PORTAIL BANCAIRE INTERNET

DOSSIER DE RACCORDEMENT TECHNIQUE

V 10.0

BANQUE DE FRANCE
EUROSYSTÈME

SOMMAIRE

1. Préambule

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 participants 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. Accès au portail POBI

L'accès aux applications proposées par la Banque de France sur son **PO**rtail **B**ancaire **I**nternet (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.

La Banque de France propose deux types d'accès au portail soumis à des règles de sécurité qui impliquent l'usage d'éléments de sécurité :

2.1. Accès standard pour une personne physique :

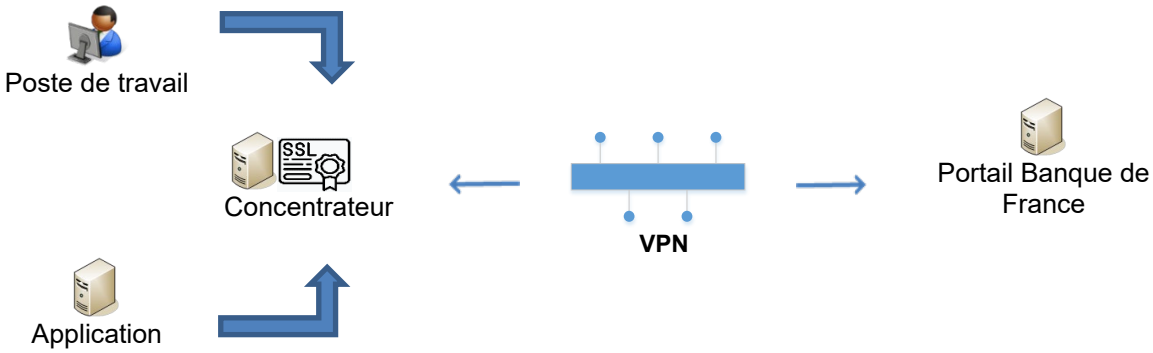
L'authentification se fait obligatoirement grâce à un certificat numérique stocké sur une carte à puce délivrée par la Banque de France. Le terminal du client accède directement au portail Web. Il nécessite la présence d'un utilisateur (saisie d'un code PIN lors de l'authentification). Ce certificat est individuel et nominatif. Il ne peut être partagé avec d'autres utilisateurs.

2.2. Accès regroupé pour un concentrateur :

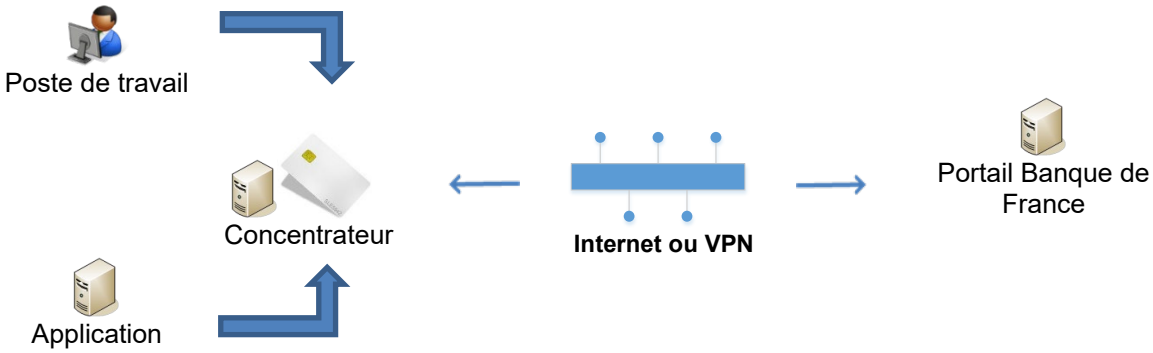
Cet accès est caractérisé par la présence d'un concentrateur assurant la communication directe avec le portail, de manière automatique.

L'authentification s'effectue :

- **Soit par un certificat numérique stocké sur le disque dur du serveur (appelé certificat logiciel)**, dont la connexion doit **obligatoirement** s'effectuer par VPN. Ce certificat est délivré par la Banque de France.



- **Soit par un certificat numérique stocké sur une carte à puce ou un token USB**, dont la connexion s'effectue par Internet ou VPN. Ce certificat est délivré par la Banque de France.



2.2.1. Spécificités liées à l'utilisation d'un certificat logiciel

L'utilisation d'un certificat logiciel nécessite obligatoirement une liaison VPN pour accéder au portail POBI de la Banque de France.

La solution de liaison VPN acceptée par la Banque de France (au 1er septembre 2023) est le VPN MEXIC.

Trois opérateurs proposent actuellement ce service:

- COLT,
- Orange Business Service,
- SFR.

1. **Votre établissement dispose d'un hébergement physique**

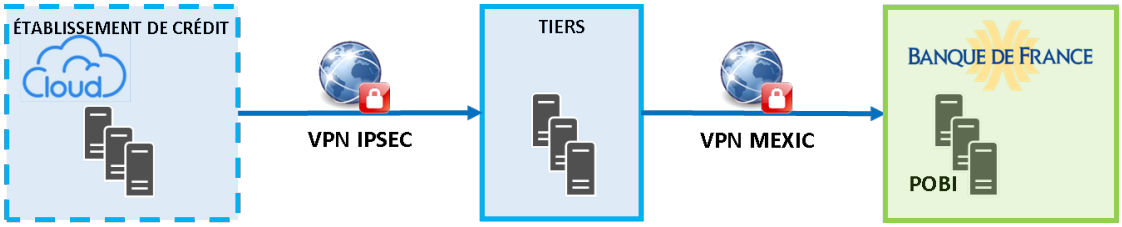
Il convient de contacter l'un des opérateurs mentionnés ci-dessus afin de commander l'interconnexion de votre SI au VPN MEXIC.

Cette démarche est un prérequis à toute demande d'adhésion à POBI.

Il est à noter que la liaison VPN MEXIC nécessite la mise en place de routeurs opérateurs physiques au sein de votre Datacenter.

Ce document ne spécifie pas les aspects techniques de raccordement au réseau VPN MEXIC, que vous traiterez avec l'opérateur choisi.

2. **Votre établissement ne dispose pas d'un hébergement physique (cas des SI hébergés sur le cloud par exemple)**



Dans ce contexte, il convient d'utiliser les infrastructures physiques d'un tiers. La liaison entre le tiers et la Banque de France est assurée par une liaison VPN MEXIC.

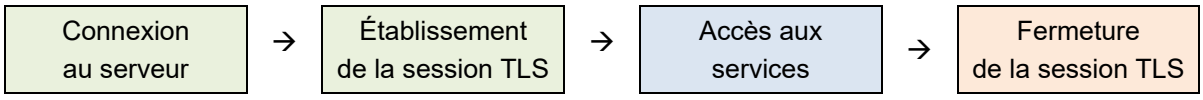
Il convient également de mettre en place une liaison IPSEC entre votre SI et l'infrastructure du tiers, afin de garantir la confidentialité des données.

3. 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.

3.1. 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.

3.2. Spécifications fonctionnelles

3.2.1. 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.

3.2.2. 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/).

3.2.3. 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**.

3.2.4. 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.

3.3. 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. Il convient donc de privilégier un stockage des clés sur des composants matériels tels que des HSM ou puces TPM qui représente une solution plus robuste qu'un stockage sur système de fichier.*
- **La configuration logicielle du concentrateur ne doit être effectuée que par les personnes habilitées après 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. Il est recommandé également de tracer et d'horodater les accès réussis ou en échec sur les ressources du concentrateur.*

4. Certificats

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 de préférence).

L'accès au portail depuis ces terminaux nécessite l'acquisition de certificats numériques délivrés par la Banque de France, ils peuvent être stockés :

- Soit sur carte à puce ou token USB pour les accès personnels depuis des postes de travail ou pour certains dispositifs de concentration. L'utilisation d'une carte à puce peut nécessiter l'acquisition d'un lecteur de cartes. Ce dernier peut être commandé en même temps que le certificat.
- Soit sous forme logicielle dans le cas des concentrateurs.

Lors 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, POOL3G et DDAC est identique. De ce fait, un établissement peut disposer d'un certificat unique pour l'accès à toutes ces applications.

L'ensemble des informations concernant l'utilisation ou la facturation des certificats émis par la banque de France est disponible à l'adresse suivante :

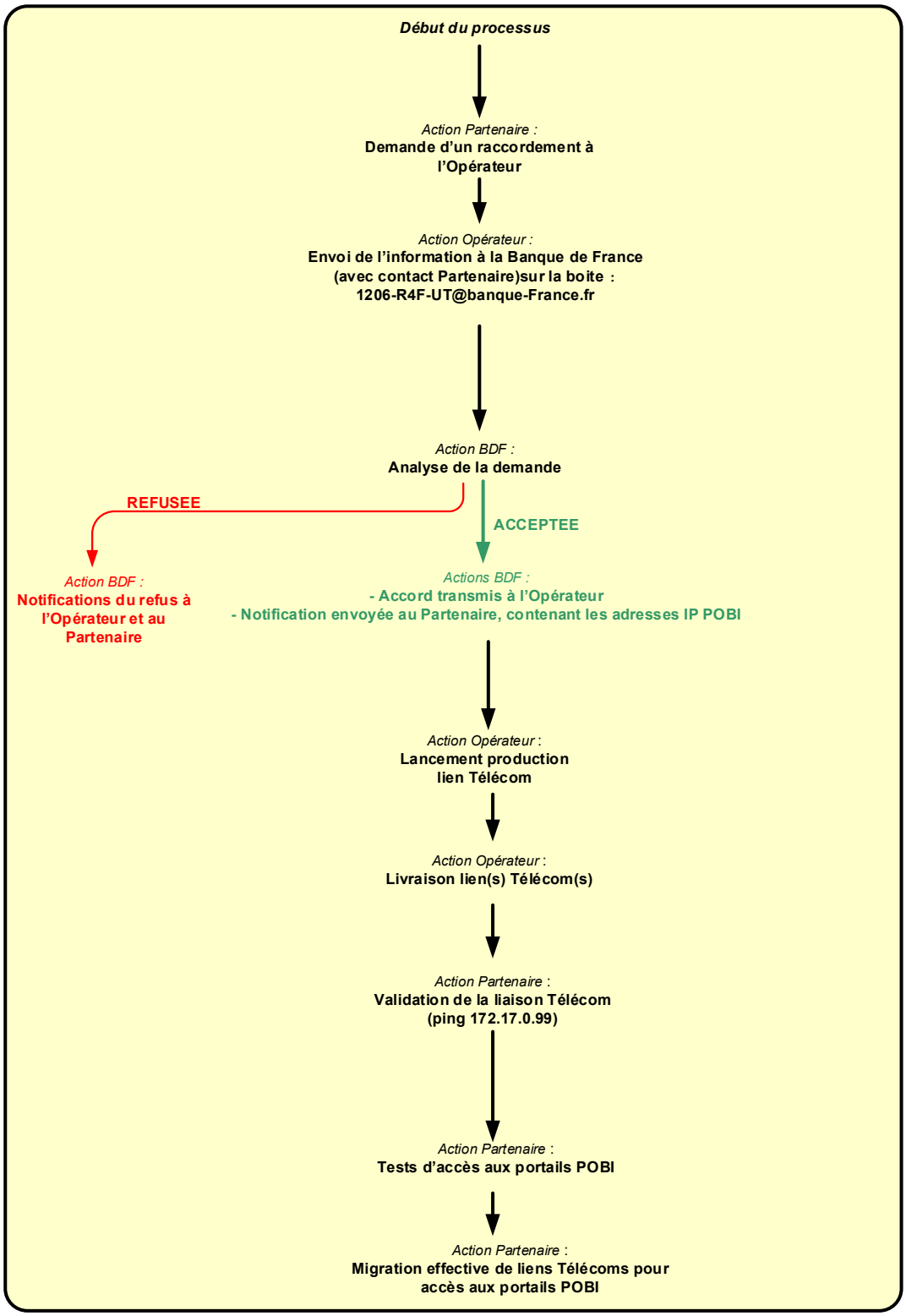
https://www.banque-france.fr/certificats

L'utilisation des certificats logiciels est interdite pour les accès Internet et est uniquement autorisée sur des équipements échangeant avec le Portail POBI au travers d'une liaison VPN MEXIC. La Banque de France pourra suspendre les autorisations d'accès en cas d'usage incorrect de ce type de certificat.

	Internet	**VPN MEXIC**
Certificats logiciels	**Interdit**	**Autorisé**
Carte à puce	**Autorisé**	**Autorisé**

5. Annexes

5.1. Schéma général de la procédure d'adhésion



5.2. Processus de raccordement

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

L'adhérent transmet le contrat d'adhésion à POBI, le formulaire de désignation des correspondants sécurité (annexe 3) et les formulaires de demande de certificat, à l'adresse ci-dessous :

Par courrier (si signature manuscrite)	Par mail (si signature électronique)
Banque de France Cellule R4F du RSI S1A-1206 31, rue croix des petits-champs 75049 Paris Cedex 01	1206-R4F-UT@banque-france.fr

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 procède à la création des certificats demandés, ainsi qu'au positionnement des droits applicatifs POBI associés à ces certificats. Les modalités de retrait des certificats sont ensuite communiquées au demandeur.

Étape 3

Le demandeur accède 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.

5.3. 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.

Pour une liaison VPN MEXIC, les adresses IP d'accès aux portails POBI (production et test) sont communiquées par l'opérateur avec lequel l'établissement client a contracté.