PORTAIL BANCAIRE INTERNET

DOSSIER DE RACCORDEMENT TECHNIQUE

V 4.0

BANQUE DE FRANCE
EUROSYSTÈME

SOMMAIRE

1. Rappel du contexte

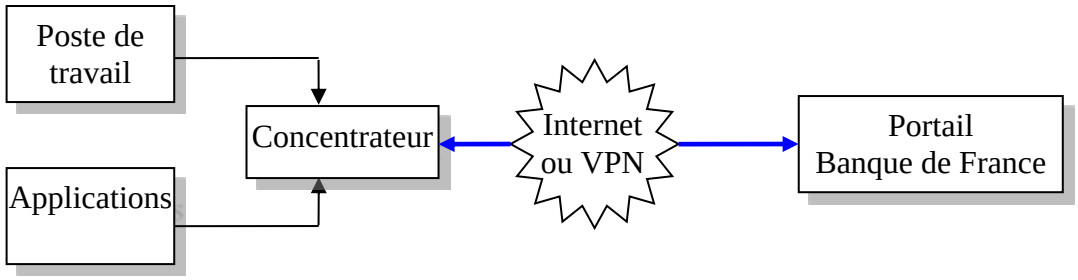
L'accès aux applications proposées par la Banque de France sur son Portail Bancaire Internet passe par la connexion de l'abonné au portail. Pour ce faire, l'établissement client doit préalablement formuler une demande d'adhésion auprès de la Banque de France, entrer en possession des composants matériels et logiciels préconisés et connaître les normes qui lui permettront de se connecter au portail pour accéder aux services.

L'architecture de connexion au portail Banque de France permet deux voies d'accès : via le réseau Internet ou 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 (voir schéma ci-dessous) : l'accès qualifié de standard, pour lequel le terminal du client accède directement au portail Web. Il nécessite la présence d'un utilisateur. L'autre type d'accès est qualifié d'accès regroupé. Il est caractérisé par la présence d'un concentrateur assurant la communication directe avec le portail, de manière automatique.

- Accès standard

- Accès regroupé (concentrateur)



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.

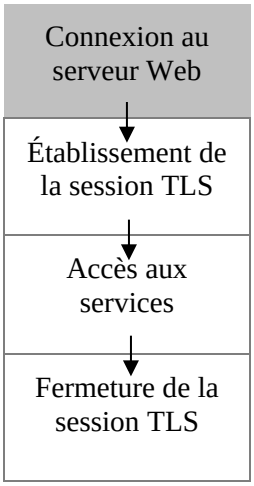
Il fournit également des éléments d'informations sur les composants techniques participant au raccordement d'un abonné à l'infrastructure tout en mettant en évidence les normes applicables à ces derniers pour assurer la réussite de la connexion.
En revanche, ce document ne spécifie pas l'aspect fonctionnel 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

Vu du portail Banque de France, 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, enfin de terminer une 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 :



a. La connexion au serveur

Elle constitue la première étape du processus de connexion. Elle est initialisée par la commande https:// à l'adresse des serveurs Web frontaux du portail.

(Cf. annexe)

b. L'établissement d'une session TLS

La commande https:// a pour conséquence l'initialisation d'une session TLS entre le concentrateur et les serveurs du portail Web. 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 du portail.

c. 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.

d. 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 Web : https:// URL_du_portail L'exécution de cette commande provoque l'initialisation d'une session TLS 1.0, 1.1 ou 1.2 entre le concentrateur et le serveur Web du Portail. Le protocole sécurisé TLS étant requis au niveau du portail, aucune communication http n'est possible.

2.2.2. Session SSL/TLS

SSL est un protocole à dialogue conçu pour réaliser l'authentification et la négociation de paramètres de chiffrement d'une session. Il apporte la sécurité par le chiffrement en établissant une connexion sécurisée entre les deux parties. Il est interopérable car les implémentations différentes sont conformes aux spécifications du standard. Il est extensible en autorisant l'implémentation de nouveaux algorithmes de chiffrement. Dans le contexte du portail Banque de France, le client et le serveur sont toujours authentifiés sur la base de leur certificat contenant la clé publique qui leur a été attribuée. Les données sont protégées car chiffrées et l'algorithme de chiffrement ainsi que la clé symétrique utilisée sont négociés à l'ouverture de la session. L'intégrité des données échangées est garantie par un MAC à base de clé et une fonction sécurisée de hachage. Une session SSL est un ensemble d'états et de paramètres négociés par le protocole à l'ouverture, notamment le « master secret » qui est une chaîne de 384 bits de long connue uniquement par le client et le serveur.

Étape 1
Lors de cette étape, le concentrateur doit établir une liaison IP avec le serveur Web du portail. Le concentrateur doit ensuite envoyer au cluster Web, un message[1] incluant le numéro de version de sa session SSL, les données de chiffrement et un nombre aléatoire.

Étape 2
Le serveur Web répond au message reçu du concentrateur en envoyant son certificat, le numéro de version de la session SSL, les données de chiffrement et un nombre aléatoire.

Étape 3
Le concentrateur doit authentifier le serveur Web en lui envoyant un message crypté avec sa clé publique (celle du serveur Web). Il doit aussi envoyer son certificat (en tant que concentrateur) pour se faire authentifier. Le serveur Web doit décrypter le message envoyé par le concentrateur et calculer les clés de session et de hachage ainsi que le vecteur d'initialisation, prouvant ainsi qu'il possède bien la clé privée correspondant à la clé publique du serveur Web. En retour, le serveur Web doit authentifier le concentrateur en lui renvoyant un message crypté avec la clé publique de ce dernier. Il doit calculer également la clé de session, de hachage et le vecteur d'initialisation.

Étape 4
Le concentrateur envoie un message crypté avec la clé de session au serveur Web. Ce dernier répond avec un message crypté avec la clé de session. La session SSL est ainsi ouverte.

[1] Le format des messages doit être conforme aux spécifications de SSL v3

2.2.3. Accès aux services

Une fois la session SSL établie, le concentrateur doit générer les requêtes adéquates auprès du portail 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 SSL. Pour envoyer des messages au serveur Web dans la session SSL, le concentrateur doit être capable d'utiliser les interfaces de programmation du fournisseur SSPI prévues à cet effet (dans les environnement Microsoft) ou toute autre fonction permettant d'envoyer des messages dans une session SSL dans le cas d'autres environnements (Unix, …).

2.2.4. Fermeture de la session SSL

Le concentrateur doit fermer la session SSL une fois les transactions terminées. Pour ce faire, il doit être capable d'utiliser les fonctions prévues à cet effet 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 plusieurs types de terminaux, selon deux modes de support des éléments de sécurité.

Vis-à-vis du portail, les terminaux peuvent être :

- des dispositifs de concentration développés par les clients, hébergés sur des serveurs (Windows Server 2008 R2 minimum souhaitable)
    - des postes de travail, de type PC sous Windows (De préférence Windows 7 SP1).

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

- soit sur carte à puce (support fortement recommandé)
- soit sous forme logicielle.

Le certificat dispose d'une clé de chiffrement de 4096 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 selon 2 critères :

- à la demande du client : lors de la procédure d'adhésion, le client commande des certificats et liste les applications pour lesquelles le droit d'accès est à autoriser. Il est possible de demander une extension, ou une restriction des droits d'accès associés à un certificat déjà en cours d'utilisation.
- selon la politique de sécurité des applications disponibles : une politique de sécurité pour l'accès aux applications est définie en fonction du type d'utilisateur, du type de données accédées, du type d'actions offertes par les applications. Les fichiers FIBEN, FCC, FICP, POOL3G et FNCI disposent de la même politique d'accès. Dès lors, un établissement peut disposer d'un certificat 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.

Réseau d'accès **Support des certificats**	**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** : La carte à puce utilisée dans le cadre de l'authentification sur le portail est la StarCOS 3.2 de Giesecke and Devrient. C'est 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 (SafeSign V3.0.87) sur les terminaux.
- **Normes** : Elle supporte les standards ISO/IEC 7816, Parts 3-4-8, FCC et 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.com/drivers?field_brand_tid=24&product_id=All&os=All

Windows7 32 bits : http://www.hidglobal.com/drivers/19355
Windows7 64 bits : http://www.hidglobal.com/drivers/21517

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 : 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, équipé d'un système d'exploitation sous Windows (Windows 7 SP1 de préférence).
Pour les cartes StarCOS 3.2 de Giesecke and Devrient, le lecteur nécessite une machine dotée d'un processeur de 133 Mhz avec 32 MB RAM, d'un port USB.
Les navigateurs utilisés pour la connexion sont Internet Explorer en version 9 et 11 ainsi que Firefox en version 42.0.

- **Concentrateurs**

Ce sont des applications embarquées sur un serveur capables de négocier une connexion SSL avec le portail Banque de France.

3.2. Composants logiciels de connexion

3.2.1. Certificats logiciels des abonnés

Les certificats dits logiciels et les clés privées correspondantes seront retirables par l'utilisateur à cette URL :
https://kregistration-user.certificat2.com/ui-user/forwardPickup.do

Ils s'installeront dans le magasin de certificats « Personnel » de l'utilisateur. Le mot de passe de protection de ce certificat sera choisi par le Correspondant Sécurité lors de la demande de certificat. Un mail lui confirmera la disponibilité du certificat demandé sur le site de retrait des certificats. Ils sont conformes à la norme X509 v3.

☞ *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 de ces certificats est indispensable à l'utilisation des certificats Utilisateurs (qu'ils soient sous formes logiciel ou sur carte à puce). Ils sont disponibles à l'URL suivante :

- https://ae.certificats.banque-france.fr/igc-bdf-v2/cert/ac/IGC-BDF-v2.p7b (IGCBDFv2)

Elles 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 » dispose d'une clé de chiffrement de 4 096 bits et d'une durée de vie de 20 ans. L'autorité de certification intermédiaire dispose d'une clé de chiffrement de 4 096 bits et d'une durée de vie de 10 ans.

3.2.3. Support de http 1.0 et 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 1.0, TLS 1.1 et TLS 1.2 est activé sur le serveur 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 SafeSign 3.0.87

C'est le logiciel qui permet l'utilisation de la carte à puce, Il est disponible sur le site suivant :

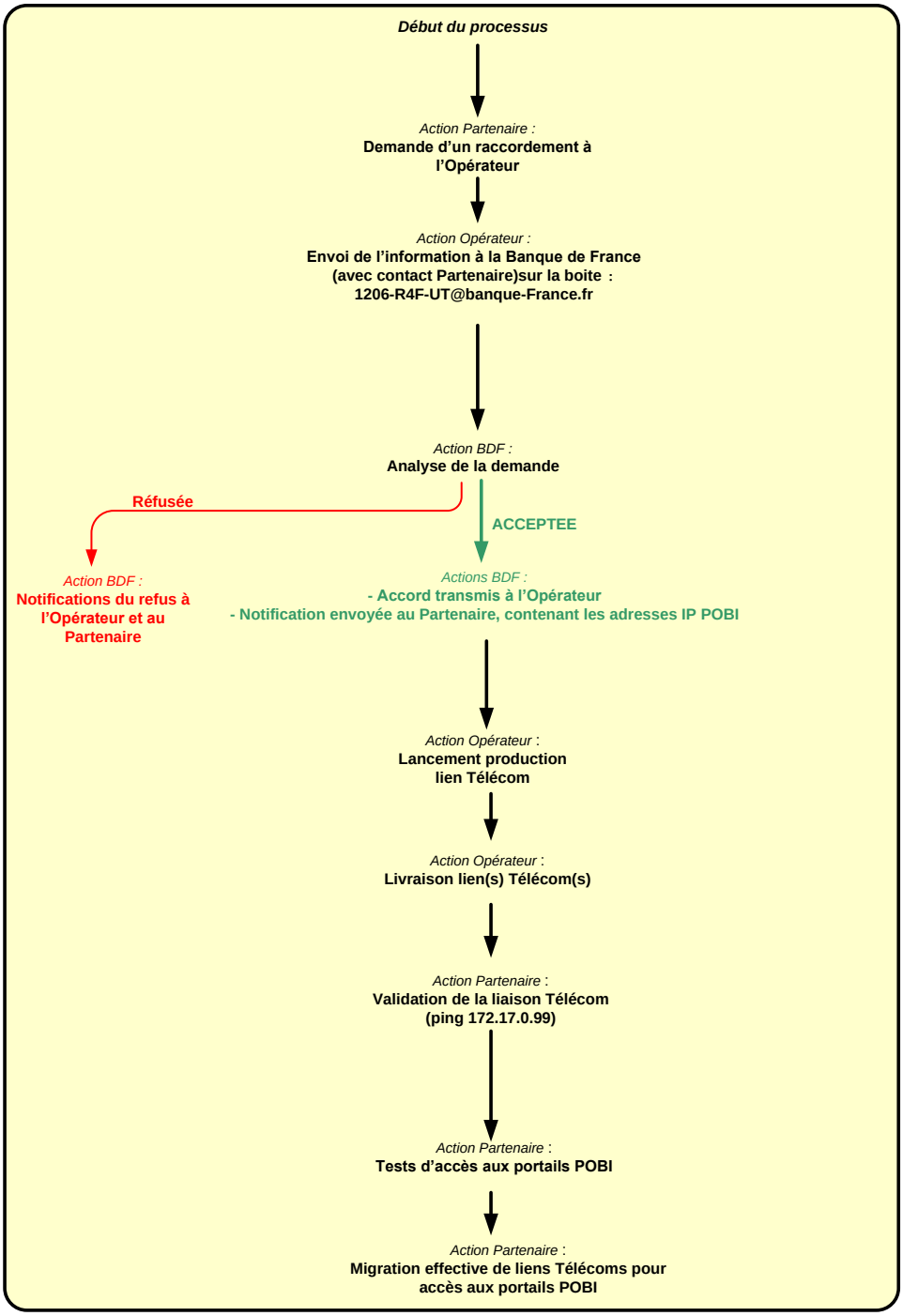
http://www.banque-france.fr/igcbdf/pilotes/SafeSign_Identity_Client-Standard-3.0.87-general-x86-win-admin-std-vc8.zip (version 32 bits).

http://www.banque-france.fr/igcbdf/pilotes/SafeSign_Identity_Client-Standard-3.0.87-general-x64-win-admin-std-vc8.zip (version 64 bits).

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)

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 des établissements clients :

Actions	Acteurs
1. Le Correspondant Sécurité transmet une demande d'adhésion comprenant le contrat d'adhésion au portail et les formulaires de demande d'éléments de sécurité. Destinataire : **Banque de France** **Cellule R4F, 26-1206, 75049 PARIS CEDEX01**	Correspondant Sécurité Client
2. La Banque de France analyse la demande, le cas échéant, contresigne le contrat d'adhésion, et transmet les éléments de sécurité au Correspondant Sécurité du Client. L'envoi comprend : - L'adresse URL permettant de télécharger les certificats publics des « autorités de certification » au portail Banque de France. https://ae.certificats.banque-france.fr/igc-bdf-v2/cert/ac/IGC-BDF-v2.p7b -Pour les certificats logiciels : aucun élément n'est envoyé. Un email automatique avertira le client de la mise à disposition du certificat logiciel sur le site de retrait des certificats logiciels POBI. https://kregistration-user.certificat2.com/ui-user/ChangeLocale.do?language=fr -Pour les cartes à puce : une carte accompagnée du lien permettant de télécharger le middleware SafeSign 3.0.87	BDF
3. Les codes secrets associés aux éléments de sécurité sont transmis au Correspondant Sécurité du Client	BDF
4. A la réception des Accusés de Réception, la Banque de France procède à l'activation de l'accès	BDF

5. Annexes

5.1. 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.