
PORTAIL BANCAIRE INTERNET

DOSSIER DE RACCORDEMENT
TECHNIQUE

V 7.0



SOMMAIRE

1. RAPPEL DU CONTEXTE	3
2. INTERFACE DE COMMUNICATION DU CONCENTRATEUR	5
2.1. PROCESSUS DE CONNEXION AU PORTAIL	5
2.2. SPÉCIFICATIONS FONCTIONNELLES	5
2.2.1. Connexion au serveur	5
2.2.2. Session TLS	6
2.2.3. Accès aux services	7
2.2.4. Fermeture de la session TLS	7
2.3. CONTRAINTES DE SÉCURITÉ	7
3. COMPOSANTS TECHNIQUES DE CONNEXION	8
3.1. COMPOSANTS MATÉRIELS DE CONNEXION	8
3.1.1. Cartes à puce	9
3.1.2. Lecteur de carte à puce	9
3.1.3. Terminal de l'abonné	9
3.2. COMPOSANTS LOGICIELS DE CONNEXION	10
3.2.1. Certificats logiciels des abonnés	10
3.2.2. Certificats publics des « Autorités de certification » du Portail	10
3.2.3. Support de HTTP 1.1, RFC 1945 et RFC 2616	11
3.2.4. Logiciels serveur côté Banque de France	11
3.2.5. Le Middleware	11
4. ANNEXES	12
4.1. SCHÉMA GÉNÉRAL DE LA PROCÉDURE D'ADHÉSION	12
4.2. PROCESSUS DE RACCORDEMENT EXTRANET	13
4.3. URL DES SITES DU PORTAIL BANQUE DE FRANCE	14

1. Rappel du contexte

L'accès aux applications proposées par la Banque de France sur son **Portail Bancaire Internet** (POBI) passe par la connexion de l'abonné au portail. Pour ce faire, l'établissement client doit préalablement :

- formuler une demande d'adhésion auprès de la Banque de France,
- entrer en possession des composants matériels et logiciels préconisés,
- connaître les normes qui lui permettront de se connecter au portail pour accéder aux services.

L'architecture de connexion au portail permet deux voies d'accès :

- via le réseau Internet,
- via un Réseau Privé Virtuel (MEXIC).

Dans le cas de l'utilisation du Réseau Privé Virtuel (**MEXIC**), ce document ne spécifie pas les aspects techniques de raccordement au réseau, l'établissement client devant contacter l'un des opérateurs prévus pour l'interconnexion au VPN : COMPLETEL, COLT, Orange Business Service ou SFR. (**Prérequis à une demande de connexion**).

L'architecture de connexion au portail Banque de France prévoit deux types d'accès :

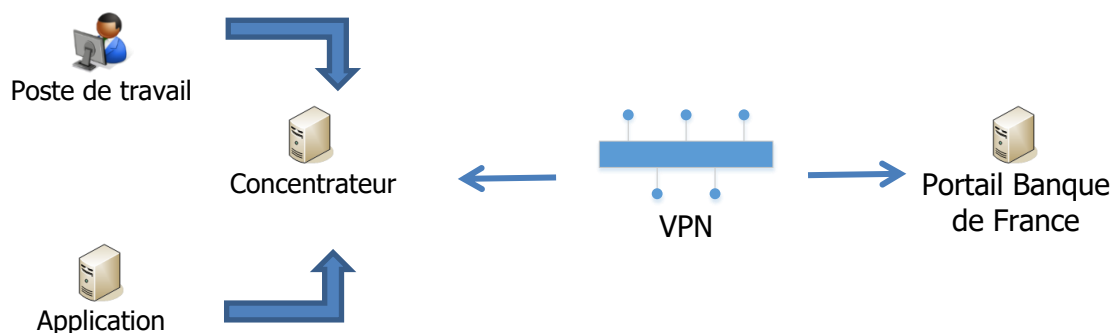
■ Accès standard :

Le terminal du client accède directement au portail Web. Il nécessite la présence d'un utilisateur.



■ Accès regroupé (concentrateur) :

Cet accès est caractérisé par la présence d'un concentrateur assurant la communication directe avec le portail, de manière automatique.



Le présent document a pour but de décrire les spécifications fonctionnelles de l'interface de communication du concentrateur devant servir de point d'entrée à la conception et au développement des automatismes d'accès au portail Banque de France.

Il fournit également des éléments d'informations sur les composants techniques participant au raccordement d'un abonné à l'infrastructure tout en mettant en évidence les normes applicables à ces derniers pour assurer la réussite de la connexion.

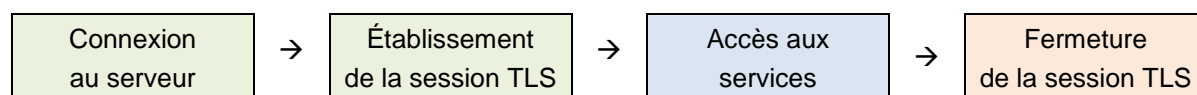
En revanche, ce document ne spécifie pas l'aspect fonctionnel lié aux applications accédées via le portail Banque de France, il se limite à préciser comment un concentrateur devra se comporter pour initialiser, maintenir et terminer correctement une session. La description fonctionnelle de l'interface avec les applications accédées est du domaine du contenu applicatif. En particulier, les formats proposés pour l'échange des flux avec le Système d'Information du Client (HTML ou XML) sont liés aux possibilités offertes par chaque application accédée via le portail, notamment dans le cas de l'utilisation des concentrateurs.

2. Interface de communication du concentrateur

Un concentrateur est capable selon un processus automatique d'initialiser une connexion **https** vers le portail, d'établir une session **TLS** avec le serveur WEB et d'initialiser des demandes d'accès aux services applicatifs, puis enfin de terminer la session **TLS**. Ce chapitre du document décrit le processus d'accès à l'infrastructure et les spécifications fonctionnelles relatives au concentrateur dans le cadre d'une connexion par ce système.

2.1. Processus de connexion au portail

Le processus d'accès au portail peut être subdivisé en quatre phases comme le montre le schéma ci-dessous :



- **La connexion au serveur** : Elle constitue la première étape du processus de connexion. Elle est initialisée par la commande **https://** à l'adresse du portail POBI. (Cf. annexe).
- **L'établissement de la session TLS** : La commande **https://** a pour conséquence l'initialisation d'une session **TLS** entre le concentrateur et l'un des serveurs WEB du portail. C'est lors de cette phase que le concentrateur et le serveur WEB s'authentifient mutuellement à l'aide des certificats émis par l'Autorité de Certification de la Banque de France.
- **L'accès aux services** : Une fois la session **TLS** établie, l'automate exécute les commandes d'accès aux services à l'intérieur de la session **TLS**.
- **La fermeture de la session TLS** : À la fin de l'opération d'accès aux services, le concentrateur doit terminer la session **TLS** afin de libérer les ressources utilisées sur le serveur WEB.

2.2. Spécifications fonctionnelles

2.2.1. Connexion au serveur

Le concentrateur doit être capable de générer une commande de connexion http sécurisée à l'adresse du portail POBI. L'exécution de cette commande provoque l'initialisation d'une session **TLS** entre le concentrateur et le serveur WEB. Le protocole sécurisé **TLS** étant requis au niveau du portail POBI, aucune communication http n'est possible.

2.2.2. Session TLS

TLS est un protocole de sécurisation des échanges numériques. Il est conçu pour permettre au client et au serveur de s'authentifier mutuellement, puis de négocier un algorithme de chiffrement en vue de l'établissement d'une connexion sécurisée au sein d'une session.

TLS (Transport Layer Security) assure donc la sécurisation du protocole TCP avec l'utilisation d'une connexion **https** sur le port standard **443**.

Une session **TLS** sécurise ainsi les échanges, tant au niveau de la confidentialité, que de l'intégrité des données, et permet une authentification à la fois du serveur, mais aussi du client.

Dans le contexte du portail POBI, **TLS** permet :

- la négociation des algorithmes de chiffrement (symétriques et asymétriques)
- la négociation des longueurs de clés symétriques
- la négociation des algorithmes de signature (HMAC)
- l'authentification du serveur par le client
- l'authentification du client par le serveur

Le client et le serveur choisissent les algorithmes les plus puissants qui sont en commun. Si aucun algorithme n'est trouvé, la communication est directement coupée (protocole Alert). La négociation des clés se fait de la même manière.

Le portail POBI n'accepte que des connexions TLS 1.2 avec les suites cryptographiques suivantes :

Code TLS	Suite cryptographique
0x009D	TLS_RSA_WITH_AES_256_GCM_SHA384
0x009C	TLS_RSA_WITH_AES_128_GCM_SHA256
0x003D	TLS_RSA_WITH_AES_256_CBC_SHA256
0x003C	TLS_RSA_WITH_AES_128_CBC_SHA256

Les échanges de type Diffie-Hellman ne sont pas acceptés. Il conviendra également de vérifier que les équipements accédant au portail POBI ne sont pas vulnérables à la faille Robot Attack (<https://robotattack.org/>). Des informations complémentaires sont disponibles sur le sujet en consultant cette URL (<https://www.cert.ssi.gouv.fr/alerte/CERTFR-2017-ALE-020/>).

2.2.3. Accès aux services

Une fois la session **TLS** établie, le concentrateur doit générer les requêtes adéquates auprès du serveur WEB afin de récupérer les données recherchées. Le concentrateur devra pour cela avoir un jeu de commandes prédéfinies qui va correspondre aux requêtes applicatives usuelles du client. Les messages échangés entre le concentrateur et le serveur WEB doivent être au format XML ou HTML en fonction des possibilités permises par chaque application.

Cet échange de messages doit bénéficier de la sécurité offerte par la session **TLS**.

2.2.4. Fermeture de la session TLS

Une fois les transactions terminées, le concentrateur doit fermer la session **TLS** en utilisant les fonctions prévues à cet effet, et ce, en fonction des implémentations.

2.3. Contraintes de sécurité

La mise en place de l'accès automatisé au portail Banque de France doit respecter les contraintes de sécurité suivantes :

- **L'accès physique au concentrateur doit être sécurisé :** *Le serveur hébergeant le dispositif de concentration devra être localisé dans une pièce à accès restreint et strictement contrôlé.*
- **La clé privée du concentrateur doit être protégée contre la duplication :** *Le concentrateur étant un équipement hors du contrôle direct de la Banque de France, il sera nécessaire de stocker la clé privée de préférence sur un dispositif matériel sécurisé. Tout autre support introduit une vulnérabilité du fait de la facilité avec laquelle le conteneur peut être dupliqué puis exploité.*
- **La configuration logicielle du concentrateur ne doit être faite que par les personnes habilitées.** *Elle doit être soumise à authentification et contrôle d'accès. Le concentrateur étant un point d'entrée mutualisé sur un site déporté et hors du contrôle de la Banque de France, il sera particulièrement important de veiller à ce que seules les personnes habilitées aient accès à sa configuration.*
- **Le concentrateur doit mettre en œuvre un dispositif de contrôle d'accès permettant la restriction de l'utilisation des services disponibles sur le portail aux seules personnes habilitées et identifiables.** *Il est recommandé de tracer et d'horodater les accès réussis ou en échec sur les ressources du concentrateur.*

3. Composants techniques de connexion

Le portail Banque de France est accessible par deux types de terminaux :

- Soit des dispositifs de concentration développés par les clients et hébergés sur des serveurs.
- Soit des postes de travail, de type PC (sous Windows 10 de préférence).

Les certificats numériques distribués par la Banque de France peuvent être stockés :

- Soit sur carte à puce pour les accès personnels depuis des postes de travail (support fortement recommandé)
- Soit sous forme logicielle dans le cas des concentrateurs.

Le certificat dispose d'une clé de chiffrement de 2048 bits et a une durée de validité de 3 ans à partir de sa date de création. Ce certificat, qu'il soit stocké sous forme logicielle ou sur une carte à puce, peut donner l'accès à tout ou partie des applications disponibles sur le portail POBI.

Lors de la procédure d'adhésion et/ou de la commande de certificats, le client liste les applications pour lesquelles un droit d'accès est demandé. Il est possible de demander une extension ou une restriction des droits d'accès associés à un certificat déjà en cours d'utilisation. La politique de sécurité des applications POBI suivantes FCC, FICP, FNCI, FIBEN, ELIG et POOL3G est identique. De ce fait, un établissement peut disposer d'un certificat unique pour l'accès à toutes ces applications.

Pour des raisons de sécurité inhérentes aux composants logiciels, l'usage des cartes à puce est fortement recommandé.

L'utilisation des certificats logiciels est interdite pour les accès Internet.

	Internet	Extranet
Certificats logiciels	Interdit	Autorisé
Carte à puce	Obligatoire	Recommandé

3.1. Composants matériels de connexion

Les composants matériels nécessaires à la connexion des abonnés sur le portail sont les suivants :

- La carte à puce, qui sert de lieu de stockage et de moyens de transport des éléments de sécurité que sont les clés privées RSA et le certificat X509 v3.

- Le lecteur de carte à puce dont le terminal se sert pour accéder au contenu de la carte à puce.
- Le terminal, à partir duquel les opérations d'accès aux services sont exécutées. Le terminal joue aussi le rôle de stockage des éléments de sécurité (clés privées de l'abonné et son certificat) en cas d'utilisation de certificats logiciels.

3.1.1. Cartes à puce

- **Description** : Il s'agit d'une carte contenant un microprocesseur avec mémoire, pour stocker les clés privées et les certificats numériques. Elle est transmise par la Banque de France dans le cadre de la procédure d'adhésion. Son usage requiert l'installation préalable d'un middleware. Depuis mai 2019, les cartes à puce délivrées sont du type GEMALTO. Elles nécessitent l'installation sur les terminaux du middleware SafeNet.
- **Normes** : Elle supporte les standards ISO/IEC 7816, Parts 3-4-8, FCC, CE et Microsoft PC/SC.

3.1.2. Lecteur de carte à puce

Pour communiquer avec la carte à puce, le terminal a besoin d'un lecteur de carte à puce. Dans le cadre de la solution de raccordement des abonnés au portail, tout lecteur répondant au standard PC/SC peut être utilisé.

La Banque de France préconise l'usage du lecteur **CardMan 3121 USB** de la marque **OMNIKEY**.

Ce lecteur est disponible auprès de la Cellule R4F (Cf. Bon de commande en annexe).

Les drivers 32 bits et 64 bits pour ce type de lecteur sont disponibles sur le site du constructeur, à l'adresse suivante : <https://www.hidglobal.fr/drivers/32909>

3.1.3. Terminal de l'abonné

Pour accéder aux services, l'abonné a besoin d'un équipement lui permettant d'envoyer et de recevoir des commandes aux applications. Ces équipements peuvent être classés en deux catégories : les terminaux interactifs (PC) et les concentrateurs (automates) :

- **Terminaux interactifs**

Ils nécessitent la présence d'un utilisateur pour faire appel aux services du portail. Le client a le choix de mettre en place le type d'ordinateur de son choix de préférence équipé d'un système d'exploitation sous Windows 10.

Pour les cartes, le lecteur nécessite une machine équipée d'un port USB.

Les navigateurs qualifiés par la Banque de France pour les accès aux applications du portail POBI sont au 1^{er} juin 2020 :

- **Internet Explorer** - version 11.1610.17134.0
- **Chrome** - version 81.0.4044.113
- **Firefox** - version 68.9.0esr

- **Concentrateurs**

Ce sont des applications embarquées sur un serveur capable de négocier une connexion TLS avec le portail POBI.

3.2. Composants logiciels de connexion

Une nouvelle version de l'Autorité de Certification Banque de France est entrée en production en septembre 2020. Tous les certificats émis avant cette date restent valides jusqu'à leur expiration, soit au plus tard en octobre 2022. On nommera par convention l'Autorité de Certification arrivant à expiration en octobre 2022 **IGCBDFv2**, et la nouvelle **IGCBDFv3**.

3.2.1. Certificats logiciels des abonnés

La délivrance d'un certificat nécessite la création d'un compte sur le portail FBI de la Banque de France.

Ce compte permet de se connecter à l'interface de gestion des certificats Banque de France.

Le certificat logiciel et sa clé privée associée pourront y être retiré (cf. annexe 4.2)



Ce type de support offre une souplesse de déploiement. Nous soulignons ici qu'un risque de sécurité est inhérent à ce type de support pour lequel la clé privée n'est pas protégée par un dispositif matériel. Ainsi, un risque existe d'usurpation ou de duplication de tout élément logiciel. De ce fait, l'utilisation de certificats Logiciels est uniquement autorisée sur des équipements échangeant avec le Portail POBI au travers de liaisons VPN, la Banque de France pourra suspendre les autorisations d'accès en cas d'usage incorrect de ce type de certificat.

3.2.2. Certificats publics des « Autorités de certification » du Portail

La partie publique des certificats de l'Autorité de Certification Banque de France est indispensable à l'utilisation des certificats Utilisateurs (qu'ils soient sous formes logiciel ou sur carte à puce). Ils sont à retirer aux URLs suivantes :

IGCBDFv2 (pour la gestion des certificats délivrés avant le mois d'octobre 2020)

<https://ae.certificats.banque-france.fr/igc-bdf-v2/cert/ac/IGC-BDF-v2.p7b>

IGCBDFv3

<http://www.banque-france.fr/igcbdf/v3/IGC-BDF-v3-Chaine.p7b>

Ils sont à intégrer par l'utilisateur dans les magasins de certificats « Autorité de certification racine de confiance » et « Autorité de certification ».

L'autorité de certification « Racine » et les autorités de certification intermédiaires de l'IGCBDFv3 disposent d'une clé de chiffrement de 4 096 bits et d'une durée de vie de 20 ans.

3.2.3. Support de HTTP 1.1, RFC 1945 et RFC 2616

Par défaut, l'infrastructure d'accès POBI supporte les deux versions des RFC (1945 et 2616). Néanmoins, il est préconisé de s'appuyer sur le protocole HTTP 1.1, qui implémente une gestion optimisée de la persistance des connexions.

3.2.4. Logiciels serveur côté Banque de France

Les serveurs du portail sont accessibles uniquement en https. Par conséquent, le support de **TLS 1.2** est activé sur les serveurs WEB de la plate-forme. Le terminal du client doit donc être capable d'établir une connexion **TLS** avec le serveur WEB du portail en vue de l'authentification des abonnés.

3.2.5. Le Middleware

Il permet en outre de changer le code PIN de la carte (le code initial est transmis par la Banque de France dans le cadre de procédure d'adhésion).

SafeNet est le logiciel qui permet l'utilisation de la carte à puce GEMALTO. Il est disponible sur le site suivant :

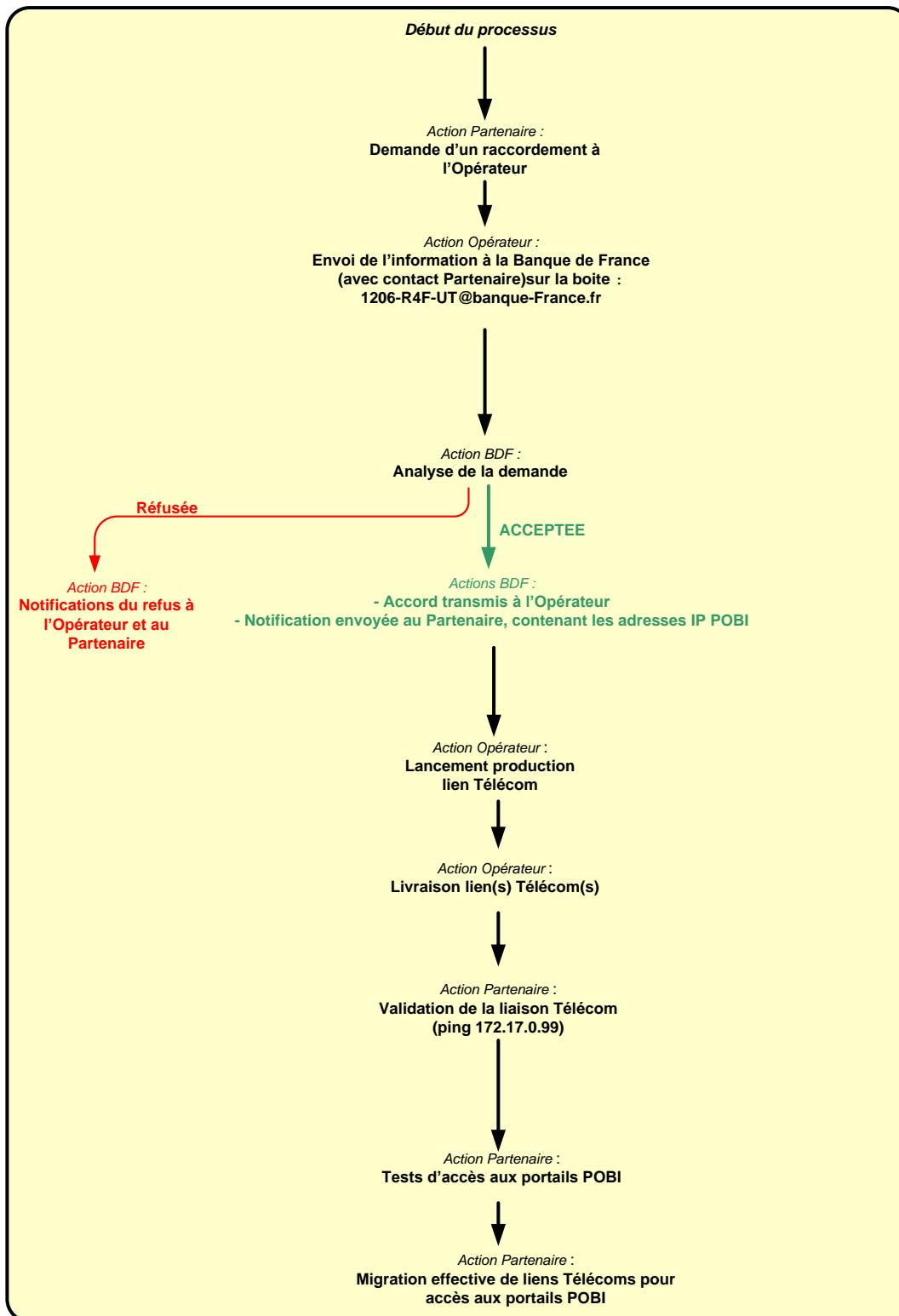
<https://www.banque-france.fr/certificats>

Onglet : *Prérequis techniques*

Paragraphe : *Installation des drivers pour le middleware*

4. Annexes

4.1. Schéma général de la procédure d'adhésion



4.2. Processus de raccordement Extranet

Le raccordement d'un abonné se réalise en plusieurs étapes impliquant la participation de la Banque de France et le Correspondant Sécurité de l'établissement client :

Étape 1

Le Correspondant Sécurité transmet une demande d'adhésion comprenant le contrat d'adhésion au portail et les formulaires de demande de certificat.

Destinataire :

**Banque de France
Cellule R4F
26-1206
75049 PARIS CEDEX 01**

Étape 2

La Banque de France analyse la demande, puis le cas échéant, contresigne le contrat d'adhésion.

Pour chacun des formulaires de demande de certificat, la cellule R4F crée, si elle n'existe pas, une identité permettant à chacun des demandeurs (référéncé par son adresse de courrier électronique) de se connecter à l'interface de gestion des certificats Banque de France (cf. étape 3). Suite à cette création d'identité, le demandeur est notifié de la création de son compte FBI par la réception d'un courriel lui indiquant son login et son mot de passe de connexion.

La cellule R4F procède à la création des certificats demandés, ainsi qu'au positionnement des droits applicatifs POBI associés à ces certificats.

La cellule R4F transmet par voie électronique au Correspondant Sécurité du Client l'adresse URL permettant de télécharger les certificats publics des « autorités de certification » au portail Banque de France.

IGCBDFv3

<http://www.banque-france.fr/igcbdf/v3/IGC-BDF-v3-Chaine.p7b>

ATTENTION

Le poste client ou le serveur doit également pouvoir reconnaître des certificats émis avant octobre 2020, il conviendra donc de s'assurer de l'installation des certificats publics de l'autorité de certification suivante :

IGCBDFv2 (pour la gestion des certificats délivrés avant le mois d'octobre 2020)

<https://ae.certificats.banque-france.fr/igc-bdf-v2/cert/ac/IGC-BDF-v2.p7b>

Suite à la création d'un certificat logiciel, un courriel sera adressé directement au demandeur lui indiquant la mise à disposition du certificat (cf. étape 3).

Suite à la création d'un certificat sur carte à puce, un courriel sera adressé directement au demandeur lui indiquant l'envoi postal de sa carte à puce accompagnée du lien permettant de télécharger le middleware SafeNet. Suite à sa réception, le demandeur devra se connecter à l'interface de gestion des certificats Banque de France (cf. étape 3).

Étape 3

Le demandeur se connectera à l'aide de son compte FBI, à l'interface de gestion des certificats Banque de France disponible à l'URL suivante : <https://igcv3.certificats.banque-france.fr>

Le demandeur pourra y récupérer le code associé à son certificat, ainsi que son certificat si celui-ci est logiciel.

4.3. URL des sites du portail Banque de France

Environnements	URL
Environnement de production	https://portail.banque-france.org
Environnement de test	https://portail-test.banque-france.org

L'environnement de test est mis à disposition des banquiers pour le développement et le test des dispositifs de concentration. Son accès requiert des certificats spécifiques.

Les adresses IP d'accès aux portails POBI (production et test) sont communiquées par la Banque de France lors des abonnements MEXIC.

