CFONB
Comité Français d'Organisation et de Normalisation Bancaires

Migration des protocoles ETEBAC vers EBICS et SWIFTNet
FAQ CFONB

Cette FAQ est mise à jour périodiquement en fonction des questions reçues et des documents publiés par le CFONB.
Cette version inclue les réponses aux questions reçues suite à la publication le 12 février 2009 du Guide de mise en œuvre d'EBICS en France. De plus une rubrique EBICS Tests a été crée.

.-.-.-.-.

Plan de la FAQ

.-.-.-.

1. La migration des protocoles ETEBAC vers EBICS et SWIFTNet

N°	Questions	Réponse
1	Qu'est-ce qu'ETEBAC ?	ETEBAC (**E**changes **T**élématiques **E**ntre **BA**nques et **C**lients) est le nom du protocole d'échange de fichiers entre clients et banques défini par le CFONB. Les banques françaises offrant des services de paiement proposent généralement ETEBAC à leurs clients.
2	A quoi sert ETEBAC?	ETEBAC est un protocole de communication qui définit les modalités de transferts des fichiers : - D'ordres remis par les clients (virements fournisseurs, virements de salaires, prélèvements, LCR,..) - D'informations transmises par les banques aux clients (fichiers d'extrait de comptes, de rejets de paiements,..).
3	Qui est concerné par ce protocole ?	ETEBAC s'adresse particulièrement aux entreprises, administrations, associations,.. qui échangent des fichiers avec leurs banques.
4	Quelles sont les différences entre ETEBAC 3 et ETEBAC 5 ?	ETEBAC 3 le protocole le plus répandu, il ne dispose pas de la signature électronique jointe aux données du fichier, et ceci contrairement à ETEBAC 5 (pour plus de détail voir §4)
5	Pourquoi faut-il remplacer les protocoles ETEBAC ?	Définis à partir de 1984, ces protocoles de transmission deviennent obsolètes à l'ère d'Internet. France-Télécom a annoncé la clôture en 2011 du réseau de transport à l'ancienne norme X25 sur lequel reposent les protocoles ETEBAC.
6	Quels ont été les critères de choix ?	Le CFONB a rédigé une expression de besoins et recherché des solutions qui soient à l'état de l'art, sécurisées, s'appuyant sur des outils standards, disponibles sur le marché, d'un accès libre/public et ouvertes sur l'Europe. Ainsi, l'option de définir un protocole purement français pour remplacer les ETEBAC n'a pas été retenue.
7	Quels sont les solutions retenues par le CFONB ?	Le CFONB a retenu 2 solutions : . le protocole EBICS spécifié en Allemagne par le ZKA, . les solutions SWIFTNet proposées par SWIFT.

N°	Questions	Réponse
8	Les acteurs ont-ils été impliqués ?	Les banques qui sont en relations permanentes avec leurs clients et les éditeurs qui proposent des progiciels ETEBAC, ont participé aux groupes de travail du CFONB en charge du choix de remplacement d'ETEBAC. Le CFONB a organisé plusieurs réunions d'informations ouvertes aux éditeurs, entreprises, Administrations,…
9	Chaque banque doit-elle développer les 2 solutions ?	Non, à chaque banque de positionner ses offres pour son marché. Les 2 solutions recommandées par le CFONB constituent l'offre multi-bancaire. Les clients choisiront la solution la plus adaptée à leurs besoins.
10	Les formats actuels CFONB sont ils supportés par EBICS et SWIFTNet ?	Oui, tous les types de fichiers sont supportés dont les formats actuels (Virements Ordinaires, LCR, extraits de comptes,..).
11	Il existe un contrat type ETEBAC5. Quid avec EBICS et SWIFTNet ?	Le CFONB travaille sur des contrats types EBICS en liaison avec le Groupe national des Utilisateurs de SWIFT en France.
12	EBICS et SWIFTNet seront-ils disponibles hors France métropolitaine : Monaco, DOM, TOM	Ces solutions peuvent être mises à disposition par les banques en fonction de leur offre dans toute la France, DOM/TOM inclus, ainsi qu'à Monaco.

2. SWIFTNet généralités

N°	Questions	Réponse
1	Qu'est ce que SWIFTNet ?	La société SWIFT propose des solutions de la famille SwiftNet qui sont déjà utilisées par les grandes entreprises à caractère multinational pour communiquer avec leurs banques. En complément elle a récemment élaboré une solution légère susceptible de répondre plus spécifiquement aux besoins d'entreprises de taille plus réduite (SWIFTNet Lite)
2	Comment obtenir des informations sur les solutions SWIFTNet ?	Pour en savoir plus (documentation, plus d'information, mise en œuvre…) contacter : ➢ Votre banque si vous êtes un client, ➢ ou SWIFT si vous êtes un éditeur André Casterman responsable du bureau de Paris (01 53 43 23 42: andre.casterman@swift.com)

3. EBICS

3.1. EBICS généralités

N°	Questions	Réponse
1	Qu'est ce qu'EBICS ?	La solution EBICS (Electronic Banking Internet Communication Standard) repose sur un protocole de communication sécurisé permettant l'échange de fichiers entre des clients et des établissements bancaires. EBICS a été conçu par le ZKA. Le CFONB va préciser les modalités d'utilisation pour la communauté française dans un « Guide de mise œuvre ». Ses modalités de fonctionnement et de distribution sont analogues à celles d'ETEBAC.
2	A qui s'adresser pour mettre en œuvre EBICS ?	Il convient de s'adresser aux fournisseurs de solution de communication bancaire.
3	Quel est l'intérêt d'EBICS par rapport à ETEBAC ?	EBICS répond aux critères définis : il est basé sur les technologies Internet (IP). Déployé en Allemagne dans une version non compatible (version 2.3) l'accord de coopération signé permet de le déployer en France en version 2.4 et ultérieurement dans d'autres pays qui souhaiteront l'adopter.
4	En plus de la France et de l'Allemagne, d'autres pays pourront-ils utiliser EBICS ?	L'accord de coopération a prévu la possibilité d'ouverture à d'autres pays.
5	Où en est le déploiement d'EBICS en Allemagne ?	La version 2.3 d'EBICS est proposée par l'ensemble des banques allemandes depuis janvier 2008.
6	Quelle est la version commune d'EBICS en Allemagne et en France ?	La version 2.4 d'EBICS est la version commune.
7	A partir de quand sera déployée cette version commune ?	Il est prévu un délai d'un an entre la publication des spécifications et la commercialisation des offres bancaires, soit novembre 2009.
8	Quel est le planning EBICS en France ? 1. Phases de tests entre éditeurs et banques 2. Pilotes entre clients en banques 3. Début du déploiement de masse	Le déploiement d'EBICS en France se déroulera en phases successives, la première visant à remplacer les postes fonctionnant sous ETEBAC 3. Pour cette phase 1, les dates visées sont : 1. Tests à partir du printemps 2009 2. Pilotes en été 2009 3. Novembre 2009 La phase suivante du déploiement concernera le remplacement d'ETEBAC 5.
9	Quand les banques seront-elles prêtes et comment savoir celles qui sont prêtes?	Le déploiement de masse débutera à partir de novembre 2009. Le CFONB ne publiera pas de liste de banques prêtes.
10	Peut-on utiliser le même poste client EBICS pour travailler avec des banques en France et en Allemagne ?	Oui avec le logiciel EBICS version 2.4 et sous réserve du respect des règles d'implémentation de chaque pays.
11	Quelles sont les différences entre les modalités d'utilisation en France et en Allemagne ?	Se reporter aux guides d'implémentation dans chaque pays.
12	Quand pensez-vous pouvoir mettre à disposition le guide d'implémentation d'EBICS pour la phase 2 ?	Le CFONB va lancer les travaux relatifs à la phase 2 et communiquera aux acteurs concernés le guide d'implémentation d'EBICS pour cette phase aussi vite que possible

3.2. EBICS : tests

N°	Questions	Réponse
1	Quel support le CFONB propose-t-il pour les tests ?	Le CFONB va publier un document de cadrage des tests incluant des scénarii de tests. Il n'y aura pas de certification des logiciels par le CFONB. Pour les modalités de tests/pilotes prendre contact avec votre banque.
2	Le CFONB publiera t il pour les éditeurs de logiciels une liste complète avec les contacts appropriés pour la mise en place du protocole EBICS et/ou SWIFTNet.	Le CFONB ne gère pas de liste de contact de banque ni pour EBICS ni pour SWIFTNet. Nous vous conseillons de prendre contact à votre banque ou avec la/les banque(s) de vos clients pour planifier des tests.
3	Savez-vous quand le document de cadrage des tests incluant des scénarii de tests sera disponible ?	Le document de cadrage incluant des scénarii de tests devrait être mis à disposition sur le site du CFONB début mai2009.

3.3. EBICS : aspects techniques

N°	Questions	Réponse
1	Peut-on utiliser EBICS hors Internet ?	Ce n'est pas la recommandation CFONB.
2	Certaines banques utilisent la notion d'indices chronologiques avancés : récupération du relevé mensuel du mois précédent, récupération du dernier relevé bimensuel, récupération du dernier relevé décadaire. Par exemple : pour le relevé bimensuel, selon le jour où le relevé est requêté, soit le fichier envoyé est du 1er au 15eme jour ouvré du mois (date de requête supérieure au 16eme jour du mois) , soit ce sera un relevé du 16éme au dernier jour ouvré du dernier mois si la date de la requête est avant le 15eme jour du mois. A-t-on moyen de récupérer via EBICS ce type de relevés ? Y a-t-il une zone libre ou on pourrait renseigner le type de relevé souhaité du client si les paramètres de date en plus de l'Order type FDL ne suffisent pas ?	Ce besoin peut être couvert via l'utilisation d'extension propriétaire dans le nom du fichier utilisé dans le Request/Type. La méthode décrite et recommandée pour nommer les fichiers permet de couvrir les besoins relatifs aux services spécifiques offerts par les banques. Ce type de paramétrage spécifique à un établissement doit être indiqué dans les annexes du contrat d'abonnement. La version V1.1 des IG reprend ce point.

N°	Questions	Réponse
3	Dans le guide de la mise en œuvre d'EBICS en France, il y a une référence à la création du Payment Status Report. Ce document doit-il être généré pour chaque transaction effectuée par le client ?	L'utilisation du format PSR n'est pas obligatoire, mais recommandée, en effet le PTK (OrderType du Kunden Protokoll) est également possible. Dans le cas où le PSR est utilisé, il doit être géré pour chaque transaction EBICS (ficher envoyé) de manière obligatoire en cas d'échec. La version V1.1 des IG reprend ce point.
4	Dans le cas ou le client effectue plusieurs échanges avant de faire la demande de PSR comment doit être généré ce fichier ? Concaténation technique de plusieurs fichiers XML ? Dans ce cas, le fichier ne pourra pas être parsé par un parseur XML (présence de plusieurs header XML dans le même fichier ? Génération d'un fichier XML parsable contenant le résultat de plusieurs envois ? Envoi du dernier fichier généré ?	Dans ce cas, le fichier ne pourra pas être déparsé, il devra être découpé en fichier XML unitaire par le poste client avant d'utiliser le parseur. La version V1.1 des IG reprend ce point.
5	Concernant la phase de test, les spécifications ne sont pas claires sur le mode d'implémentation. S'agit-il d'un paramètre des Ordertype FUL/FDL? Dans ce cas, quelle est la syntaxe précise?	L'indication « test » doit figurer dans les balises «OrderParam » sur le modèle suivant : <FULOrderParams> <Parameter> <Name>TEST</Name> <Value>TRUE</Value> </Parameter> <FileFormat CountryCode="FR">pain.xxx.cfonb160.dct</FileFormat> </FULOrderParams>
6		

3.4. EBICS : sécurité

N°	Questions	Réponse
1	La sécurité des transmissions sera-t-elle assurée ?	Bien sûr ceci est une préoccupation constante des banques et était un des critères de choix.
2	Qu'est que la signature de transport ?	Une signature de transport assure l'authentification des parties, le chiffrement et l'intégrité des données échangées. La signature de transport n'est pas une signature personnelle distribuée par les différentes AC du marché. Pour EBICS, la signature de transport fait partie intégrante du protocole.
3	Comment sera mise en œuvre la signature de transport sous EBICS ?	Se reporter au « Guide de mise œuvre ».
4	Qu'est ce que l'ordre d'exécution ?	L'ordre d'exécution est une signature personnelle qui apporte la non-répudiation des ordres transmis. Il vient en complément de la signature de transport. Il peut être jointe aux données du fichier (type ETEBAC 5) ou disjointe par un autre canal (type ETEBAC 3), en fonction des offres de chaque banque.
5	Comment la signature électronique est elle proposée sous EBICS ?	La signature électronique sera proposée au moyen de certificats X509. Les modalités détaillées sont en cours de définition .
6	En France y aura-t-il une multi-acceptance de la signature électronique ou faudra t il acheter un certificat par banque ?	La cible est bien la multi-acceptance. Les modalités détaillées sont en cours de définition (phase 2 du déploiement).
7	La signature électronique en Allemagne sera-t-elle compatible avec celle en France ?	Les Allemands évolueront vers X509 à partir de septembre 2009.
8	Sous EBICS existera t il une gestion de preuve allant jusqu'à l'horodatage des ordres ?	La signature électronique, incluant l'horodatage des remises, permettra d'assurer cette gestion de preuves. Les modalités détaillées sont en cours de définition.
9	Pour l'algorithme de chiffrement, comment choisir entre le DES et l'AES ?	En version A005 et A006, c'est l'algorithme AES qui est retenu. La version V1.1 des IG reprend ce point.
10	La procédure d'échange des lettres d'initialisation en Allemagne ne comprend que 2 lettres : Celle concernant la clé de signature et celle concernant la clé d'authentification et la clé de chiffrement. En France la procédure contient 3 lettres... Est ce obligatoire ?	En France, l'utilisation de trois documents, c'est à dire un document par certificats, est obligatoire. La version V1.1 des IG reprend ce point.

N°	Questions	Réponse
11	Le contrôle de signature d'un fichier de remise d'ordres doit-il être fait pendant ou après la transaction Ebics.	C'est au serveur de choisir son mode de fonctionnement : mode synchrone (pendant la transaction EBICS le serveur vérifie la signature et renvoie une erreur dans la trame de réponse à la réception de ce dernier segment.) ou en asynchrone (après la fin de la transaction). Si le serveur fonctionne en mode asynchrone, en cas d'erreur, il devra produire un PSR ou PTK en mode asynchrone. La version V1.1 des IG reprend ce point.
12	Comment est calculée la signature du A006 ? Il semble que la signature n'est pas calculée sur le message lui-même ; donc explicitement Si(Hash(M)) ; mais sur le hash du message ; donc explicitement Si(Hash(Hash(M)).	Avec A006, il y a un double calcul de hash[1], la signature n'est pas calculée sur le message lui-même ; donc explicitement Si(Hash(M)) ; mais sur le hash du message ; donc explicitement Si(Hash(Hash(M)). L'explication résulte de la mise en place d'EBICS en Allemagne : la carte de signature ZKA avec SECCOS 6 et l'utilisation de la AUT key (le nom de la clef de carte à puce) avec un remplissage PSS (c'est-à-dire. A006) est toujours hashée sur la carte à puce, après avoir soumis la valeur de hash, la valeur de hash est calculée une deuxième fois. Rappel de la spécification 2.4 EBICS, chapitre 15 : "puisque des demandes d'applications bancaires utiliseront pour les calculs de signatures électroniques l'AUT-key et également la DS-key, les conditions spéciales suivantes de SECCOS 6 pour l'utilisation de ces clefs doivent être prises en compte : - Pour l'AUT-key la signature sera calculée en utilisant la commande INTERNAL AUTHENTICATE. Si utilisée avec le remplissage (padding) de PSS [PKSC1], la carte à puce SECCOS calculera toujours une valeur de hash sur les données dans l'exécution de la commande INTERNAL AUTHENTICATE. Puisque l'application calcule habituellement aussi une valeur de hash sur le message réel M avant l'appel à INTERNAL AUTHENTICATE, cette procédure aboutira à un double calcul de la valeur hash ; exemple : la valeur hash (hash (M)) sera calculée. - Pour cette raison, A006 sera définie d'une telle façon qu'une valeur de hash calculée antérieurement sur le message M, sera utilisée comme données pour le mécanisme de signature plutôt que le message M lui-même. "

[1] Voir l'explication des motifs dans la FAQ

N°	Questions	Réponse
13	Pouvez-vous confirmer les caractéristiques KeyUsage des certificats de la banque. En effet, les deux certificats dans le document doivent avoir à la fois le KeyUsage de DigitalSignature et de KeyEncipherment.	En effet, les certificats serveurs sont assimilés à des certificats SSL TLS et donc les KeyUsage de DigitalSignature et les KeyEnciphement sont utilisés en même temps. La version V1.1 des IG reprend ce point.

3.5. EBICS : documentation et référencement

N°	Questions	Réponse
1	Les spécifications EBICS sont en anglais, y aura-t-il une version en français ?	Les spécifications EBICS de base en Anglais ne seront pas réécrites en Français. Le guide de mise en œuvre en France et la FAQ correspondante sont en français.
2	Peut-on poser des questions au CFONB sur la migration ETEBAC ?	Oui, les questions peuvent être envoyées sur l'adresse mail migration-etebac.cfonb@fbf.fr
3	Comment se faire référencer ?	Les modalités de référencement se trouvent sur le site CFONB : www.cfonb.org