

Sterling B2B Integrator



# Concepts du serveur bancaire EBICS

*Version 5.2.5*



Sterling B2B Integrator



# Concepts du serveur bancaire EBICS

*Version 5.2.5*

**Remarque**

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 25.

**Copyright**

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- <http://www.fr.ibm.com> (serveur IBM en France)
- <http://www.ibm.com/ca/fr> (serveur IBM au Canada)
- <http://www.ibm.com> (serveur IBM aux Etats-Unis)

*Compagnie IBM France  
Direction Qualité  
17, avenue de l'Europe  
92275 Bois-Colombes Cedex*

© Copyright IBM France 2015. Tous droits réservés.

La présente édition s'applique à la version 5.2.2 de Sterling B2B Integrator et à toutes les éditions et modifications ultérieures, sauf mention contraire dans les nouvelles éditions.

© **Copyright IBM Corporation 2000, 2015.**

---

## Table des matières

|  |          |   |           |
|--|----------|---|-----------|
| <b>Avis aux lecteurs canadiens . . . . .</b>             | <b>v</b> | Segmentation et récupération . . . . .            | 11        |
|  |          | Traitement VEU . . . . .                          | 12        |
| <b>Concepts de serveur EBICS (version</b>                |          | Gestion des clés . . . . .                        | 13        |
| <b>5.2.5 ou ultérieure) . . . . .</b>                    | <b>1</b> | Générer et récupérer des rapports EBICS . . . . . | 15        |
| Architecture du serveur bancaire EBICS . . . . .         | 2        | Gestion du serveur EBICS . . . . .                | 15        |
| Gestion des informations du gestionnaire                 |          | Gestion des commandes système . . . . .           | 16        |
| d'abonnements . . . . .                                  | 6        | Traitement des données de commande . . . . .      | 19        |
| Gestion des transactions EBICS . . . . .                 | 8        | Intégration à Sterling File Gateway . . . . .     | 22        |
| Chargement à partir d'un abonné (FUL) . . . . .          | 9        |   |           |
| Téléchargement à partir du serveur EBICS (FDL) . . . . . | 10       | <b>Remarques . . . . .</b>                        | <b>25</b> |



---

## Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

### Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

### Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

| IBM France                    | IBM Canada             |
|-------------------------------|------------------------|
| ingénieur commercial          | représentant           |
| agence commerciale            | succursale             |
| ingénieur technico-commercial | informaticien          |
| inspecteur                    | technicien du matériel |

### Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.








### OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

### Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

| France   | Canada  | Etats-Unis        |
|--|---|-------------------|
|  (Pos1)     |  | Home              |
| Fin  | Fin   | End               |
|  (PgAr)     |  | PgUp              |
|  (PgAv)     |  | PgDn              |
| Inser  | Inser   | Ins               |
| Suppr  | Suppr   | Del               |
| Echap  | Echap   | Esc               |
| Attn   | Intrp   | Break             |
| Impr<br>écran  | ImpEc   | PrtSc             |
| Verr<br>num  | Num   | Num<br>Lock       |
| Arrêt<br>défil   | Défil   | Scroll<br>Lock    |
|  (Verr maj) | FixMaj  | Caps<br>Lock      |
| AltGr  | AltCar  | Alt<br>(à droite) |

## Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

## Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.



---

## Concepts de serveur EBICS (version 5.2.5 ou ultérieure)

EBICS (Electronic Banking Internet Communication Standard) est une norme de communication et de sécurité basée sur Internet qui est principalement utilisée pour le transfert de données à distance entre votre organisation et une banque pour les transactions de paiement de l'entreprise.

EBICS permet l'échange de fichiers de données quels que soient les normes et les formats de message utilisés. EBICS utilise des procédures de chiffrement et de signature numérique reconnues. Ses fonctions sont basées sur des normes internationales pour la communication Internet et la sécurité améliorée comme, par exemple, XML, HTTPS, TLS et SSL. EBICS possède également des capacités multi-bancaires où les clients de l'entreprise dans les pays qui ont adopté EBICS peuvent faire des transactions avec n'importe quelle banque dans ces pays qui utilisent le même logiciel.

L'utilisateur (associé à un partenaire) doit remplir une série de conditions préalables pour pouvoir effectuer des transactions techniques/bancaires EBICS avec une banque spécifique. La condition préalable de base pour effectuer des transactions EBICS est la signature d'un contrat entre le partenaire et la banque. Les informations suivantes sont définies dans le cadre de ce contrat :

- La nature des transactions commerciales (types de commandes techniques/bancaires) que le partenaire va effectuer avec la banque
- Des informations sur les comptes bancaires de l'utilisateur.
- Les utilisateurs associés au partenaire qui travaillent avec le système de la banque
- Les autorisations et les droits dont dispose l'utilisateur

Le partenaire reçoit les données d'accès de la banque (paramètres bancaires) après la signature du contrat. La banque configure les données maître du partenaire et de l'utilisateur dans le système bancaire conformément aux dispositions contractuelles.

Les autres conditions préalables sont l'initialisation réussie de l'abonné, le téléchargement des certificats publics de la banque par l'utilisateur et la vérification réussie des certificats publics de l'utilisateur par la banque.

Le serveur bancaire EBICS Sterling B2B Integrator est une solution EBICS complète incluant une banque et un partenaire et assurant la gestion des utilisateurs et des certificats, les transactions par fichiers sécurisées, la reprise en cas d'erreur et la génération de rapports. Utilisez Sterling B2B Integrator pour envoyer ou recevoir des transactions EBICS.

Le serveur bancaire EBICS Sterling B2B Integrator prend en charge la spécification EBICS version 2.5 pour les implémentations en français et en allemand.

Sterling File Gateway fonctionne sur la plateforme Sterling B2B Integrator et permet le transfert sécurisé des fichiers entre des partenaires internes et externes à l'aide de protocoles de communication, de conventions de dénomination de fichiers et de format de fichier identiques ou différents. Sterling File Gateway prend en charge les mouvements liés à des transferts de fichiers importants et très volumineux ; il offre une visibilité des mouvements de fichiers dans une structure

orientée processus hautement évolutive, qui permet de relever les défis posés par les transferts de fichiers, comme le courtage de protocoles et de fichiers, l'automatisation et la sécurité des données.

## **Espace requis du système de fichiers pour les demandes FDL**

Parce que le type de commande FDL utilise le système de fichiers pour stocker le contenu, il est important de planifier le stockage du système de fichiers en conséquence. Un grand contenu FDL nécessite environ 6 fois plus d'espace fichier que la taille du contenu lui-même. Par exemple, un contenu de 5 Go nécessite plus de 30 Go d'espace fichier dans Sterling B2B Integrator pour traiter la demande.

Lorsque vous utilisez EBICS Banking Server dans un environnement cluster, vous devez configurer le système de fichier partagé comme stockage de documents entre les noeuds, même si le type de stockage de documents par défaut est défini sur "Base de données". Pour les instructions, consultez la documentation d'*Installation* appropriée.

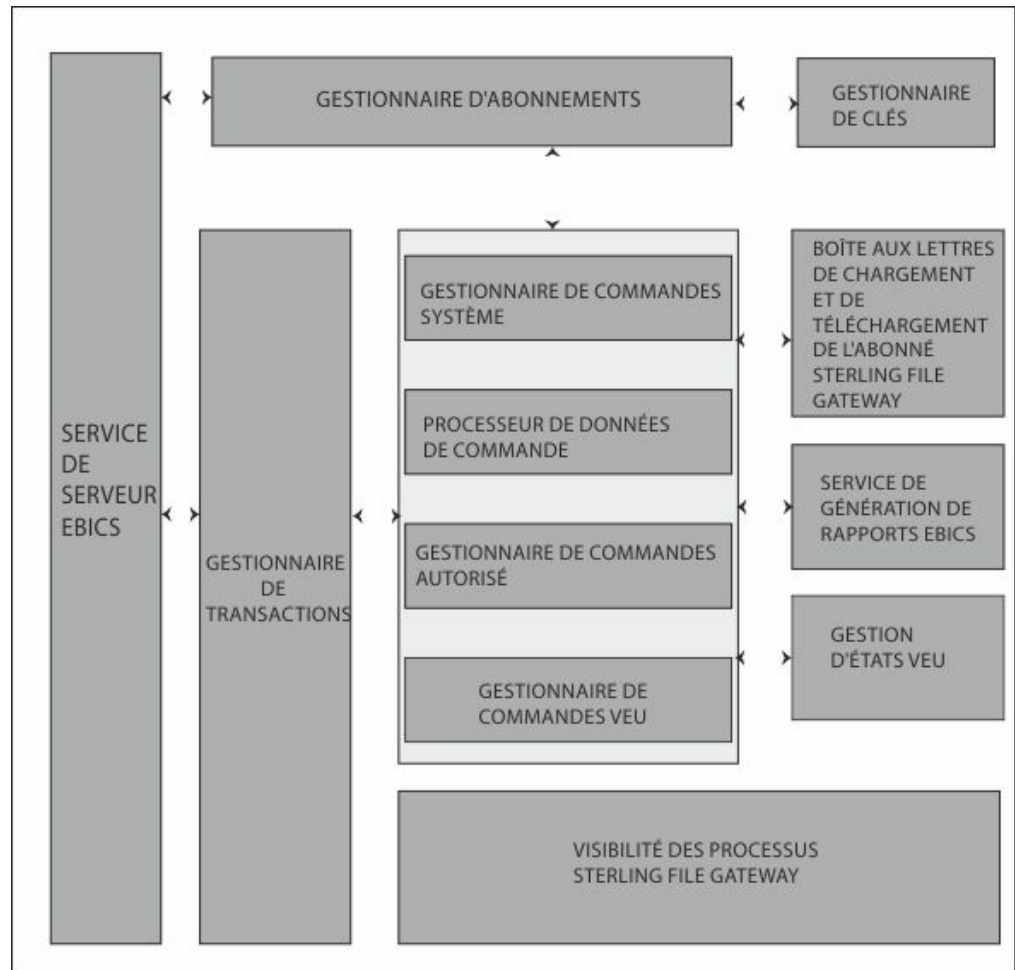
---

## **Architecture du serveur bancaire EBICS**

Le serveur bancaire EBICS permet d'effectuer des transactions avec des partenaires et des utilisateurs via EBICS.

Ses fonctions comprennent la création et la gestion des profils (banques, partenaires et utilisateurs), l'association de partenaires et d'utilisateurs à des types de commande et à des formats de fichier, l'affectation de droits d'utilisateur, la création et la gestion de certificats, le traitement des données de commande, le stockage et l'extraction des informations de profil, des certificats et des messages, la gestion des flux de messages et de transaction, le transfert des fichiers à l'aide de protocoles sécurisés, etc.

Le diagramme suivant présente l'architecture du serveur bancaire EBICS :



Le *gestionnaire d'abonnements* comprend les fonctions suivantes :

- Gestion de profil - Pour créer et gérer des profils de banques, partenaires et utilisateurs
- Configuration de type de commande - Pour configurer des types de commandes et des formats de fichier
- Configuration d'offre - Pour grouper un ensemble de types de commandes et de formats de fichier avec une liste de clients
- Configuration des droits utilisateur - Pour affecter des types de commande et des formats de fichier aux utilisateurs
- Importation d'informations du gestionnaire d'abonnements - Pour importer les informations de configuration des banques, des partenaires, des utilisateurs, des offres, des droits d'utilisateur, des types de commande et des formats de fichier sur le serveur bancaire EBICS depuis un répertoire externe
- Exportation d'informations du gestionnaire d'abonnements - Pour exporter les informations de configuration des banques, des partenaires, des utilisateurs, des offres, des droits d'utilisateur, des types de commande et des formats de fichier dans un répertoire externe à partir du serveur bancaire EBICS

Les *boîtes aux lettres de chargement et de téléchargement de l'abonné* sont configurées dans le gestionnaire d'abonnements lors de la configuration des abonnements de l'utilisateur.

La *gestion de clés* forme une interface principalement avec le gestionnaire d'abonnements pour créer, mettre à jour, supprimer et interroger des certificats.

La gestion de clés inclut les fonctions suivantes :

- Les certificats autosignés - Pour la génération et la gestion des certificats autosignés qui utilisent une longueur de 2048 clés
- Certificats de l'autorité d'accréditation - Pour la gestion des certificats de l'autorité d'accréditation
- Certificat de clés - Pour fournir les fichiers de clés pour les certificats et gérer le renouvellement et l'expiration des certificats
- Importation et exportation de certificats - Pour importer et exporter des certificats
- Validation de la clé de l'abonné - Pour valider les valeurs hachées du certificat de l'abonné
- Valeur hachée du certificat - Pour prendre en charge la création de la valeur hachée du certificat grâce à SHA256

Interface de *service de serveur EBICS* avec un gestionnaire d'abonnements pour récupérer les informations de profil des banques, partenaires, utilisateurs et types de commandes nécessaires à la vérification et l'authentification des messages et des transactions. Elle fonctionne en collaboration étroite avec le gestionnaire de transactions pour gérer toutes les transactions EBICS.

Le service de serveur EBICS comprend les fonctions suivantes :

- Demande et réponse - Pour traiter les demandes EBICS entrantes (via HTTP et HTTPS) selon les spécifications du protocole EBICS et renvoyer une réponse appropriée au demandeur
- Flux de messages - Pour gérer le flux de messages pour l'initialisation et les phases de transfert de fichiers des transactions EBICS
- Authentification et autorisation - Pour effectuer des authentifications de messages et des vérifications d'autorisation d'utilisateur

Le *gestionnaire de transactions* forme une interface étroite avec le service de serveur EBICS pour gérer le flux de chargement et de téléchargement des types de commande système et des types de commandes techniques/bancaires.

Le gestionnaire de transactions comprend les fonctions suivantes :

- Transaction asynchrone - Pour gérer le flux de transactions asynchrones pour le type de commande de chargement technique/bancaire (FUL). Elle gère le flux de traitement des commandes autorisé en collaboration avec le processeur de données de commandes pour décompresser les données de commande et transmettre les données de commandes décompressées à la boîte aux lettres de chargement de destination, selon les paramètres de profil d'utilisateur.
- Transaction synchrone - Pour gérer le flux de transactions synchrones pour des types de commandes système et techniques/bancaires de chargement et téléchargement. Elle gère les flux de traitement des commandes système, de traitement de rapports (FDL, PSR) et de traitement des commandes techniques/bancaires (FDL).
- Segmentation et reprise - Pour gérer les reprises sur non-répétition, segmentation et incident

Le *gestionnaire de commandes système* est responsable de la mise à jour et de l'analyse des informations de gestion des clés et des informations des référentiels d'utilisateurs.

Le gestionnaire de commandes système travaille en étroite collaboration avec le gestionnaire de transactions et le gestionnaire d'abonnements pour mettre à jour et analyser les certificats de clé et les informations des référentiels d'utilisateurs ou pour télécharger les paramètres et les certificats bancaires.

Le *gestionnaire de commandes autorisé* est responsable du lancement du processeur de données de commande pour décompresser les données de commande à partir de la demande de type de commande FUL. Il est également chargé du l'acheminement des données de commande décompressées vers la boîte aux lettres de chargement de l'abonné en arrière plan et de son changement de nom selon une convention de dénomination définie.

Le *gestionnaire de commandes VEU* est responsable du traitement des commandes VEU (types de commande HVD, HVE, HVS, HVT, HVU ou HVZ).

Le *processeur de données de commande* est responsable de la compression et de la décompression des données de commande. Il sert d'interface avec le gestionnaire d'abonnements et le gestionnaire de transactions pour récupérer les informations pertinentes obligatoires pour la compression et la décompression des données de commande. Ses fonctions comprennent :

- Compression - Pour compresser des données de commande telles que la signature, la compression, le chiffrement et le codage base64 selon les exigences du type de commande
- Décompression - Pour décompresser les données de commande telles que la vérification, la décompression, le déchiffrement et le décodage base64 selon les exigences du type de commande

Le *service de génération de rapports* est responsable de la génération de rapports d'état de paiement (PSR) associée à la décompression de données de commande lors d'un chargement asynchrone de flux de transactions de commandes techniques/bancaires.

La fonction de *gestion d'états VEU* est responsable de la gestion des informations des commandes VEU qui n'ont pas encore été intégralement autorisées (signatures en attente, par exemple).

*Sterling File Gateway* utilise des modèles pour décrire comment chaque transaction EBICS est interprétée afin de déterminer comment et où elle doit être transmise. Il fournit les détails des transferts à des fins d'audit et de dépannage.

Sterling File Gateway comprend les fonctions suivantes :

- Transformations de fichiers ou de noms de fichier - Pour le mappage des noms du fichier d'entrée et de sortie, des stratégies propres aux systèmes, aux groupes et aux partenaires, des tâches communes de traitement de fichiers, telles que la compression et la décompression, le chiffrement et le déchiffrement PGP et la signature
- Visibilité de transfert de fichiers - Les événements sont enregistrés pour la surveillance et la génération de rapports ; le suivi détaillé de traitement de structure de fichier d'entrée et de sortie et la détermination de chemin dynamique ; la capacité de consulter et de filtrer les flux de données pour tous les utilisateurs

- Support de protocole de communication étendu - FTP, FTP/S, SSH/SFTP, SSH/SCP et Sterling Connect:Direct sont pris en charge lors de l'installation et des protocoles supplémentaires (tels que AS2, AS3 ou Odette FTP) peuvent être configurés à l'aide de la fonction d'extensibilité
- L'interface partenaire (myFileGateway) - Interface basée sur un navigateur Web qui permet aux partenaires de charger/télécharger des fichiers, de s'abonner à des notifications d'événements, de gérer des mots de passe, de rechercher et d'afficher les activités de transfert de fichiers et de générer des rapports sur ce type d'activité
- Structures de boîte aux lettres flexible - Possibilité de spécifier des structures de boîte aux lettres qui optimisent des stratégies de correspondance et capacité de définir des attributs qui doivent être vrais pour tous les partenaires ou un sous-ensemble de partenaires
- Acheminement dynamique - Client dérivé pendant la phase d'exécution, soit par la structure de boîte aux lettres, le nom de fichier, le nom du client dérivé du processus technique ou le nom du client dérivé de la mappe

---

## Gestion des informations du gestionnaire d'abonnements

Le menu Gestionnaire d'abonnements de Sterling B2B Integrator permet d'effectuer les opérations suivantes :

- Créer et gérer des profils banque, partenaire et utilisateur dans la base de données système
- Créer et gérer des offres
- Assigner des types de commande et des formats de fichier à une offre
- Assigner des droits aux utilisateurs

Une banque peut avoir un seul profil avec un ID de banque unique. Un profil de banque contient les informations suivantes :

- ID unique de la banque

**Remarque :** Chaque ID de banque devrait avoir un numéro de port unique.

- Nom de la banque
- Adresse de la banque
- Certificats de chiffrement, d'authentification et d'identification publics et privés
- URL HTTP de la banque
- Version du protocole EBICS

Une banque peut avoir plusieurs URL. L'URL de la banque correspondante est donnée à un utilisateur pour envoyer les demandes à la banque. L'URI est configuré dans l'adaptateur du serveur HTTP pour écouter le port et recevoir les demandes EBICS, le cas échéant.

Les versions suivantes des types et des protocoles bancaires sont prises en charge :

- Version du protocole EBICS - H004, H003, H000
- Versions des signatures - A005, A006
- Version d'authentification - X002
- Version de chiffrement - E002

Chaque partenaire peut avoir plusieurs informations de compte et ID de partenaire. Vous devez indiquer le numéro de compte, soit au format national

(allemand) ou international (IBAN). Vous pouvez associer un ID de partenaire à une offre. Le profil de partenaire contient les informations suivantes :

- ID unique du partenaire
- Code d'organisation du partenaire
- Nom du partenaire
- Adresse du partenaire
- ID du compte et nom du titulaire du compte
- Devise dans laquelle la transaction est effectuée
- Numéro de compte
- Code de banque

Un utilisateur peut être en-dessous d'un ou plusieurs partenaires. Une banque peut créer un utilisateur en associant ou non un utilisateur à un partenaire. Pour permettre un échange de messages EBICS entre un partenaire et un utilisateur, vous devez associer un ID utilisateur à un ID de partenaire.

Un utilisateur transmet les certificats publics à la banque selon deux canaux de communication indépendants :

- INI - Envoie la clé technique bancaire publique
- HIA - Envoie la clé d'identification et d'authentification publique et la clé de chiffrement public

Lorsqu'un utilisateur est d'abord assigné à un partenaire, le statut de l'utilisateur est Nouveau. Si l'utilisateur envoie uniquement une demande INI à la banque correspondante, le statut est modifié en Partiellement Initialisé (INI). Si l'utilisateur envoie uniquement une demande HIA à la banque, le statut est modifié en Partiellement Initialisé (HIA). Après l'envoi à la banque des deux demandes (INI et HIA) par l'utilisateur, le statut est modifié en Initialisé. L'utilisateur envoie les lettres d'initialisation des clés INI et HIA à la banque. Lorsque la banque reçoit les lettres d'initialisation appartenant à INI et HIA, elle vérifie les valeurs hachées dans les certificats par rapport à sa base de données. Une fois la vérification terminée, le statut de l'utilisateur est modifié en Prêt, ce qui signifie que l'utilisateur peut désormais faire des transactions avec la banque. L'utilisateur télécharge ensuite les certificats publics de la banque en utilisant le type de commande système HPB.

Vous pouvez utiliser les types de commande HKD et HTD pour extraire les informations d'abonné stockées par la banque une fois que l'utilisateur possède le statut *Prêt*.

Utilisez le service du gestionnaire d'abonnements EBICS pour valider les clés sur les lettres d'initialisation INI et HIA. Une fois la validation terminée, le statut de l'utilisateur est mis à jour, (Prêt, par exemple), ce qui signifie que l'utilisateur a envoyé les lettres d'initialisation HIA et INI à la banque. Vous pouvez également utiliser ce service pour importer ou exporter les données du gestionnaire d'abonnements vers ou à partir de la base de données du système de la banque.

Le profil utilisateur contient les informations suivantes :

- ID unique de l'utilisateur
- Nom de l'utilisateur
- Adresse de l'utilisateur
- ID du partenaire auquel l'utilisateur est associé

- Paramètres de la boîte aux lettres pour pouvoir télécharger et archiver les messages

Les types de commande EBICS indiquent les diverses transactions qui peuvent avoir lieu entre le serveur EBICS et un client EBICS. Un type de commande peut n'avoir aucun format de fichier ou en avoir plusieurs. Vous pouvez associer des formats de fichier aux types de commande de téléchargement techniques bancaires. Vous pouvez le téléchargement des types de commande pour télécharger des données de commandes d'un client EBICS vers un serveur EBICS et télécharger les types de commande pour télécharger les données de commande d'un serveur EBICS vers un client EBICS. Un type de commande contient les attributs suivants :

- Le type de commande
- Version du protocole EBICS
- Type de transfert - Type de téléchargement
- Type de données de commande - Système ou technique

Un format de fichier contient les attributs suivants :

- Le format de fichier
- Indicatif de pays du format de fichier

Une banque peut créer une ou plusieurs offres. Une offre fournit une méthode simple pour grouper un ensemble de types de commande et de formats de fichier à une liste de partenaires. À chaque partenaire est attribuée une liste de types de commande pour permettre les transactions entre la banque et le partenaire. Une offre fournit un moyen facile à la banque de mettre en place un contrat avec le partenaire. Une offre contient les informations suivantes :

- ID de la banque
- Nom de l'offre
- Les types de commande et les formats de fichier pour lesquels le partenaire peut échanger des messages
- Niveau d'autorisation du type de commande
- Nombre de signatures nécessaires pour autoriser la commande

Un partenaire peut être associé à un ou plusieurs utilisateurs. Une banque affecte les droits suivants à un utilisateur :

- Les types de commande et les formats de fichier pour lesquels l'utilisateur peut échanger des messages
- Niveau d'autorisation du type de commande
- Le montant maximal d'une transaction d'un utilisateur (compte d'un partenaire spécifique). Vous pouvez associer plusieurs comptes de partenaire à un montant maximal différent.
- La devise dans laquelle le montant maximal de l'utilisateur est indiqué. Elle varie en fonction du compte du partenaire associé au montant maximal.

---

## Gestion des transactions EBICS

Le gestionnaire de transactions du serveur EBICS est responsable de la maintenance des états de transaction. Il détermine le segment qui est requis pour générer le message de réponse XML.



Le gestionnaire de transactions assure le chargement et le téléchargement des flux de transactions et prend en charge la segmentation et la récupération de données de commande.

## Chargement à partir d'un abonné (FUL)

Le type de commande FUL est utilisé pour envoyer les données par téléchargement vers une banque.

La transaction de chargement comprend les phases suivantes :

- Initialisation
- Transfert de données

L'utilisateur envoie la demande de chargement (FUL) à la banque. FUL est un type de commande de chargement technique/bancaire.

**Important :** Pour de grands contenus FUL, la valeur du paramètre Temps maximal d'inactivité (MaxIdleTime) d'EBICS Server Service doit être augmentée. Si la valeur de ce paramètre est trop faible, la transaction pourrait être annulée avant d'être terminée. La valeur appropriée pour de grands contenus FUL est 300 minutes.

Le service d'autorisation de commande EBICS traite les demandes de commande entrantes pour le type de commande de chargement technique/bancaire. Si une commande a obtenu le nombre requis de signatures, ce service transmet la commande à la boîte aux lettres de chargement de l'abonné. Sinon, ce service conserve les données de commande dans la base de données jusqu'à ce que le nombre total de signatures nécessaires soit obtenu.

Le processus technique handleEBICSRequest reçoit une demande de l'utilisateur. Si la demande de l'utilisateur contient le dernier segment des données de commande, il appelle le processus technique EBICSOrderAuthorizationProcessing en mode asynchrone pour décompresser les données de commande et générer les fichiers suivants :

**Remarque :** La décompression des données de commande comprend le décodage, le déchiffrement et la décompression des mêmes données.

- .DAT - Contient les données de commande décompressées dans une boîte aux lettres de chargement d'un utilisateur
- .SIG - Contient la signature des données de commande dans une boîte aux lettres de chargement d'un utilisateur
- .PRM - Contient les paramètres de commande dans la boîte aux lettres de chargement de l'utilisateur
- .PSR - Contient un rapport de statut de traitement asynchrone dans la boîte aux lettres de téléchargement de l'utilisateur

## Initialisation du traitement

Un utilisateur démarre une transaction en soumettant les demandes contenant les informations sur la commande entrante. En se basant sur ces informations, le serveur EBICS vérifie le type de commande, effectue le test de répétition du message, vérifie l'authentification du message et les autorisations de l'utilisateur avant d'accepter la demande.

Après avoir vérifié les données de commande, la banque génère un identifiant de transaction et inclut l'identifiant dans sa réponse à l'utilisateur.

## Transfert de données de traitement

Lorsque plusieurs segments sont nécessaires pour transférer les données de commande, la banque effectue une authentification de message, vérifie la transaction, le numéro et la taille de segment. Après réception par le serveur EBICS du dernier segment des données de commande, les données de commande complètes sont transférées au processus technique EBICSOrderAuthorizationProcessing de manière asynchrone et la transaction se termine.

Le processus technique EBICSOrderAuthorizationProcessing décompresse les données de commande et les achemine vers la boîte aux lettres de chargement de l'utilisateur. Le processus technique EBICSOrderAuthorizationProcessing génère un rapport de post-traitement (PSR) et l'achemine vers la boîte aux lettres de téléchargement de l'utilisateur. Ce processus technique génère également les fichiers .SIG et .PRM à acheminer vers la boîte aux lettres de chargement de l'utilisateur. Un fichier .err est généré lorsque le processus technique EBICSOrderAuthorizationProcessing détecte une erreur, comme une signature électronique non valide. Utilisez le fichier .err pour examiner un fichier de données de commande non valide, si nécessaire.

## Téléchargement à partir du serveur EBICS (FDL)

Le type de commande FDL est utilisé pour télécharger les données d'une banque.

La transaction de téléchargement comprend les phases suivantes :

- Initialisation
- Transfert de données
- Accusé de réception

Un utilisateur soumet un type de commande FDL à la banque. L'utilisateur demande le téléchargement du rapport .PSR pour obtenir le statut de la demande FUL. L'utilisateur peut également demander de télécharger des formats de fichier valide autres que .PSR en utilisant le type de commande FDL.

**Important :** Pour de grands contenus FDL, la valeur du paramètre Temps maximal d'inactivité (MaxIdleTime) d'EBICS Server Service doit être augmentée. Si la valeur de ce paramètre est trop faible, la transaction pourrait être annulée avant d'être terminée. La valeur appropriée pour de grands contenus FDL est 300 minutes.

### Initialisation du traitement

La banque vérifie le message de l'utilisateur. Après avoir vérifié la demande de l'utilisateur, la banque collecte les données de commande dans la boîte aux lettres de téléchargement de l'utilisateur basées sur les informations de format de fichier de la demande.

Si plus d'un message correspond au format de fichier, la banque joint le contenu de chaque message dans des données de commande uniques et fait appel de manière synchrone au processeur de données de commande pour comprimer les données de commande.

Si le formulaire encodé des données de commande dépasse 1 Mo, les données de commande sont séparées en segments. Le premier segment de données de commande et l'ID de transaction sont compris dans la réponse à l'utilisateur.

## Transfert de données de traitement

L'utilisateur envoie la demande pour le segment de données suivant. La banque authentifie le message, vérifie la transaction et le numéro et la taille du segment.

Dans chaque phase de transfert, la banque transfère tous les segments jusqu'à ce que le dernier segment des données de commande soit inclus dans sa réponse à l'utilisateur.

## Accusé de réception des données de traitement

Après avoir reçu le dernier segment des données de commande de la part de la banque, l'utilisateur initie la dernière phase, la demande d'accusé de réception, pour indiquer que le transfert de données s'est déroulé avec succès.

Si la banque reçoit un accusé de réception positif (code de réception=0) de la part de l'utilisateur, la banque déplacera les messages téléchargés de la boîte aux lettres de téléchargement vers la boîte aux lettres d'archives de l'utilisateur. Si la banque reçoit un accusé de réception négatif de la part de l'utilisateur, la banque retiendra les messages téléchargés dans la boîte aux lettres de téléchargement de l'utilisateur.

Si un utilisateur souhaite télécharger des formats de fichier valides autres que les rapports .PSR à partir de la boîte aux lettres d'archives de l'utilisateur, celui-ci doit indiquer une plage de dates dans la demande EBICS. L'utilisateur doit s'assurer que la plage de dates corresponde à la date de déplacement du fichier .DAT entre la boîte aux lettres de téléchargement de l'utilisateur et la boîte aux lettres d'archives.

## Segmentation et récupération

La demande de données de commande (téléchargement) ne peut pas dépasser 1 Mo au format compressé, chiffré, codé base64. Si la demande de données de commande dépasse 1 Mo, le format codé doit être divisé en segments. Le serveur bancaire EBICS est chargé de combiner tous ces segments pour rétablir les données de commande dans leur format d'origine.

Si une erreur se produit lors de la livraison des segments de données de commande, on peut effectuer la récupération. L'utilisateur peut télécharger le segment approprié selon le point de récupération envoyé en réponse par le serveur.

La récupération permet la transmission d'une commande pour continuer malgré une erreur, sans avoir à retransmettre tous les segments de données de commande qui ont été transmis avec succès.

Un point de récupération peut être utilisé pour poursuivre les transactions à partir de l'étape de transaction qui suit ce point de récupération dans la séquence d'étape de transaction. Les points de récupération doivent être définis lors du processus de reprise :

- Pour les transactions de téléchargement, le point de récupération est la dernière étape de transaction au cours de laquelle la banque a reçu avec succès le message de demande et transmis une réponse à l'utilisateur. Le point de récupération est déterminé par l'état de la transaction dans le système bancaire.

- Pour les transactions de téléchargement, plusieurs points de récupération peuvent exister. Toutes les étapes de transaction précédentes au cours desquelles la banque a reçu avec succès le message de demande et transmis une réponse à l'utilisateur.

## Traitement VEU

Le serveur bancaire EBICS prend en charge la signature électronique distribuée (VEU) qui permet à plusieurs partenaires (ou abonnés) d'autoriser une commande.

VEU est une abréviation allemande qui signifie Signature électronique distribuée. Elle permet à plusieurs partenaires (ou abonnés) d'autoriser une commande. Différents partenaires de plusieurs clients ou du même client peuvent signer une commande spécifique. Les partenaires peuvent demander les commandes dont les signatures sont en attente et les signer ou les annuler. Le système de gestion VEU du serveur bancaire EBICS sauvegarde les commandes en attente de signatures de différents partenaires jusqu'à ce que l'un des événements suivants se produise :

- Le nombre nécessaire de signatures autorisées a été reçu.
- La commande est annulée.

VEU utilise les types de commande suivants :

- HVU
- HVD
- HVZ
- HVE
- HVS
- HVT (facultatif)

Les signataires autorisés d'un client peuvent utiliser différents processus de signature capables de prendre en charge plusieurs processus de hachage générant différentes valeurs hachées. Dans le processus VEU, la valeur hachée des données de commande est fournie lorsque les types de commande HVD et HVZ sont exécutés. Cette valeur hachée est établie à partir de la version de la signature utilisée par l'abonné exécutant HVZ et HVD. La valeur hachée est fournie avec la version de la signature utilisée en tant qu'attribut.

La section suivante présente un récapitulatif des processus VEU standard :

1. Un client EBICS (Partenaire A) soumet une commande en transmettant les données de commande dans une transaction EBICS avec l'attribut de commande OZHNN et en la signant avec la classe de signature E, ou T.
2. Lorsque la commande est reçue par le serveur bancaire EBICS, le système de gestion VEU analyse le type de la commande et les signatures qui ont déjà été soumises, y compris leur classe. Si d'autres signatures sont nécessaires pour traiter la commande, celle-ci est stockée provisoirement pour le processus VEU avec sa valeur hachée.
3. Un autre client EBICS (Partenaire B) qui a une signature en attente et doit signer une commande stockée effectue une demande d'informations à l'aide du type de commande HVU ou HVZ pour identifier les commandes qu'il est autorisé à signer. La réponse inclut les informations suivantes :
  - Type de commande
  - Numéro de commande
  - Nombre de signatures nécessaires et nombre déjà atteint (en déterminant si leur propre signature est nécessaire ou a déjà été donnée)

- Partie d'origine de la commande
- Taille des données de commande non compressées
- (Type de commande HVZ uniquement) La valeur hachée des données de commande

Si le type de commande HVZ a été utilisé, ignorez l'étape suivante.

4. Le partenaire B utilise le type de commande HVD pour vérifier la commande et obtenir la valeur hachée associée.
5. Facultatif. Si le type de commande HVT est pris en charge par la banque, le partenaire B peut télécharger des informations supplémentaires sur la commande en utilisant le type de commande HVT. En fonction des paramètres de la demande, il reçoit des informations sur des transactions spécifiques de la commande (données du compte, montant, date de traitement, données d'utilisation et autres descriptions) ou sur l'ensemble des données de la commande.
6. Lorsque toutes les informations nécessaires sont reçues, le partenaire B peut signer la commande à l'aide du type de commande HVE. Le système de gestion VEU du serveur bancaire EBICS valide et ajoute la signature à la commande.
7. Le partenaire B peut décider d'annuler la commande à l'aide du type de commande HVS.
8. Lorsque toutes les signatures sont obtenues, le serveur bancaire EBICS traite la commande dans son intégralité.

---

## Gestion des clés

Vous pouvez insérer, mettre à jour et extraire des certificats stockés dans le référentiel Sterling B2B Integrator.

Vous pouvez insérer un certificat codé en base64 (public ou privé) et importer et exporter des certificats dans le référentiel Sterling B2B Integrator.

Vous pouvez également effectuer les tâches suivantes dans Sterling B2B Integrator :

- Créez un certificat autosigné avec la longueur de clé de 2048 pour EBICS
- Gérez les certificats de l'autorité de certification
- Stockez les certificats et gérez le renouvellement et l'expiration des certificats
- Acceptez un certificat public d'un utilisateur
- Validez les clés d'abonné suivantes en utilisant SHA256 comme algorithme de hachage :
  - Valeur de hachage de clés d'identification et d'authentification (au format Hex)
  - Valeur de hachage de clé de chiffrement (au format Hex)
  - Valeur de hachage de clé de signature électronique (au format Hex)

Utilisez le service d'exportation de certificats EBICS pour exporter les certificats stockés dans Sterling B2B Integrator vers un système externe. Utilisez ce service lorsque vous souhaitez synchroniser les certificats stockés dans Sterling B2B Integrator avec une base de données ou un système externe.

Utilisez le service d'importation de certificats EBICS pour ajouter des certificats d'un référentiel externe à Sterling B2B Integrator. Vous pouvez également supprimer les certificats qui ont expiré ou sont invalides.

## Fonction du gestionnaire de clés

La fonction de gestion et de stockage des clés effectue les opérations suivantes :

- Validation de clés en double : Le certificat utilisé pour l'authentification ou le chiffrement ne doit pas être identique au certificat à signature électronique. Utilisez un jeu de clés unique pour l'authentification ou le chiffrement et la signature.
- Extension de l'utilisation des clés X.509 – Le serveur bancaire EBICS prend en charge la norme X.509 pour l'extension de l'utilisation des clés.
- Vérification des certificats OCSP et CRL

Le gestionnaire de clés gère les certificats du référentiel Sterling B2B Integrator. Il insère, met à jour et extrait les certificats dans le référentiel Sterling B2B Integrator et exécute des fonctions, telles que le calcul de la valeur hachée du certificat.

Le gestionnaire de clés valide les certificats du client archivés sur le serveur pour permettre leur utilisation. Vous devez obtenir des certificats signés par une autorité de certification auprès d'une autorité de certification. Dans un certificat signé par une autorité de certification, l'émetteur signe le certificat. Pour vérifier l'authenticité du certificat de l'utilisateur, le serveur bancaire EBICS effectue une vérification de signatures en chaîne jusqu'au certificat de l'autorité de certification racine.

Avant d'exécuter des transactions EBICS, l'administrateur EBICS doit vérifier les certificats signés par l'autorité de certification et les certificats signés par une autorité de certification intermédiaire dans le magasin de certificats de l'autorité de certification Sterling B2B Integrator.

Le client doit fournir trois types de certificat :

- Certificat d'authentification
- Certificat de chiffrement
- Certificat avec signature électronique (ES)

La clé publique du certificat d'authentification est utilisée pour vérifier des signatures numériques. Les certificats d'authentification peuvent être des certificats signés par une autorité de certification ou des certificats autosignés. La valeur de la zone indiquant l'utilisation de la clé pour un certificat d'authentification est l'option de signature numérique. Une signature numérique est utilisée pour l'authentification d'entité et l'authentification de l'origine des données avec contrôle d'intégrité.

La clé publique du certificat de chiffrement permet de chiffrer les données de commande. Les certificats de chiffrement peuvent être des certificats signés par une autorité de certification ou des certificats autosignés. La valeur de la zone indiquant l'utilisation de la clé pour un certificat d'authentification est l'option de chiffrement de clé. Dans EBICS, une clé symétrique est utilisée pour transmettre les données de commande chiffrées et déchiffrées. La clé symétrique est chiffrée avec la valeur de la clé publique du certificat de chiffrement pour la transmission. L'option de chiffrement de clé est utilisée lorsqu'il y a un certificat avec un protocole qui chiffre des clés.

La clé publique du certificat avec signature électronique permet de vérifier la signature des données de commande. La valeur de la clé publique d'un certificat de signature électronique ne doit pas être identique à celle d'un certificat d'authentification ou de chiffrement. La valeur de la zone indiquant l'utilisation

d'une clé pour un certificat avec signature électronique est l'option de non-répudiation. Le mécanisme de non-répudiation permet d'éviter qu'une entité signataire refuse à tort une action et exclut la signature d'un certificat ou d'une liste de révocation de certificats. Les signatures électroniques sont de deux types :

- Signature de transport – Peut être signé par une autorité de certification ou autosigné
- Signature personnelle – Doit être signé par une autorité de certification

---

## Générer et récupérer des rapports EBICS

Utilisez le service de génération de rapports EBICS pour générer un rapport de statut de paiement (PSR) avec chaque demande de commande de téléchargement (FUL). Le rapport .PSR est au format XML et suit le schéma pain.002.001.02. Après la génération réussie du rapport .PSR, il est placé dans la boîte aux lettres de téléchargement de l'utilisateur EBICS.

Un rapport .PSR est généré après un traitement de commande asynchrone de chaque FUL. Un utilisateur peut envoyer une demande FDL avec le format de fichier pain.002.001.02.ack pour récupérer le rapport .PSR. S'il n'y a pas de plage de dates indiquée dans la demande EBICS, la banque concatène les rapports PSR dans la boîte aux lettres de téléchargement de l'utilisateur et intègre les données de commande dans la réponse EBICS.

Lorsque la banque reçoit un accusé de réception positif de l'utilisateur basé sur la valeur de paramètre fournie sous l'élément FDLOrderParams dans la demande FDL, les rapports .PSR dans la boîte aux lettres de téléchargement de l'utilisateur sont transférés dans la boîte aux lettres d'archivage de l'utilisateur. Si aucun accusé de réception positif n'est reçu après le délai d'attente spécifié, le planificateur du service de serveur EBICS attribue à nouveau la valeur 1 au nombre d'éléments extractibles pour les rapports .PSR dans la boîte aux lettres de téléchargement de l'utilisateur afin de permettre à l'utilisateur de télécharger à nouveau le rapport .PSR.

Si l'utilisateur souhaite télécharger les rapports .PSR à partir de la boîte aux lettres d'archivage de l'utilisateur, il doit indiquer une plage de dates dans la demande EBICS. L'utilisateur doit s'assurer que la plage de dates correspond à la date de déplacement du fichier .PSR entre la boîte aux lettres de téléchargement de l'utilisateur et la boîte aux lettres d'archivage.

---

## Gestion du serveur EBICS

Le serveur EBICS est mis en oeuvre en tant que service dans Sterling B2B Integrator. Le service de serveur EBICS est responsable du traitement des demandes EBICS entrantes (via HTTP et HTTPS), selon les spécifications du protocole EBICS, et de la génération et de l'envoi de la réponse appropriée aux utilisateurs.

Le serveur EBICS traite la génération et la vérification de la signature électronique (ES) et de l'identification et de l'authentification des messages EBICS. Il sert également d'interface au gestionnaire d'abonnements pour récupérer les informations de profil des banques, des partenaires, des utilisateurs et des types de commande nécessaires à la vérification et à l'authentification des messages et des transactions. Les flux de processus (asynchrone et synchrone) des demandes, tels que FUL et FDL, sont également gérés par le service. Vous pouvez configurer le service pour mettre à jour le référentiel EBICS et envoyer des notifications

d'événements à une application externe au cours d'une transaction synchrone. La gestion du flux de messages pour l'initialisation et le transfert des phases de transactions EBICS est également une des responsabilités clés du service. Le cycle de vie des transactions EBICS dans le système bancaire et le statut de transactions ouvertes sont gérés par le serveur EBICS, qui fonctionne également comme stockage intermédiaire pour les segments de données transmis et les signatures électroniques (ES).

Lors du téléchargement des données de commande techniques/bancaires, le serveur EBICS collecte toutes les données disponibles dans la boîte aux lettres de l'utilisateur et les concatène dans un seul document ; il envoie alors le document au processeur de données de commande pour le compresser, c'est-à-dire le signer, le compresser, le chiffrer et le coder.

Pour plus d'informations sur la configuration du service de serveur EBICS, reportez-vous à la rubrique relative au service de serveur EBICS.

---

## Gestion des commandes système

Le gestionnaire de commandes système fonctionne en étroite collaboration avec le gestionnaire de transactions et le gestionnaire d'abonnements pour mettre à jour et extraire les certificats de clé et les informations du référentiel d'utilisateurs, ou pour télécharger les paramètres et les certificats bancaires. Il génère et récupère des données de commande XML basées sur les informations de profil.

Le gestionnaire de commandes système assure également la mise en oeuvre des commandes système de chargement et de téléchargement. Le tableau suivant répertorie les types de commande système de chargement pris en charge pour les transactions EBICS :

| Type de commande système de chargement | Description  |
|--|--|
| INI                                    | Utilisé lors de l'initialisation de l'abonné. Envoie le certificat public technique bancaire d'un client au serveur EBICS Banking Server. Les données de commande sont compressées et codées en base64.  |
| HIA                                    | Utilisé pour transmettre les certificats publics de l'utilisateur pour l'identification, l'authentification et le chiffrement dans le cadre de l'initialisation de l'abonné. Les données de commande sont compressées et codées en base64.     |
| PUB                                    | Utilisé pour mettre à jour les certificats du client. Envoie le certificat public technique bancaire du client pour mettre à jour le serveur bancaire EBICS. Les données de commande sont signées, compressées, chiffrées et codées en base64. |



| Type de commande système de chargement | Description   |
|--|---|
| HCA                                    | Utilisé pour mettre à jour le certificat du client. Envoie les certificats suivants pour mettre à jour le serveur EBICS Banking Server : <ul style="list-style-type: none"> <li>• Certificat public d'identification et d'authentification</li> <li>• Certificat public de chiffrement</li> </ul> Les données de commande sont signées, compressées, chiffrées et codées en base64.   |
| HCS                                    | Utilisé pour mettre à jour le certificat du client. Envoie les certificats suivants pour mettre à jour le serveur EBICS Banking Server : <ul style="list-style-type: none"> <li>• Certificat public technique bancaire</li> <li>• Certificat public d'identification et d'authentification</li> <li>• Certificat public de chiffrement</li> </ul> Les données de commande sont signées, compressées, chiffrées et codées en base64. |
| SPR                                    | Utilisé pour suspendre l'autorisation d'accès d'un utilisateur. Les données de commande sont signées, compressées, chiffrées et codées en base64.   |

Le tableau suivant répertorie les types de commande du système de téléchargement pris en charge pour les transactions EBICS :

| Type de commande système de téléchargement | Description  |
|--|--|
| HPB  | Utilisé pour télécharger des certificats publics bancaires à partir du serveur EBICS Banking Server. Les données de commande sont compressées, chiffrées et codées en base64. Le message de réponse est signé avec une signature numérique XML à l'aide du certificat d'authentification. Les données de commande ne sont pas signées. |
| HPD  | Utilisé pour télécharger les paramètres bancaires à partir du serveur EBICS Banking Server. Les données de commande sont compressées, chiffrées et codées en base64. Le message de réponse est signé avec une signature numérique XML à l'aide du certificat d'authentification. Les données de commande ne sont pas signées.          |
| HEV  | Utilisé pour télécharger les informations sur les versions EBICS prises en charge. Le message de réponse est en texte clair. Il n'y a pas de données de commande dans une réponse HEV.   |

| Type de commande système de téléchargement | Description   |
|--|---|
| HKD  | Utilisé pour télécharger les données des clients et des abonnés. Peut être utilisé lorsque l'utilisateur possède le statut Prêt. Extrait les informations stockées par la banque et relatives à la société de l'abonné et aux abonnés associés (y compris les propres informations de la banque). Les données de commande sont compressées, chiffrées et codées en base64. Le message de réponse est signé avec une signature numérique XML à l'aide du certificat d'authentification. Les données de commande ne sont pas signées. |
| HTD  | Utilisé pour télécharger les données des clients et des abonnés. Peut être utilisé lorsque l'utilisateur possède le statut Prêt. Extrait des informations stockées par la banque et relatives à la société de l'abonné ou à la banque elle-même. Les données de commande sont compressées, chiffrées et codées en base64. Le message de réponse est signé avec une signature numérique XML à l'aide du certificat d'authentification. Les données de commande ne sont pas signées.  |

Le gestionnaire de commandes système extrait des informations stockées par la banque et relatives à la société de l'abonné. Les abonnés peuvent extraire les informations stockées par la banque et applicables à la société de l'abonné et à tous les abonnés associés à l'aide des types de commande HKD et HTD, une fois que le statut de l'utilisateur est Prêt (indiquant que l'utilisateur peut effectuer des transactions avec la banque). La réponse de la banque contient une liste des comptes du client.

Les informations de compte sont incluses dans la réponse HKD si au moins l'une des conditions suivantes est remplie :

- Le document contractuel signé avec la banque stipule que les relevés bancaires doivent être partagés avec le client
- Au moins l'un des abonnés du client est autorisé à signer pour ce compte

Les abonnés peuvent extraire des informations stockées par la banque, qui s'appliquent à la société de l'abonné ou incluent les propres informations de la banque à l'aide du type de commande HTD. Toutefois, les informations relatives aux abonnés associés de la société ne sont pas partagées dans ce type de commande. Vous devez utiliser le type de commande HKD pour extraire les informations relatives à la société et aux abonnés associés (y compris les propres informations de la banque). La réponse HKD et HTD inclut la liste des comptes associés du partenaire auxquels l'abonné est autorisé à accéder.

Le message de réponse de la commande système de téléchargement HKD inclut les paramètres suivants :

- HostID
- PartnerInfo - Inclut les informations du partenaire, telles que l'adresse, les informations des comptes auxquels l'abonné est autorisé à accéder et les types de commande que le partenaire est autorisé à utiliser.

- UserInfo - Inclut les détails de l'abonné, tels que l'ID de l'abonné, le statut de l'abonné et les droits de l'utilisateur. Les informations relatives aux droits de l'utilisateur incluent le niveau d'autorisation de la liste des types de commande, les comptes associés et le seuil limite du montant.

---

## Traitement des données de commande

Pour garantir un transfert sécurisé des données de commande, les données de commande doivent être compressées. La compression des données de commande inclut la signature, la compression, le chiffrement et le codage en base64 en fonction des spécifications du type de commande. Le récepteur doit décompresser les données de commande pour visualiser les attributs. La décompression des données de commande inclut la vérification, la décompression, le déchiffrement et le décodage en base64 en fonction des spécifications du type de commande.

Le processeur des données de commande est responsable de la compression et de la décompression des données de commande. Il sert d'interface avec le gestionnaire d'abonnements et le gestionnaire de transactions pour récupérer les informations pertinentes obligatoire pour la compression et la décompression des données de commande. Par exemple, les informations de profil peuvent inclure l'identifiant de transaction, le sens du flux (chargement ou téléchargement), le type de réponse (synchrone ou asynchrone), le type de processus requis, l'identifiant objet de la clé chiffrée et l'identifiant objet de la signature électronique (ES). Le service de traitement de commande EBICS effectue les transactions EBICS et la récupération utilisateur et la compression et la décompression des clés symétriques chiffrées. En fonction des informations de profil extraites, le service de traitement de la commande EBICS détermine si la compression ou la décompression des données de commande est nécessaire et appelle le service de compression ou décompression approprié.

Le gestionnaire de commandes autorisé est responsable du lancement du processeur de données de commande pour décompresser les données de commande à partir de la demande de type de commande FUL. Il est également chargé de l'acheminement des données de commande décompressées vers la boîte aux lettres de chargement de l'abonné en arrière-plan et de son changement de nom selon une convention de dénomination définie.

Hormis le service de traitement de commande EBICS, les services suivants sont disponibles dans Sterling B2B Integrator pour traiter les données de commande :

- Le service d'autorisation de commande EBICS traite les demandes de commande entrantes pour le type de commande de chargement technique/bancaire (FUL). Si une commande a obtenu le nombre de signatures nécessaires, ce service achemine la commande vers la boîte aux lettres de chargement de l'abonné. Sinon, ce service transfère la commande à la boîte aux lettres de la commande en attente.
- Le service du flot de données de commande EBICS compresse et décompresse les données de commande qui utilisent la fonction de pipeline de Sterling B2B Integrator.
- Le service de conditionnement du service de chiffrement EBICS compresse ou décompresse les informations clés qui sont utilisées pour la signature et la vérification du service de chiffrement.
- Le service de compression EBICS effectue la compression et la décompression des données de commande en utilisant zlib en mode pipeline.

- Le service de chiffrement EBICS effectue le chiffrement et le déchiffrement des données de commande en utilisant l'algorithme AES-128 en mode pipeline. L'algorithme de chiffrement E002 est pris en charge.
- Le service de codage EBICS effectue le codage et le décodage des données de commande en utilisant la méthode base64 en mode pipeline.
- Le service de signature EBICS effectue la signature et la vérification des données de commande sur l'historique SHA-256 calculé en mode pipeline. L'algorithme de signature A005 et A006 est pris en charge.

Les données de commande doivent être décompressées pour charger les transactions et compressées pour les récupérer.

Le processus de compression implique la séquence suivante. Cependant, basés sur le type de commande, un ou plusieurs des processus suivants ne sont peut-être pas obligatoires :

1. Signature
2. Compactage
3. Chiffrement
4. Codage base64

L'exemple suivant illustre le chiffrement d'un type de commande. Un processus technique fait appel au service de chiffrement. Si les données de commande ont été signées, le processus technique passe la clé symétrique au service de chiffrement. Si les données de commande n'ont pas été signées, le service de chiffrement génère et renvoie la clé symétrique au processus technique. Si la clé symétrique a été créée, le processus technique fait appel au service de traitement de commande EBICS avec le type de message de sortie défini sur `setEncryptedKey`.

Le processus de décompression implique la séquence suivante. Cependant, basés sur le type de commande, un ou plusieurs des processus suivants ne sont peut-être pas obligatoires :

1. Décodage base64
2. Déchiffrement
3. Décompression
4. Vérification de la signature

L'exemple suivant illustre le déchiffrement d'un type de commande. Un processus technique fait appel au service de traitement de commande EBICS avec le type de message de sortie défini sur `getEncryptedKey`. La clé secrète codée base64 est récupérée et définie dans les données de processus pour être utilisée par le service de chiffrement.

## Signatures électroniques

La signature électronique (ES) garantit l'authentification des données de commande. Les signatures garantissent l'intégrité et la non-répudiation des données de commande envoyées par le client au serveur bancaire.

EBICS spécifie deux classes pour la signature électronique :

- Signature personnelle
  - Signature unique de type E
  - Première signature de type A

- Seconde signature de type B
- Signature de transport de type T

Sterling B2B Integrator prend en charge les types de signature suivants :

- Signature de transport de type T
- Signature personnelle ou signature électronique technique/bancaire de type E – Signature unique

Les signatures de transport peuvent être des certificats autosignés ou signés par une autorité de certification. Les signatures personnelles doivent être des certificats signés par une autorité de certification ou reconnus par la banque. Utilisez la signature de transport pour soumettre la commande et la signature personnelle pour autoriser la commande.

Pour les signatures personnelles, vous devez indiquer le nombre de signatures pour chaque type de commande ou format de fichier dans le contrat pour traiter les données de commande. Le nombre maximal de signatures personnelles autorisé est 2. La signature personnelle de type E peut inclure les signatures suivantes :

- Unique
- Double facultative
- Double obligatoire

## **Prévalidation**

Lors de l'utilisation de type de commande de chargement technique/bancaire, l'abonné peut envoyer les informations à la banque lors de la première étape de la transaction. La banque peut prévalider les données de commande. La prévalidation des données de commande inclut les éléments suivants :

- Vérification du prétraitement des données
- Autorisation du compte
- Vérification du montant limite

Une fois que la prévalidation des données de commande a abouti, le système bancaire reçoit le fichier FUL. La banque peut utiliser la prévalidation pour traiter les données de commande si les conditions préalables suivantes sont remplies :

- La banque prend en charge la fonction de prévalidation
- Le noeud Prevalidation se trouve dans la demande entrante

### **Prévalidation du prétraitement des données**

La banque peut vérifier le prétraitement des données si les conditions préalables suivantes sont remplies :

- La banque prend en charge la fonction de prévalidation.
- Un noeud Prevalidation ou DataDigest se trouve dans la demande entrante.
- La commande peut correspondre à n'importe quel type de commande de chargement, à l'exception d'une demande SPR.

### **Prévalidation de l'autorisation du compte et montant limite**

La banque peut vérifier l'autorisation du compte et le montant limite si les conditions préalables suivantes sont remplies :

- La banque prend en charge la fonction de prévalidation.

- Le noeud Prevalidation ou AccountAuthorization se trouve dans la demande entrante.
- L'attribut OrderAttribute n'a pas pour valeur DZHNN dans la demande entrante.
- Le type de commande correspond au type de commande de chargement technique (FUL) dans la demande entrante.
- La classe de signature du signataire correspond au moins à la classe B dans les droits définis dans le contrat.

La prévalidation vérifie les informations du compte désigné par le signataire et le montant limite si le nombre minimal et maximal de signatures personnelles nécessaires pour autoriser la commande est défini. Le compte indiqué sous le noeud AccountAuthorization doit être un compte de partenaire valide. Tous les signataires doivent être configurés avec des droits d'utilisateur sur tous les comptes indiqués sous le noeud Prevalidation. Le montant de la devise indiquée ne doit pas dépasser le montant maximal défini dans la configuration du droit d'utilisateur du signataire.

---

## Intégration à Sterling File Gateway

Sterling File Gateway permet le transfert sécurisé de fichiers entre des partenaires internes et externes à l'aide de protocoles de communication, de conventions de dénomination et de formats de fichiers identiques ou différents. Sterling File Gateway prend en charge EBICS pour les mouvements générant des transferts de fichiers importants et très volumineux ; il offre une visibilité totale des mouvements de fichiers dans une structure orientée processus hautement évolutive, qui permet de relever les défis posés par les transferts de fichiers, comme le courtage de protocoles et de fichiers, l'automatisation et la sécurité des données.

Les fichiers sont transférés entre le serveur EBICS et Sterling File Gateway par l'intermédiaire de boîtes aux lettres partagées et de partenaires. Le gestionnaire d'abonnements crée des boîtes aux lettres dans la structure utilisateur/partenaire/boîte de réception lors de la création du partenaire.

Sterling File Gateway utilise des faits d'approvisionnement comme composant de la définition du modèle de canal de routage. Le modèle de canal de routage utilisé dans les scénarios EBICS doit comprendre la configuration de faits d'approvisionnement. Les canaux de routage utilisant les modèles doivent comprendre la spécification des valeurs pour les faits d'approvisionnement.

Pour les scénarios entrants, le processeur de données de commande (ODP) EBICS prend un téléchargement de fichier de commande (FUL) EBICS d'un client EBICS vers un serveur EBICS, décompresse la charge et la dépose dans une structure de boîte aux lettres utilisateur/partenaire/boîte de réception. Sterling File Gateway est configuré pour assurer l'acheminement à partir de cette boîte aux lettres pour le traitement en aval et la livraison finale au consommateur.

Dans le scénario sortant, Sterling File Gateway est configuré pour déposer un message dans la boîte aux lettres d'un client, qui est acheminé et stocké dans une structure utilisateur/partenaire/boîte d'envoi. Lors d'un téléchargement de fichier de commande (FDL) EBICS d'un client EBICS vers un serveur EBICS, le processeur de données de commande (ODP) EBICS compresse le message et le met à la disposition du client.

Sterling File Gateway permet aux opérateurs de rechercher des transactions et d'afficher des détails d'acheminement et de livraison.

Certaines procédures sont nécessaires pour effectuer l'intégration à Sterling File Gateway. Pour plus d'informations sur l'intégration à Sterling File Gateway, voir *Sterling File Gateway Integration with EBICS* à l'adresse [http://www.ibm.com/support/knowledgecenter/SS4TGX\\_2.2.0/com.ibm.help.sfg\\_ebics.doc/SFGEB\\_IntegrationwEBICS.html](http://www.ibm.com/support/knowledgecenter/SS4TGX_2.2.0/com.ibm.help.sfg_ebics.doc/SFGEB_IntegrationwEBICS.html).





---

## Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM® non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

*IBM Director of Licensing*

*IBM Corporation*

*North Castle Drive*

*Armonk, NY 10504-1785*

*U.S.A.*

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

*Intellectual Property Licensing*

*Legal and Intellectual Property Law*

*IBM Japan Ltd.*

*19-21, Nihonbashi-Hakozakicho, Chuo-ku*

*Tokyo 103-8510, Japan*

**Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales : LE PRÉSENT DOCUMENT EST LIVRÉ "EN L'ÉTAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DÉCLINE NOTAMMENT TOUTE RESPONSABILITÉ RELATIVE À CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DÉFAUT D'APTITUDE A L'EXÉCUTION D'UN TRAVAIL DONNÉ. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.**

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

*IBM Corporation*

*J46A/G4*

*555 Bailey Avenue*

*San Jose, CA 95141-1003*

*U.S.A.*

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

#### LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. IBM ne peut donc pas garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les exemples de programmes sont fournis "en l'état", sans garantie d'aucune sorte. IBM ne sera en aucun cas responsable des dommages liés à l'utilisation de ces programmes exemples.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit :

© IBM 2015. Des segments de code sont dérivés des Programmes exemples d'IBM Corp. © Copyright IBM Corp. 2015.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

## Marques

IBM, le logo IBM et [ibm.com](http://www.ibm.com) sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, le logo Adobe, PostScript et le logo PostScript sont des marques d'Adobe Systems Incorporated aux États-Unis et/ou dans certains autres pays.

IT Infrastructure Library est une marque de The Central Computer and Telecommunications Agency qui fait désormais partie de The Office of Government Commerce.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium et Pentium sont des marques d'Intel Corporation ou de ses filiales aux États-Unis et/ou dans certains autres pays.

Linux est une marque de Linus Torvalds aux États-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux États-Unis et/ou dans certains autres pays.

ITIL est une marque de The Office of Government Commerce et est enregistrée au bureau américain Patent and Trademark Office.

UNIX est une marque enregistrée de The Open Group aux États-Unis et/ou dans certains autres pays.

Java™ ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Cell Broadband Engine est une marque de Sony Computer Entertainment, Inc. aux États-Unis et/ou dans certains autres pays et est utilisée sous license.

Linear Tape-Open, LTO, le logo LTO, Ultrium et le logo Ultrium sont des marques de HP, IBM Corp. et Quantum aux États-Unis et/ou dans certains autres pays.

Connect Control Center, Connect:Direct, Connect:Enterprise, Gentran, Gentran:Basic, Gentran:Control, Gentran:Director, Gentran:Plus, Gentran:Realtime, Gentran:Server, Gentran:Viewpoint, Sterling Commerce, Sterling Information Broker et Sterling Integrator sont des marques de Sterling Commerce, Inc., une filiale d'IBM Company.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.





Imprimé en France