informé que l'utilisation de son compte utilisateur est nécessaire pour authentifier toute demande de révocation depuis l'interface de gestion des certificats.

3.2.3.2. Enregistrement d'un porteur sans MC

Cette section concerne exclusivement les porteurs internes de la Banque de France. L'intervention d'un MC (*MC interne*) n'est pas prévue dans leur cas.

Pour une demande de certificat de chiffrement, le futur porteur :

- Doit être un agent de la Banque de France,
- Doit disposer d'un compte utilisateur sur le système de gestion des identités de la Banque de France.

Pour une demande de certificat dans le cadre du badge agent :

Tout agent de la Banque de France est doté d'un badge agent unique sur lequel un certificat de chiffrement émis par l'AC « Banque de France AC v3 Chiffrement » est généré, sans nécessité de constituer un dossier d'enregistrement.

La validation de l'identité du porteur est effectuée par les processus RH d'arrivée, et à la remise du badge agent après contrôle d'identité en face à face.

Pour une demande de certificat en dehors du cadre du badge agent :

Tout agent de la Banque de France a la possibilité de demander un certificat de chiffrement directement auprès de l'AC « Banque de France AC v3 Chiffrement » sans nécessité de constituer un dossier d'enregistrement.

Le porteur est informé que l'utilisation de son compte utilisateur ou de son badge agent est nécessaire pour authentifier toute demande de certificat ou toute demande de révocation.

Le porteur est également informé des conditions de séquestre de la clef privée correspondante à son certificat.

La validation de l'identité d'un porteur interne à la Banque de France est effectuée par les processus RH d'arrivée. Suite à ces processus, un compte utilisateur est créé sur le système de gestion des identités de la Banque de France, et le porteur est doté d'un badge agent contenant des certificats d'authentification et des certificats de signature émis par l'AC « Banque de France AC v3 ID Forte ». Le porteur doit par la suite utiliser ce compte utilisateur ou son badge agent pour authentifier toute demande de certificat, ou demande de révocation.

3.2.3.3. Enregistrement sans MC d'un RC pour un certificat de service applicatif à émettre ou d'un nouveau RC pour un certificat de service applicatif déjà émis

Cette section concerne exclusivement les agents de la Banque de France. L'intervention d'un MC (*MC interne*) n'est pas prévue dans leur cas.

Pour une demande de certificat de service applicatif (*pour une entité ou une machine*) à émettre, le futur RC :

- Doit être un agent de la Banque de France ,
- Doit disposer d'un compte utilisateur sur le système de gestion des identités de la Banque de France.

Le RC est informé que l'utilisation de son compte utilisateur ou de son badge agent est nécessaire pour authentifier toute demande de certificat ou toute demande de révocation.

Le RC est également informé des conditions de séquestre de la clef privée correspondante au certificat émis pour le service applicatif dont il est responsable.

La validation de l'identité d'un RC à la Banque de France est effectuée par les processus RH à l'embauche. Suite à ces processus, un compte utilisateur est créé sur le système de gestion des identités de la Banque de France, et

le porteur est doté d'un badge agent contenant des certificats d'authentification et des certificats de signature émis par l'AC « Banque de France AC v3 ID Forte » Le RC doit par la suite utiliser ce compte utilisateur, ou son badge agent, pour authentifier toute demande de certificat, ou demande de révocation.

Pour un service applicatif de type entité

Tout agent de la Banque de France peut être un RC pour l'entité à laquelle il est rattaché.

Pour un service applicatif de type machine

Un agent de la Banque de France et responsable de l'exploitation d'une machine est reconnu comme tel sur le système de gestion des identités de la Banque de France et par conséquent reconnu comme RC de la machine concernée sur l'IGCv3.

Pour un certificat de service applicatif (*pour une entité ou une machine*) déjà émis :

Un certificat d'entité est rattaché au RC qui a fait la demande (*et qui reçoit le certificat*). Un changement de cet utilisateur *a posteriori* n'est pas possible sans révocation du certificat.

Un certificat de machine est rattaché à une application et au RC qui a fait la demande et a reçu le certificat. Le changement de cet utilisateur *a posteriori* n'est pas possible sans révocation du certificat.

Par ailleurs, une application est identifiée par des Responsables d'Application, qui reçoivent les notifications liées au cycle de vie de certificat. Le changement d'un Responsable d'Application est possible à tout moment, mais il n'y a pas de lien direct entre le Responsable de l'Application et le RC (*utilisateur ayant fait la demande*).

3.2.3.4. Enregistrement d'un porteur via un MC

Cette section concerne exclusivement les porteurs externes à la Banque de France. Ces derniers doivent être authentifiés par un MC de leur entité (*MC externe*) qui doit constituer un dossier d'enregistrement.

Pour une demande de certificat de chiffrement, le futur porteur :

- Doit disposer d'un compte utilisateur sur le système de gestion des identités de la Banque de France. S'il ne dispose pas de compte utilisateur, celui-ci est créé lors de la demande de certificat.

Pour une demande de certificat pour un porteur de son périmètre, le MC constitue et transmet à l'AE un dossier d'enregistrement contenant :

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

Le porteur est informé que l'utilisation de son compte utilisateur est nécessaire pour authentifier toute demande de révocation depuis l'interface de gestion des certificats.

3.2.3.5. Enregistrement d'un RC via un MC pour un certificat de service applicatif à émettre ou d'un nouveau RC pour un certificat de service applicatif déjà émis

Cette section concerne exclusivement les RC externes de la Banque de France. Ces derniers doivent être authentifiés par un MC de leur entité (*MC externe*) qui doit constituer un dossier d'enregistrement.

Pour une demande de certificat de service applicatif (*pour une entité)* à émettre, le futur RC :

- Doit disposer d'un compte utilisateur sur le système de gestion des identités de la Banque de France. S'il ne dispose pas de compte utilisateur, celui-ci est créé lors de la demande de certificat.

Pour une demande de certificat pour un RC de son périmètre, le MC constitue et transmet à l'AE un dossier d'enregistrement contenant :

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

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

Le RC est informé que l'utilisation de son compte utilisateur est nécessaire pour authentifier toute demande de révocation depuis l'interface de gestion des certificats.

Pour un certificat de service applicatif (*pour une entité*) déjà émis :

Un certificat d'entité est rattaché au RC qui a fait la demande (*et qui reçoit le certificat*). Un changement de cet utilisateur *a posteriori* n'est pas possible sans révocation du certificat.

3.2.4. Informations non vérifiées du porteur

Seuls l'UPN et l'adresse email du porteur ne font l'objet d'aucune vérification.

3.2.5. Validation de l'autorité du demandeur

La validation de l'autorité du MC, lorsque son intervention est nécessaire, est effectuée par l'AE au moment de son enregistrement.

Pour les agents de la Banque de France, aucune vérification particulière n'est nécessaire. Tout agent de la Banque de France est habilité à demander un certificat de porteur pour lui-même ou pour un service applicatif en fonction de ses habilitations sur l'IGCv3.

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 du bi-clef d'un porteur/service applicatif entraîne automatiquement la génération et la fourniture d'un nouveau certificat.

Un nouveau certificat ne peut pas être fourni au porteur/service applicatif sans renouvellement du bi-clef correspondant (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, 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 porteurs/services applicatifs peuvent être révoqués.

La demande de révocation peut être effectuée via :

- un service en ligne après authentification sur le Portail Utilisateur, accessible sur le lien suivant : https://igcv3.certificats.banque-france.fr,
- par courriel (1206-r4f-ut@banque-france.fr), ou via un canal de communication sécurisé proposé par la Banque de France,
- ou par courrier (Banque de France, 39 rue croix des petits champs, S1A-1206 Cellule R4F, 75001 Paris).

Lorsque la demande de révocation est faite via le service en ligne, le demandeur est formellement authentifié par vérification de son identifiant et mot de passe (initialement transmis lors de son enregistrement) lui permettant d'accéder au service de révocation en ligne.

Lorsque la demande de révocation est effectuée par courrier ou par courriel, elle doit être signée par le demandeur et être accompagnée d'une copie de la pièce d'identité du demandeur (notamment carte nationale d'identité, passeport ou carte de séjour), et le service de gestion des révocations s'assure de l'identité du demandeur

(vérification de la signature manuscrite par rapport à la signature préalablement enregistrée) et de son autorité par rapport au certificat à révoquer.

4. Exigences opérationnelles sur le cycle de vie de certificats

4.1. Demande de certificat

Selon le cas, une demande de certificat peut être effectuée par tout ou partie des acteurs listés ci-dessous et disposant d'un compte sur le système de gestion des identités de la Banque de France :

- Le futur porteur / futur RC (*dans le cas d'un certificat de service applicatif*)
- Un MC habilité à demander des certificats (*exclusivement dans le cas d'un porteur ou d'un RC externe à la Banque de France*),

4.1.1. Origine d'une demande de certificat

4.1.1.1. Pour un certificat de porteur

Une demande de certificat de chiffrement pour un porteur peut être effectuée pour le compte :

- D'un agent de la Banque de France :
  Pour une demande de certificat dans le cadre du badge agent :
  La demande de certificat de chiffrement fait partie du processus RH d'attribution du badge agent.
  Pour une demande de certificat en dehors du cadre du badge agent :
  Dans ce cas, une demande de certificat émane du futur porteur.

- D'une personne externe à la Banque de France : dans ce cas, une demande de certificat ne peut être adressée à l'AE que par un MC avec consentement préalable du futur porteur.

4.1.1.2. Pour un certificat de service applicatif

Une demande de certificat de chiffrement pour un service applicatif ne peut être effectuée que pour le compte :

- D'une entité interne de la Banque de France : dans ce cas, la demande de certificat émane d'un agent de la Banque de France rattaché à l'entité concernée sur l'IGC.
- D'une entité externe de la Banque de France : dans ce cas, la demande de certificat ne peut être adressée à l'AE que par un MC externe avec consentement préalable du futur RC.
- D'une machine interne de la Banque de France : dans ce cas, la demande de certificat émane d'un agent de la Banque de France déclaré comme responsable de l'exploitation de l'application en lien avec la machine concernée sur l'IGC.

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

Une demande de certificat pour un porteur ou pour un service applicatif est initiée :

- Soit directement par l'AE dans le cadre d'attribution du badge agent (Exclusivement pour les porteurs internes Banque de France),
- Soit directement par le futur porteur/RC à partir du Portail Utilisateur (Exclusivement dans le cas où le porteur/RC est un agent de la Banque de France),

- Soit par papier directement auprès de l'AE,

Dans tous les cas :

- Le porteur/RC est informé du séquestre de la privée correspondant au certificat sur lequel porte la demande,
- La demande de certificat est traitée par l'AE.

Demande initiée par l'AE dans le cadre de l'attribution du badge agent :

Dans ce cas précis, le futur porteur est un agent de la Banque de France et son enregistrement suit les actions suivantes :

- Lors du processus RH d'attribution d'un badge agent, une demande de certificat de chiffrement est faite pour le compte du futur porteur (agent Banque de France),
- L'AE déclenche l'émission du certificat de chiffrement sur le badge agent.

Demande initiée par l'AE dans le cadre de l'attribution du badge agent temporaire :

Dans ce cas précis, le futur porteur est un agent de la Banque de France et son enregistrement suit les actions suivantes :

- En cas de perte, vol ou oubli d'un badge agent, un agent de la Banque de France peut demander un badge agent temporaire le temps de l'attribution d'un nouveau badge agent nominal,
- L'AE ou l'AED vérifie l'identité du futur porteur en face à face et lui délivre un badge agent temporaire,
- L'AE déclenche l'émission du certificat de chiffrement sur le badge agent temporaire.

Demande initiée par le futur porteur/RC sur le portail Utilisateur sans MC :

Dans ce cas précis, le futur porteur/RC est un agent de la Banque de France et son enregistrement suit les actions suivantes :

- Le futur porteur/RC initie une demande de certificat sur le Portail Utilisateur :
  - Cas du porteur : pour lui-même,
  - Cas du RC :
    - Pour un service applicatif de type entité uniquement pour l'entité à laquelle il est rattaché sur l'IGCv3,
    - Pour un service applicatif de type machine uniquement pour un serveur lié à l'application pour laquelle il est déclaré comme responsable d'exploitation sur l'IGCv3.
- Le futur porteur/RC accepte les conditions générales d'utilisation en ligne avant de soumettre la demande,
- L'AE reçoit une notification de la création de la demande de certificat sur le portail,
- A réception de la demande électronique sur le Portail de Gestion, l'AE contrôle la complétude de la demande,
- Si la demande électronique est complète, l'AE valide la demande de certificat et déclenche l'émission du certificat.

Demande initiée directement au format papier auprès de l'AE :

La demande de certificat peut être initiée directement auprès de l'AE au format papier. Ce dispositif ne concerne que les demandes de certificat nécessitant l'intervention d'un MC (*demandes pour les porteurs externes à la Banque de France*).

Le cas échéant, les éléments du dossier de demande de certificat, ainsi que ceux de l'enregistrement du MC, sont téléchargeables sur le site institutionnel de la Banque de France.

Dans ce cas :

- Le MC télécharge le dossier de demande de certificat vierge disponible sur le site institutionnel de la Banque de France,
  - Le dossier de demande contient les éléments de la demande de certificat et le cas échéant les éléments du dossier d'enregistrement du MC si celui-ci n'est pas encore enregistré.
- Le MC imprime le dossier de demande et échange avec le futur porteur pour signer conjointement le dossier de demande imprimé.
- Le MC transmet à l'AE le dossier de demande papier complet et signé.
- A réception du dossier papier complet et signé, l'AE contrôle le dossier puis crée la demande de certificat sur le Portail de Gestion et déclenche l'émission du certificat.

4.1.2.1. Pour un certificat de porteur

Une demande de certificat de chiffrement pour un porteur contient *a minima* les informations suivantes :

- les nom et prénom(s) du porteur ;
- le matricule du porteur (*dans le cas d'un porteur interne Banque de France*) ;
- l'adresse électronique du porteur ;
- la dénomination de l'entité du porteur et son identifiant (numéro SIREN ou SIRET) ;

4.1.2.2. Pour un certificat de service applicatif de type entité

Une demande de certificat de chiffrement pour un service applicatif de type entité contient *a minima* les informations suivantes :

- Le nom significatif de l'entité ou du service ;
- Les nom et prénom(s) du RC ;

- Le matricule du RC ;
- L'adresse électronique du RC ;
- La dénomination de l'entité et son identifiant (numéro SIREN ou SIRET) ;

4.1.2.3. Pour un certificat de service applicatif de type machine

Une demande de certificat de chiffrement pour un service applicatif de type machine contient *a minima* les informations suivantes :

- Le nom significatif du serveur ;
- Les nom et prénom(s) du RC ;
- Le matricule du RC ;
- L'adresse électronique du RC ;
- La dénomination de l'entité à laquelle le serveur est rattaché et son identifiant (numéro SIREN ou SIRET) ;

4.2. Traitement d'une demande de certificat

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

Les identités "personne physique" et "personne morale" sont vérifiées conformément aux exigences du chapitre 3.2.

Les processus d'identification et de validation de la demande sont explicités au chapitre 4.1.2.

A l'issue de la validation de la demande, l'AE émet la demande de génération du certificat vers la fonction adéquate de l'IGC (*cf. chapitre 1.4.1*).

L'AE conserve ensuite une trace des justificatifs d'identité présentés en particulier dans le cas d'une demande de certificat pour un porteur/RC externe de la Banque de France, sous forme d'une photocopie.

4.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le porteur/RC et le MC le cas échéant en indiquant les raisons du rejet.

En cas d'acceptation, l'AE procède à la délivrance du certificat.

4.2.3. Durée d'établissement du certificat

Tout dossier complet est traité dans les 10 jours ouvrés suivant la réception de la demande.

4.3. Délivrance du certificat

Lorsque la demande est validée par l'AE, cette dernière déclenche le processus de génération de certificat auprès de la fonction de gestion de certificats de l'AC.

Délivrance d'un certificat de porteur sur un nouveau badge agent :

Ce mode de délivrance concerne exclusivement les agents de la Banque de France. La génération des certificats sur un nouveau badge agent est faite par l'AE.

Les certificats et les clefs privées associées sont générés par l'AC et stockés dans un dispositif de protection (badge agent). Celui-ci est remis au porteur en face à face par l'AE ou par l'AED. Le dispositif de protection respecte les exigences du chapitre 12 de ce document, et a fait l'objet d'une certification CC EAL4+.

L'utilisation de la clef privée est protégée par la saisie de « données d'activation » (*code PIN*) que le porteur récupère en s'authentifiant sur le Portail Utilisateur. Après authentification, les données d'activation sont accessibles pour un accès unique sur le Portail Utilisateur.

Délivrance d'un certificat de porteur sur un badge agent temporaire :

Ce mode de délivrance concerne exclusivement les agents de la Banque de France. La génération des certificats sur le badge agent temporaire est faite par le futur porteur depuis son Portail Utilisateur.

Les certificats et les clefs privées associées sont générés par l'AC et stockés dans un dispositif de protection (badge agent temporaire). Celui-ci est remis au porteur au préalable lors d'un face à face. Le dispositif de protection respecte les exigences du chapitre 12 de ce document, et a fait l'objet d'une certification CC EAL4+.

L'utilisation de la clef privée est protégée par la saisie de « données d'activation » (code PIN) que le porteur choisit lors de la génération des certificats depuis le Portail Utilisateur.

Délivrance d'un certificat de porteur sur un badge agent déjà en possession du futur porteur :

Ce mode de délivrance concerne exclusivement les agents de la Banque de France. La génération des certificats sur un dispositif de sécurité déjà en possession du futur porteur est faite par le futur porteur depuis son Portail Utilisateur.

Les certificats et les clefs privées associées sont générés par l'AC et stockés dans le dispositif de protection déjà en possession du porteur. Le dispositif de protection respecte les exigences du chapitre 12 de ce document, et a fait l'objet d'une certification CC EAL4+.

L'utilisation de la clef privée est protégée par la saisie de « données d'activation » (code PIN) du dispositif existant.

Délivrance d'un certificat de porteur/service applicatif en dehors du badge agent :

Le certificat de chiffrement pour un porteur/service applicatif et la clef privée associée sont générés et stockés par l'AC dans une archive logicielle protégée par un mot de passe. L'archive logicielle est transmise par voie électronique au porteur/RC à travers le Portail Utilisateur, et est accessible après authentification en accès-unique.

L'utilisation de la clef privée est protégée par la saisie de « données d'activation » (*mot de passe*) que le porteur/RC récupère en s'authentifiant sur le Portail Utilisateur.

La récupération des données d'activation ne peut se faire que si l'archive logicielle a été récupérée au préalable sur le Portail Utilisateur. Les données d'activation ne sont pas rendues disponibles en même temps que l'archive logicielle sur le Portail Utilisateur.

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

Pour toute demande de certificat de chiffrement pour un porteur, l'AC effectue les opérations suivantes :

- Authentification de l'origine de la demande (AE) ;
- Vérification de l'intégrité de la demande ;
- Vérification technique de la demande ;
- Génération de la bi-clef par l'AC ;
- Création du certificat du futur porteur ;
- Signature du certificat à l'aide de la clef privée de l'AC ;
- Création de l'archive logicielle contenant la clef privée et le certificat ;

Pour toute demande de certificat de chiffrement pour un service applicatif de type entité et machine, l'AC effectue les opérations suivantes :

- Authentification de l'origine de la demande (AE) ;
- Vérification de l'intégrité de la demande ;
- Vérification technique de la demande ;
- Génération de la bi-clef par l'AC ;
- Création du certificat du service ;
- Signature du certificat à l'aide de la clef privée de l'AC ;
- Création de l'archive logicielle contenant la clef privée et le certificat ;

L'ensemble de ces opérations est détaillé dans la DPC.

Les conditions de génération des clefs et des certificats, les mesures de sécurité à respecter, sont précisées dans les chapitres 5 et 6.

4.3.2. Notification par l'AC de la délivrance du certificat au porteur/RC

L'AC notifie au porteur/RC la délivrance du certificat et la mise à disposition de l'archive logicielle contenant le certificat. Le porteur/RC est invité à récupérer l'archive logicielle sur le Portail Utilisateur.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

L'acceptation d'un certificat vaut acceptation de la PC de l'AC « Banque de France AC v3 Chiffrement ».

4.4.1.1. Pour un certificat de porteur

La démarche d'acceptation est réalisée une fois que le porteur a récupéré successivement l'archive logicielle contenant le certificat et le mot de passe associé sur le Portail Utilisateur.

L'acceptation du certificat par le porteur est réalisée en ligne sur le Portail Utilisateur.

Le porteur dispose d'un délai de 21 jours pour accepter son certificat. Passé ce délai, l'AC prend des mesures allant jusqu'à la révocation du certificat.

Toutefois, le porteur est tenu d'avertir l'AE et son MC le cas échéant de toute inexactitude ou défaut du certificat ou de l'archive logicielle envoyée à la réception de son certificat. Le cas échéant, le certificat est révoqué par l'AC.

En cas de refus explicite du certificat par le porteur, le certificat est révoqué par l'AC.

Dans le cadre du badge agent :

- L'acceptation des certificats n'est pas requise lors de la remise du badge initiale, ou lors de la génération de certificat sur un badge temporaire.
- L'acceptation des certificats est requise lors d'une demande de certificat sur un badge existant.

Acceptation en ligne

À l'issue de la récupération du mot de passe, le porteur est invité à vérifier les informations du certificat (*a minima le DN du certificat et le numéro de série*). À cette occasion, les informations du certificat sont présentées au porteur qui doit confirmer que celles-ci sont correctes ou non.

4.4.1.2. Pour un certificat de service applicatif de type entité ou de machine

La démarche d'acceptation est réalisée une fois que le RC a récupéré successivement l'archive logicielle contenant le certificat et le mot de passe associé sur le Portail Utilisateur.

L'acceptation du certificat entité par le RC est réalisée en ligne sur le Portail Utilisateur.

Le RC dispose d'un délai de 21 jours pour accepter le certificat. Passé ce délai, l'AC prend des mesures allant jusqu'à la révocation du certificat.

Toutefois, le RC est tenu d'avertir de toute inexactitude ou défaut du certificat ou de l'archive logicielle envoyée à la réception du certificat. Le cas échéant, le certificat est révoqué par l'AC.

En cas de refus explicite du certificat par le RC, le certificat est révoqué par l'AC.

Acceptation en ligne

A l'issue de la récupération du certificat, le RC est invité à vérifier les informations du certificat (*a minima le DN du certificat et le numéro de série*). A cette occasion, les informations du certificat sont présentées au RC qui doit confirmer que celles-ci sont correctes ou non.

4.4.2. Publication du certificat

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

Les certificats de porteur sont publiés dans une base accessible depuis le réseau interne de la Banque de France.

Les certificats de service applicatif ne font pas l'objet d'une publication.

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

L'AE et le MC le cas échéant sont informés de la délivrance du certificat.

4.5. Usages de la bi-clef et du certificat

4.5.1. Utilisation de la clef privée et du certificat par le porteur/RC

L'utilisation de la clef privée et du certificat associé est décrite au chapitre 1.5.1, de façon limitative. Les porteurs/RC s'engagent à respecter strictement ces usages autorisés. Dans le cas contraire, leur responsabilité peut être engagée, et le certificat associé peut 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 :

- Pour les porteurs :
  - à « *keyEncipherment* » pour les certificats de chiffrement,
- Pour les services applicatifs de type entité et machine :
  - à « *keyEncipherment* » pour les certificats de chiffrement,

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 du porteur/service applicatif*). La génération d'un nouveau bi-clef est systématique pour toute délivrance d'un certificat.

Toutefois, une notification est envoyée au porteur/RC à l'approche de la date d'expiration du certificat de façon à préparer un renouvellement au sens délivrance d'un nouveau certificat (*cf. chapitre 4.7*).

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 porteurs/services applicatifs et les certificats correspondants, sont renouvelées au minimum tous les 3 ans.

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

- par anticipation,
- ou suite à la révocation du certificat du porteur/service applicatif (*cf. chapitre 4.9*).

Nota – Dans la suite du présent chapitre, le terme « fourniture d'un nouveau certificat » recouvre également la fourniture d'un nouveau bi-clef au porteur.

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

Une notification est envoyée au porteur/RC à l'approche de la date d'expiration du certificat de façon à préparer la délivrance d'un nouveau certificat.

Le déclenchement de la fourniture d'un nouveau certificat peut être :

- soit automatique (*dans le cadre de la notification d'arrivée à expiration du certificat*),
- soit à l'initiative du porteur/RC ou du MC le cas échéant.

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 3.3.

Exclusivement, les porteurs internes à la Banque de France peuvent demander le renouvellement des certificats porteurs (chiffrement) avec la réutilisation du dispositif de protection déjà en leur possession (badge agent). Dans ce cas, un contrôle est effectué par l'AC pour vérifier l'association entre le dispositif de protection et le futur porteur de certificat. Le certificat arrivant à expiration n'est pas supprimé du dispositif de protection.

4.7.4. Notification au porteur/RC 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 de toute information autre que les dates de validité, sans changement de la clef publique (cf. chapitre 4.7), 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 de porteurs/services applicatifs

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un porteur/service applicatif :

- Les informations du porteur/service applicatif figurant dans son certificat ne sont pas ou plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (*dont départ de l'entité ou changement de fonction du porteur*), ceci avant l'expiration normale du certificat ;
- Le porteur/RC n'a pas respecté les modalités d'utilisation du certificat ;
- Le porteur/RC et/ou le cas échéant le MC ou l'entité n'ont pas respecté leurs obligations découlant de la PC dont le certificat dépend ;
- Une erreur (*intentionnelle ou non*) a été détectée dans le dossier d'enregistrement du porteur/RC ;
- La clef privée associée au certificat du porteur/service applicatif est suspectée de compromission, est compromise, est perdue ou volée (*éventuellement les données d'activation associées*) ;
- Le porteur/RC ou une entité autorisée (*représentant légal de l'entité ou MC par exemple*) demande la révocation du certificat (*notamment dans le cas d'une destruction ou altération de la clef privée du porteur/service applicatif et/ou de son support*) ;
- Le décès du porteur ;
- Le départ du porteur / RC de l'entité ;
- La cessation d'activité de l'entité du porteur/RC.

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 des porteurs/services applicatifs

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

- Pour un certificat de porteur :
  - Le porteur au nom duquel le certificat a été émis,
  - Le cas échéant un MC de l'organisme du porteur (*exclusivement pour un porteur externe de la Banque de France*),
  - Un représentant légal (RL) de l'organisme du porteur,
  - L'AC ayant délivré le certificat,
  - L'AE ou l'AED rattachée à l'AC.
- Pour un certificat de service applicatif (*entité ou machine*)
  - Le RC enregistré pour le service applicatif considéré,
  - Le cas échéant un MC de l'organisme du RC (exclusivement pour un RC externe à la Banque de France),

- Un représentant légal de l'organisme du RC,
- L'AC ayant délivré le certificat,
- L'AE ou l'AED rattachée à l'AC.

L'authentification du demandeur et la vérification de la validité de la demande se font selon les modalités définies dans le paragraphe 3.3.2.

Le porteur est informé d'une demande de révocation de son certificat par les personnes ou entités à l'origine de cette demande.

Le RC est informé d'une demande de révocation du certificat dont il a la responsabilité par les personnes ou entités à l'origine de cette demande.

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

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

4.9.3.1. Certificats de porteurs/services applicatifs

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 du porteur/service applicatif figurant dans le certificat (*nom et prénom / nom du service ou du serveur*) ;
- Le nom du demandeur de la révocation ;
- 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'AE révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée par un répondeur en temps réel (OCSP) et en faisant introduire le numéro de série du certificat et la date de révocation dans la Liste de certificats révoqués (LCR).

Si la demande n'est pas recevable, l'AE en informe le demandeur, par l'intermédiaire de l'AED ou du MC le cas échéant.

Le demandeur, le porteur/RC et le MC le cas échéant, sont informés par email de la prise en compte de la demande de révocation via accusé de réception émanant de l'AE.

L'opération de révocation est enregistrée dans les journaux d'événements de l'AC « Banque de France AC v3 Chiffrement ». L'AE enregistre et archive les demandes de révocation.

Les causes de révocation définitive des certificats ne sont pas publiées. Tout certificat révoqué est systématiquement retiré de la base accessible en interne le cas échéant.

Des précisions, concernant la procédure de traitement de révocation, sont apportées dans la DPC.

4.9.3.2. Certificats d'une composante de l'IGC

La procédure à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC est décrite dans la DPC.

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

- Informer l'ensemble des porteurs/RC concernés dans les plus brefs délais, via leur MC, 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 au porteur/RC pour formuler la demande de révocation

Dès que le porteur/RC a connaissance de la survenance d'une des causes possibles de révocation, de son ressort, il 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 de porteurs/services applicatifs

L'AE traite dès réception les demandes qui lui parviennent.

La LCR est mise à jour de préférence immédiatement ou dans un délai maximal de 24h à compter de la date de réception de la demande de révocation authentifiée.

La fonction de gestion des révocations est disponible 24h/24 et 7j/7.

Cette fonction a une durée maximale d'indisponibilité par interruption de service (*panne ou maintenance*) conforme à 2h et une durée maximale totale d'indisponibilité par mois conforme à 8h.

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 de porteur/service applicatif 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 LCR sont générées au maximum toutes les 24 heures.

4.9.8. Délai maximum de publication d'une LCR

La LCR 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 (cf. chapitre 4.9.5.1).

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

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 de porteurs/services applicatifs

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.

Les porteurs/RC :

- Sont tenus d'interrompre immédiatement et définitivement l'usage de leur certificat de chiffrement,

- S'engagent, dans la mesure du possible, à déchiffrer les données précédemment chiffrées au moyen du certificat de chiffrement compromis et à les protéger en confidentialité par tout autre moyen.

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 fera 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 sera 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 le porteur/RC et l'AC

En cas de fin de la relation entre le porteur et l'AC avant la fin de validité du certificat, l'AE procède à la révocation du certificat du porteur.

L'AC révoque tout certificat électronique pour lequel il n'y a plus de RC explicitement identifié.

4.12. Séquestre de clef et recouvrement

Un séquestre des clefs privées des porteurs et des services applicatifs est réalisé dans le cadre de la présente PC.

Seules les clefs privées correspondantes à des certificats de chiffrement émis par l'AC « Banque de France AC v3 Chiffrement » font l'objet d'un séquestre.

4.12.1. Politiques et pratiques de recouvrement par séquestre des clefs

4.12.1.1. Demande de séquestre

Tout demande de certificat de chiffrement (*pour un porteur ou un service applicatif*) émis par l'AC « Banque de France AC v3 Chiffrement » intègre systématiquement un séquestre de la clef privée.

Les demandes et dossiers d'enregistrement intègrent systématiquement les informations relatives au séquestre qui est obligatoire pour les certificats émis par l'AC « Banque de France AC v3 Chiffrement ».

La durée de conservation des clefs privées correspondant aux certificats de chiffrement émis par l'AC « Banque de France AC v3 Chiffrement » est de dix ans à compter de leur génération.

Le porteur/RC est informé du séquestre de la clef privée correspondant au certificat sur lequel porte sa demande ainsi que de sa durée de conservation.

4.12.1.2. Traitement d'une demande de séquestre

Une fois la demande de certificat de chiffrement validée par l'AE, celle-ci déclenche le processus d'émission du certificat comprenant la génération de la bi-clef et l'émission du certificat. La clef privée correspondant au certificat émis par l'AC « Banque de France AC v3 Chiffrement » fait systématiquement l'objet d'un séquestre suite à sa génération.

La clef privée est conservée par la fonction de séquestre et de recouvrement de l'AC sous forme chiffrée pour une durée de dix ans et est recouvrable sur cette période même si le certificat associé est expiré ou révoqué.

La clef privée conservée au sein de la fonction de séquestre et de recouvrement de l'AC est identifiée avec le numéro de série du certificat associé.

Les conditions de séquestre sont détaillées dans la DPC.

4.12.1.3. Origine d'une demande de recouvrement

Une demande de recouvrement de clef privée d'un porteur peut être effectuée par :

- Le porteur lui-même,
- Un représentant légal de l'entité du porteur,
- Le MC le cas échéant,
- L'AE,
- L'AE dans le cadre de la production d'un badge agent,
- Toute entité autorisée par la loi.

Une demande de recouvrement de clef privée d'un service applicatif peut être effectuée par :

- Le RC enregistré,
- Un représentant légal de l'entité responsable du service applicatif,
- L'AE,
- Toute entité autorisée par la loi.

4.12.1.4. Identification et validation d'une demande de recouvrement

La demande de recouvrement d'une clef privée d'un porteur/service applicatif peut être effectuée via :

- Un service en ligne,
- Par courrier (Banque de France, 39 rue croix des petits champs, S1A-1206 Cellule R4F, 75001 Paris),

Lorsque la demande de recouvrement est faite via le service en ligne, le demandeur est formellement authentifié par vérification de son identifiant et mot de passe (initialement transmis lors de son enregistrement) lui permettant d'accéder au service de recouvrement en ligne.

Lorsque la demande de recouvrement est effectuée par courrier, elle doit être signée par le demandeur et être accompagnée d'une copie d'une pièce d'identité du demandeur (*notamment carte nationale d'identité, passeport ou carte de séjour*), et le service de gestion des recouvrements s'assure de l'identité du demandeur (vérification de la signature manuscrite par rapport à la signature préalablement enregistrée) et de son autorité par rapport au certificat à révoquer.

Dans tous les cas, la demande de recouvrement comporte *a minima* :

- Le motif du recouvrement de la clef privée,
- Les informations permettant d'identifier la clef privée à recouvrer (*n° de série du certificat associé, nom du porteur associé*).

Dans le cas d'une demande de recouvrement dans le cadre de la génération d'un nouveau badge agent, l'ensemble des clés séquestrés par l'AC sont remis sur le badge agent.

4.12.1.5. Traitement d'une demande de recouvrement

Suite à l'identification et la validation de la demande de recouvrement, le service de gestion des recouvrements émet la demande auprès de la fonction de séquestre et recouvrement de l'AC. La demande est protégée en intégrité et en confidentialité.

Au moins deux opérateurs de l'AE habilités au recouvrement sont saisis pour le recouvrement de la clef privée du porteur/service applicatif. Ces opérateurs sont authentifiés par la fonction de séquestre et recouvrement préalablement à l'opération de recouvrement.

4.12.1.6. Destruction des clefs séquestrées

Dès la fin de la période de conservation d'une clef séquestrée, tout exemplaire de cette clef détenue par l'AC est détruit de manière fiable afin de ne pouvoir ni recouvrer ni reconstituer la clef.

4.12.1.7. Disponibilité des fonctions liées au séquestre et au recouvrement

La fonction de séquestre et de recouvrement est disponible 24h/24 et 7j/7.

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 de 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 du porteur/service applicatif 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 met 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 fournie 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. Évènements 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,
- envoi de l'archive logicielle contenant la clef privée et le certificat au porteur/RC,
- accusé de réception du porteur/RC
- acceptation ou rejet explicite par le porteur/RC,
- activation du support par le porteur,
- réception d'une demande de recouvrement d'une clef privée d'un porteur/service applicatif ,
- validation / rejet d'une demande de recouvrement,
- remise d'une clef privée recouvrée au demandeur du recouvrement.

5.4.1.3. Évènements 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 des porteurs/services applicatifs,
- génération des certificats des porteurs/services applicatifs,
- personnalisation des supports et génération des codes d'activation,
- publication et mise à jour des informations liées aux AC (*PC/DPC, certificats d'AC, CGU, …*)
- génération puis publication des LCR,
- requêtes et réponses OCSP,
- séquestre d'une clef privée de porteur/service applicatif,
- recouvrement d'une clef privée.

5.4.1.4. Évènements 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 (clef*s, données d'activation, mots de passe ou code porteur, …*).

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 engagements signés des MC,
- les justificatifs d'identité des porteurs/RC 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.

Les archives peuvent être mises à disposition des personnes habilitées (*définies dans la DPC relative à la présente PC*) sous deux (2) jours ouvrés.

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 dix ans à compter de la date d'acceptation du certificat par le porteur/RC.
- À l'expiration de la durée d'archivage, le dossier et les pièces justificatives font l'objet d'une destruction.

Pour les dossiers de demande de recouvrement d'une clef privée d'un porteur/service applicatif**:**

- les dossiers et les pièces justificatives sont archivés pour une durée de cinq (5) ans à compter de la date de fin du séquestre par l'AC de la clef privée correspondante.
- À l'expiration de la durée d'archivage, le dossier et les pièces justificatives font l'objet d'une destruction.

Pour les certificats et LCR émis par l'AC :

- les certificats et les LCR émis par l'AC sont conservés pendant au moins dix ans à compter de leur génération.
- À l'expiration de la durée d'archivage, les LCR 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.
- À 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 au moins dix ans à compter de leur date de génération.
- À 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 tous les porteurs/RC 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: tous les porteurs/RC 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 porteurs/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 LCR), 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 d'activité.

L'AC prévient tous les porteurs/RC, et les MC 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 porteurs/RC et les 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 LCR 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 tous les MC et/ou porteurs/RC des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement (cf. chapitre 3.2.3).

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 générés 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. La gestion de ces secrets est régie par les dispositions de la PC de l'AC racine.

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 porteurs générées par l'AC

Les clefs des porteurs sont générées par l'AC dans un environnement sécurisé. Les clefs privées générées font l'objet d'un séquestre par l'AC.

6.1.1.3. Clefs services applicatifs générées par l'AC

Les clefs des services applicatifs (*entité et machine*) sont générées par l'AC dans un environnement sécurisé. Les clefs privées générées font l'objet d'un séquestre par l'AC.

6.1.2. Transmission de la clef privée à son propriétaire

Pour les certificats de porteur dans le cadre de la délivrance d'un nouveau badge agent :

La clef privée est générée par l'AC et stockée dans le dispositif de protection (badge agent) qui est remis au porteur en face à face. Une fois remise, la clef privée est sous le contrôle exclusif du porteur.

Pour les certificats de porteur dans le cadre de la délivrance sur un dispositif déjà en possession du porteur :

La clef privée est générée par l'AC et stockée dans le dispositif de protection (badge agent) qui est déjà en possession du porteur. La clef privée est sous le contrôle exclusif du porteur.

Pour les certificats de porteur / service applicatif en dehors du badge agent :

La clef privée et le certificat associé pour un porteur/service applicatif sont générés et stockés par l'AC dans une archive logicielle protégée par un mot de passe. L'archive logicielle est transmise par voie électronique au porteur/RC à travers le Portail Utilisateur, et est accessible en accès-unique après authentification sur le Portail Utilisateur.

6.1.3. Transmission de la clef publique à l'AC

Les clefs publiques des porteurs/services applicatifs sont transmises à l'AC, aux fins de signature, dans des conditions qui garantissent leur intégrité et leur origine.

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

La clef publique de l'AC est transmise aux utilisateurs via les certificats des AC, garantissant leur intégrité et leur origine.

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 (*cf. chapitre 1.1*) ;
- 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 émettrices disposent d'une clef RSA de 4096 bits.

Les porteurs et les services applicatifs disposent d'une clef RSA d'une longueur supérieure ou égale à 2048 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.

Le bi-clef du porteur/service applicatif est généré et stocké dans une archive logicielle protégée par un mot de passe. Dans le cadre du badge agent, la bi-clef est importé sur le dispositif de protection (badge agent).

6.1.7. Objectifs d'usage de la clef

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

L'utilisation de la clef privée du porteur/service applicatif est strictement limitée au service de confidentialité.

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 Chiffrement » utilise un module cryptographique répondant aux critères communs au niveau EAL4+ et au niveau renforcé répondant ainsi aux exigences du chapitre 11.

6.2.1.2. Dispositifs de protection des porteurs

Dans le cadre du badge agent : La clef privée et le certificat associé pour un porteur sont générés et stockés par l'AC dans une archive logicielle protégée par un mot de passe. La clef et le certificat sont ensuite importés sur le dispositif de protection (badge agent).

En dehors du badge agent : La clef privée et le certificat associé pour un porteur sont générés et stockés par l'AC dans une archive logicielle protégée par un mot de passe. La clef et le certificat sont ensuite installés sur le poste de travail du porteur.

6.2.1.3. Dispositifs de protection des services applicatifs

La clef privée et le certificat associé pour un service applicatif (*entité ou machine*) sont générés et stockés par l'AC dans une archive logicielle protégée par un mot de passe. La clef et le certificat sont ensuite installés sur le serveur concerné.

6.2.2. Contrôles de la clef privée par plusieurs personnes

Le contrôle des clefs privées de l'AC 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 des AC ne sont pas séquestrées.

Les clefs privées des porteurs/services applicatifs associées aux certificats de chiffrement délivrés par l'AC « Banque de France AC v3 Chiffrement » font l'objet d'un séquestre.

6.2.4. Copies de secours de la clef privée

Les clefs privées des AC font l'objet d'une copie de secours bénéficiant du même niveau de sécurité que les clefs initiales.

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 porteurs/services applicatifs font l'objet d'un séquestre. Les conditions de séquestre et de recouvrement de ces clefs sont détaillées au chapitre 4.12.

6.2.5. Archivage de la clef privée

Les clefs privées des AC ne sont pas archivées.

Les clefs privées des porteurs/services applicatifs ne sont pas archivées.

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

Dans le cadre du badge agent : La clef privée d'un porteur est transmise par l'AC par voie électronique et importée dans un dispositif de protection (badge agent).

En dehors du badge agent : La clef privée d'un porteur/service applicatif stockée dans une archive logicielle et protégée par un mot de passe est transmise par l'AC par voie électronique directement au porteur/RC à travers le Portail Utilisateur garantissant son intégrité et sa confidentialité. L'usage d'un dispositif de protection n'est pas prévu pour la clef privée d'un service applicatif.

Le transfert de la clef privée d'AC 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. Le détail est fourni dans la DPC.

6.2.7. Stockage de la clef privée dans un module cryptographique

La clef privée d'AC est stockée dans un module cryptographique.

Cf. paragraphe 6.2.1.1.

6.2.8. Méthode d'activation de la clef privée

6.2.8.1. Clef privée d'AC

L'activation de la clef privée d'AC 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*).

6.2.8.2. Clef privée du porteur

Dans le cadre du badge agent :

La clef privée, stockée sur un dispositif de protection, est activée via la saisie d'un code PIN (*cf. chapitre 6.4*). Le code PIN est transmis par un chemin de confiance différent de celui de la clef privée.

En dehors du badge agent :

La clef privée, stockée dans une archive logicielle PKCS12, est activée via la saisie du mot de passe (*cf. chapitre 6.4*). Le mot de passe est transmis par voie électronique à travers le Portail Utilisateur.

6.2.8.3. Clef privée du service applicatif

La clef privée, stockée dans une archive logicielle PKCS12, est activée via la saisie du mot de passe (*cf. chapitre 6.4*). Le mot de passe est transmis par voie électronique à travers le Portail Utilisateur.

6.2.9. Méthode de désactivation de la clef privée

6.2.9.1. Clef privée d'AC

La désactivation des clefs privées d'AC dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

6.2.9.2. Clef privée du porteur

Dans le cadre du badge agent, la clef privée est désactivée à partir du dispositif de protection sous le contrôle exclusif du porteur.

En dehors du badge agent, la méthode de désactivation de la clef privée correspond à la suppression de celle-ci sur le poste de travail du porteur.

6.2.9.3. Clef privée du service applicatif

La méthode de désactivation de la clef privée correspond à la suppression de celle-ci sur le serveur concerné.

6.2.10. Méthode de destruction de la clef privée

6.2.10.1. Clef privée d'AC

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

6.2.10.2. Clef privée du porteur

Dans le cadre du badge agent, la destruction « logique » de la clef privée d'un porteur ne peut se faire qu'à partir du dispositif de protection. Sur demande sur papier libre signée du porteur, le dispositif de protection contenant la clef privée est physiquement détruit par les opérateurs de l'AE

En dehors du badge agent, la destruction « logique » de la clef privée d'un porteur ne peut se faire qu'à partir du poste de travail du porteur.

6.2.10.3. Clef privée du service applicatif

La destruction « logique » de la clef privée d'un service applicatif ne peut se faire qu'à partir du serveur concerné.

6.2.11. Niveau d'évaluation sécurité des modules cryptographiques

Cf. Paragraphe 6.2.1.

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 porteurs/services applicatifs ont la même durée de vie.

Cette durée de vie est de 3 ans.

La fin de vie d'un certificat d'AC 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 du porteur

Dans le cadre du badge agent :

Les clefs des porteurs sont générées par l'AC et importés sur action de l'AE au sein du dispositif de protection. Dans le cas où la clef privée est importée dans un nouveau dispositif de protection, les données d'activation (code PIN) sont transmises au porteur à l'issue de la génération de façon à garantir leur intégrité et leur confidentialité.

Dans le cas où la clef privée est importée dans le dispositif de protection déjà en possession du porteur, les données d'activation (code PIN) restent celles déjà en possession du porteur.

En dehors du badge agent :

Les clefs des porteurs sont générées par l'AC et stockées dans une archive logicielle PKCS12 et protégée par un mot de passe initialisé par l'AC. Les données d'activation (mot de passe) sont transmises au porteur de façon à garantir leur intégrité et leur confidentialité à travers le Portail Utilisateur.

L'archive logicielle PKCS12 et les données d'activation ne sont jamais disponibles en même temps sur le Portail Utilisateur. Leurs transmissions sont séparées dans le temps.

Les opérations sont décrites dans la DPC.

6.4.1.3. Génération et installation des données d'activation correspondant à la clef privée du service applicatif

Les clefs des services applicatifs sont générées par l'AC et stockées dans une archive logicielle PKCS12 et protégée par un mot de passe initialisé par l'AC. Les données d'activation (mot de passe) sont transmises au porteur de façon à garantir leur intégrité et leur confidentialité à travers le Portail Utilisateur.

L'archive logicielle PKCS12 et les données d'activation ne sont jamais disponibles en même temps sur le Portail Utilisateur. Leurs transmissions sont séparées dans le temps.

Les opérations sont décrites dans la DPC.

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 détail est fourni dans la DPC. 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 du porteur

Les données d'activation sont protégées en confidentialité jusqu'à leur remise au porteur. Lorsque ces données sont sauvegardées par l'AC, celles-ci sont protégées en confidentialité.

6.4.2.3. Protection des données d'activation correspondant à la clef privée du service applicatif

Les données d'activation sont protégées en intégrité et en confidentialité jusqu'à leur remise au RC. Lorsque ces données sont sauvegardées par l'AC, celles-ci sont protégées en intégrité et en confidentialité.

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 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

La fourniture et le renouvellement de certificats peuvent faire l'objet de frais dont les tarifs sont détaillés dans un document annexe le cas échéant (*ex : contrat commercial ou dossier de demandes de certificat*).

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 protection 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, des composantes et des porteurs/services applicatifs ;
- les données d'activation associées aux clefs privées d'AC et des porteurs/services applicatifs ;
- tous les secrets de l'IGC ;
- les journaux d'événements des composantes de l'IGC ;
- les dossiers d'enregistrement des porteurs/RC ;
- 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 porteurs/RC à des tiers dans le cadre de procédures légales.

L'AC permet également l'accès à ses informations au porteur/RC.

9.4. Protection des données personnelles

9.4.1. Politique de protection des données à caractère personnel

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.

Les données personnelles recueillis par l'AC sont exclusivement réservées au traitement de l'IGC-BDF-V3, basé sur le respect d'une obligation légale. La Banque de France, en tant qu'Autorité de Certification (AC) est responsable de ce traitement.

La finalité du traitement de l'IGC-BDF-V3 est de permettre la gestion du cycle de vie des certificats numériques : vérification de l'identité des porteurs et des mandataires de certification, création de compte utilisateur sur le système de gestion des identités et des accès de la Banque de France, génération et gestion (suivi, renouvellement, révocation et recouvrement) des certificats numériques émis par l'AC.

Les données à caractère personnel collectées par l'AC sont traitées et hébergées en France.

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

Les personnes concernées disposent d'un droit d'accès et de rectification dans les conditions prévues par le règlement (UE) 2016/679 du 27 avril 2016 qu'elle peuvent exercer en contactant l'AC Banque de France par email à l'adresse suivante : 1206-r4f-ut@banque-france.fr.

Les personnes concernées disposent de la faculté de déposer une réclamation auprès de la CNIL. Les coordonnées du Délégué à la Protection des Données de la Banque de France sont : 1200-DPD-delegue-ut@banque-france.fr.

De son côté, l'entité morale qui acquiert, via le Mandataire de Certification externe, des certificats pour ses porteurs/services applicatifs est responsable du traitement des données personnelles qu'elle met en œuvre pour gérer en interne le cycle de vie des certificats émis pour son compte par l'AC (Vérification de l'identité des porteurs / responsables de certificat).

9.4.2. Données personnelles

Les informations suivantes sont des données personnelles :

- données d'identification du porteur/RC, du mandataire de certification et du représentant légal de l'organisme en relation avec la Banque de France, du correspondant métier Banque de France ;
- données renseignées dans le dossier d'enregistrement pour la demande de certificat du porteur/service applicatif ;
- données renseignées dans la demande de révocation de certificat ;
- causes de révocations des certificats des porteurs/services applicatifs (considérées comme confidentielles, sauf accord explicite du porteur/RC pour publication) ;
- journaux d'événement de l'AC,

Les données personnelles collectées 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. L'entité morale via le MC informe également les personnes concernées du traitement qu'elle réalise à cet effet.

9.4.4. Exercice des droits des personnes

L'AC gère les demandes des personnes concernées pour les traitements qu'elle gère 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 toute 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 du porteur/RC concerné, décision judiciaire ou autre autorisation légale.

Les personnes concernées sont averties de l'utilisation faite par l'AC de ces données personnelles, à l'occasion d'acceptation des conditions générales d'utilisation faite lors de l'enregistrement. Ces conditions générales d'utilisation sont signées par les porteurs, valant acceptation et consentement.

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 à caractère personnel

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 porteurs/RC ;
- 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 a pour obligation de :

- démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un porteur/service applicatif donné et que le porteur/RC 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 raisonnables pour s'assurer que ses porteurs/RC 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 un porteur/RC et l'AC 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 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 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 porteurs/RC à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

L'AC 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. Porteurs de certificats /RC

Le porteur/RC a l'obligation de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- protéger sa clef privée/la clef privée du serveur dont il est responsable par des moyens appropriés à son environnement ;
- protéger les données d'activation et les mettre en œuvre uniquement lorsque nécessaire ;
- respecter les conditions d'utilisation de sa clef privée/la clef privée du serveur et du certificat correspondant ;
- informer l'AC 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.

La relation entre le porteur/RC et l'AC ou ses composantes est formalisée par un engagement du porteur/RC visant à certifier l'exactitude des renseignements et des documents fournis.

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, du certificat du porteur/service applicatif jusqu'à l'AC racine, 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 est responsable des exigences et des principes édictés dans la présente PC, ainsi que de tout dommage causé à un porteur/RC ou utilisateur de certificat résultant d'un manquement aux procédures définies dans la PC et la DPC associée.

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

L'AC décline toute responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, et quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication. L'AC décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le porteur/RC ou le MC (cf. également chapitre 4.4.1).

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

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

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

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 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

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs/RC, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit 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 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.

Document
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° 2004-801 du 6 août 2004
[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
[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 porteurs, doit répondre aux exigences de sécurité suivantes :

- Si les bi- clefs des porteurs 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- clef s des porteurs sont générées par ce module, assurer la confidentialité des clefs privées et l'intégrité des clefs privées et publiques des porteurs lorsqu'elles sont sous la responsabilité de l'AC et pendant leur transfert vers le dispositif de protection des éléments secrets du porteur 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).

12. Annexe 3 : Exigences de sécurité du dispositif de protection

12.1. Exigences sur les objectifs de sécurité

Le dispositif de protection des éléments secrets du porteur, utilisé par le porteur pour stocker et mettre en œuvre sa clef privée et, le cas échéant, générer sa bi-clef, doit répondre aux exigences de sécurité suivantes :

- Si la bi-clef du porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clef générée ;
- Détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction des clefs privées ;
- Garantir la confidentialité et l'intégrité des clefs privées ;
- Assurer la correspondance entre la clef privée et la clef publique ;
- Générer une fonction de sécurité qui ne peut être falsifiée sans la connaissance de la clef privée ;
- Assurer la fonction de sécurité pour le porteur légitime uniquement et protéger la clef privée contre toute utilisation par des tiers ;
- Permettre de garantir l'authenticité et l'intégrité de la clef publique lors de son export hors du dispositif.

12.2. Exigences sur la certification

Dans le cadre du badge agent : Le dispositif de protection utilisé par le porteur est conforme aux exigences énoncées ci-dessus (12.1), et a fait l'objet d'une certification CC EAL4+ ou équivalent.

En dehors du badge agent : Aucune certification n'est exigée pour le dispositif de protection utilisé par le porteur ou le RC mis à part être conforme aux exigences énoncées ci-dessus.

13. Annexe 4 : Exigences de sécurité du dispositif de protection

Le dispositif de protection des éléments secrets, utilisé par le service applicatif pour stocker et mettre en oeuvre sa clef privée et, le cas échéant, générer sa bi-clef, doit répondre aux exigences de sécurité suivantes :

- Si la bi-clef du service applicatif est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clef générée ;
- Assurer la correspondance entre la clef privée et la clef publique ;
- Générer une authentification qui ne peut être falsifiée sans la connaissance de la clef privée.

Par ailleurs, des mesures de sécurité organisationnelles, procédurales ou techniques doivent être mises en place afin de :

- Détecter les défauts lors des phases d'initialisation, et d'opération et disposer de techniques sûres de destruction de la clef privée en cas de re-génération de la clef privée ;
- Garantir la confidentialité et l'intégrité de la clef privée ;
- Permettre de garantir l'authenticité et l'intégrité de la clef publique lors de son export hors du dispositif.
- Assurer pour le serveur légitime uniquement, d'une part, la fonction d'authentification et, d'autre part, la fonction de déchiffrement de clefs symétriques de session, et protéger la clef privée contre toute utilisation par des tiers ;
- Permettre de garantir l'authenticité et l'intégrité de la clef symétrique de session, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données.