Compendium EBICS

Electronic Banking Internet Communication Standard

Version du document :	9
Statut :	Validé
Date :	05/04/2023

Suivi des versions

Nom	Date	Version du document	Remarques
Rolf Münster	01/03/2006	1	Version initiale
[…]			
Michael Lembcke	20/04/2020	7	Section 6.7 : Description ajoutée concernant les notifications en temps réel
			Section 6.8.4 : Remarque ajoutée concernant le document delta traitant sur l'utilisation d'EBICS 3.0 dans le service RT1 en une seule étape et basée sur des messages
			Section 9.5 : Description ajoutée de TRAVIC-Push-Server
Michael Lembcke	28/12/2021	8	Section 1 : Introduction complétée par l'Autriche
			Section 1.2 : ■ Annexe 2 « Specification Notifications en temps réel » ajoutée ■ Figures mises à jour
			Section 2.1 : Cycle de vie crypto EBICS ajouté
			Bibliographie : Documents et versions mis à jour
Michael Lembcke	05/04/2023	9	Section 1 Version pour EBICS 3.0.2 mise à jour
			Section 1.2 : Figure 2 mis à jour
			Section 1.3 : R2P de l'EBA CLEARING ajoutée
			Section 9.1 : Figure 10 mis à jour

Nom	Date	Version du document	Remarques
			Section 9.3 : R2P de l'EBA CLEARING ajoutée
			Section 9.6 : Désignation mise à jour
			Transversal : EBICS 3.0 sans sous-version
			Bibliographie : ■ Documents et versions mis à jour ■ Cycle de vie crypto EBICS ajouté

Sommaire

Préface

À l'occasion du salon CeBIT 2006, le *Zentrale Kreditausschuss* (ZKA), organisme de normalisation bancaire allemand – aujourd'hui la *Deutsche Kreditwirtschaft* (DK, Comité allemand pour le secteur bancaire) – annonçait une extension de l'accord DFÜ (EDI) intitulée EBICS (Electronic Banking Internet Communication Standard). Aujourd'hui, ce standard est non seulement établi sur le marché allemand, mais également en France, en Suisse et en Autriche. EBICS a fait son entrée dans de nombreux autres pays et présente de bonnes chances de devenir le standard européen pour le traitement des opérations de paiement tant dans le secteur des entreprises clientes que dans les transactions interbancaires.

Depuis le 1er janvier 2018, EBICS est obligatoire pour les institutions financières allemandes dans le segment des entreprises clientes et a remplacé l'ancienne variante FTAM depuis le début de l'année 2011. En France, la migration des standards ETEBAC vers EBICS est terminée.

Le 17 juin 2010, la société EBICS SCRL a été fondée à Bruxelles, une société qui s'est donné l'objectif de détenir les droits sur le nom et de faire avancer le standard EBICS. Les membres de l'EBICS SCRL viennent des fédérations bancaires allemandes, regroupées dans la Deutschen Kreditwirtschaft, des institutions financières françaises, représentées par le Comité Français d'Organisation et de Normalisation Bancaire (CFONB), des institutions financières suisses et de la Swiss Infrastructure and Exchange (SIX), ainsi que des instituts de crédit en Autriche représentés par la PSA Payment Services Austria GmbH (PSA).

La version 3.0.2 actuelle de la spécification EBICS représente une étape importante dans l'évolution du standard. Contenant le Business Transaction Format (BTF), cette version met en œuvre une harmonisation des différents formats EBICS qui ont existé au niveau national. D'autres options encore, comme les certificats et la signature électronique disjointe, qui jusqu'ici ont été disponibles uniquement au niveau national, ont été mis à disposition. La version 3.0 est officiellement disponible depuis le 27 novembre 2018. Indépendamment de cette date clé, de différentes dates de mise en œuvre pour les nouvelles versions EBICS et de ses conditions de validités s'appliquent dans les pays EBICS.

En complément des fonctions de base, la « communication sur Internet » dans les opérations des entreprises clientes au sens large, EBICS propose des fonctionnalités telles que la signature électronique disjointe (VEU) ou la signature d'authentification et permet également l'utilisation de certificats. EBICS est également utilisé dans le secteur interbancaire. En ce moment, EBICS est en cours de préparation pour la prise en charge de paiements instantanés, tant au niveau de l'interface client que dans le secteur interbancaire.

Le présent compendium donne au lecteur un aperçu des fonctions d'EBICS. À cette fin, ce document présente d'abord les exigences qui ont été décisives pendant le processus de développement du standard et qui sont à la base des caractéristiques d'EBICS. Ensuite vient une description structurée des fonctionnalités d'EBICS. Un positionnement par rapport aux autres standards comme

FinTS ou SWIFT complétera l'examen d'EBICS. Pour conclure, nous illustrerons la mise en œuvre d'EBICS sur l'exemple de la gamme de produit TRAVIC.

L'objectif de ce compendium est de donner une vision claire de ce que signifie le passage à EBICS pour vous et votre entreprise. Nous avons essayé de vous exposer de manière aussi compréhensible que possible des contextes qui sont toutefois assez complexes. Nous vous souhaitons une bonne lecture !

PPI AG, avril 2023

Version du document 9 du 05/04/2023

1 Introduction

1.1 Exigences à EBICS

La devise « évolution au lieu de révolution » résume à elle seule l'objectif que l'on s'était fixé avec la création du nouveau standard EBICS en 2006. L'harmonisation, l'un des sujets clé de la mise en œuvre de la version 3.0, a été ajoutée, vu que des dialectes se sont créés après la création de la société EBICS conjointement avec la France et la Suisse.

Dès le départ, la spécification EBICS [1], qui entre-temps a été intégrée dans des produits de marché, appliqua le principe de l'évolution ; en effet, malgré toute l'énergie innovatrice des participants, il fallait avant tout conserver un élément indispensable : la capacité multibancaire. Les deux scénarios d'utilisation en Allemagne, en France et en Suisse le montre bien. Il n'est donc pas étonnant que la spécification se concentre concrètement sur le domaine de la communication, sur les fonctionnalités cryptographiques pour la sécurité et sur quelques nouvelles fonctionnalités nécessaires ou particulièrement intéressantes comme la signature électronique disjointe (VEU). Il n'est également pas surprenant qu'en Allemagne EBICS ait toujours été traité sous le couvert légal de l'accord DFÜ (EDI), tout à fait reconnaissable dans la structure de la spécification. La perte ou la simple restriction de la capacité multibancaire aurait été synonyme de fragmentation du marché, ce qui n'aurait pas été dans l'intérêt des instances impliquées, notamment des entreprises clientes.

La spécification EBICS 3.0 [1] est en vigueur depuis le 27 novembre 2018 et a été mise à jour pour la dernière fois en 2022 avec la version 3.0.2. Elle a pour l'objectif d'harmoniser les variantes EBICS existantes des différents pays.

Les caractéristiques du standard EBICS sont les suivantes :

Exigences	Description
Internet	EBICS s'appuie fondamentalement sur les technologies Internet. À l'origine uniquement motivé par le domaine de la communication, cet aspect s'étend à travers la spécification et concerne aussi, outre les standards de communication comme HTTP et TLS, des standards comme XML ou signatures XML.
Sécurité	Aujourd'hui, Internet et le thème de la sécurité sont devenus indissociables. Si la sphère de sécurité des réseaux fermés qui ont utilisé les normes précédentes devait être abandonnée, alors cela doit se faire sans que la sécurité soit compromise. Cela concerne certains aspects de la mise en œuvre, à savoir les structures pare-feu de même que la signature et le chiffrement, mais aussi le fait que, parallèlement à la standardisation, un concept de sécurité a été établi et approuvé.

Exigences	Description
Largeur de bande	Un des principaux avantages devait être le découplage du protocole de communication du réseau physique pour pouvoir profiter de plus de flexibilité et surtout de débits de ligne plus élevés.
Performance et rentabilité	À première vue, on pourrait penser que des aspects comme la performance et les ressources ne sont pas compatibles avec une spécification métier. Mais au deuxième coup d'œil, on s'aperçoit qu'il est décisif pour la mise en œuvre de savoir comment un protocole de communication est structuré car les processus de traitement en dépendent. Le protocole a été conçu pour pouvoir traiter de grandes quantités de données et pour aider à traiter ces données de manière rapide, sûre et économique. Un autre point résulte de l'utilisation de standards dans leur forme originaire. De cette manière, il est possible, dans le domaine des plateformes, de recourir à des produits du marché ou à des composantes largement répandus (par exemple, la compression ZIP), ce qui garantit un traitement optimal et économique.
Technicité	EBICS introduit aussi quelques nouvelles fonctionnalités, la principale étant la signature électronique disjointe (VEU) sur le plan local et temporel. Cette fonctionnalité s'est établie entre-temps auprès des clients allemands via les produits du marché et peut être utilisée sur le plan multibancaire avec EBICS. Avec EBICS 3.0, cette fonction est également disponible comme Electronic Digital Signature (EDS) pour les autres pays.
Migration	La question de la migration est décisive pour l'expansion d'EBICS. Dans de nombreux pays européens, il existe des variantes nationales et presque partout, on souhaite premièrement permettre un fonctionnement parallèle de l'ancien et du nouveau protocole et deuxièmement engendrer aussi peu de dépenses que possible du côté du client et de l'institution. Grâce à l'harmonisation visée par la version EBICS 3.0, le sujet de la migration reçoit une autre dimension.

Exigences	Description
Engagements	Dès le départ, les fédérations bancaires allemandes se sont fixées pour mission de développer le standard EBICS sous le couvert de la DK (et aujourd'hui de la société EBICS). Sur cette base, il fallait aussi prendre des engagements concrets : à partir de quand EBICS serait-il implanté globalement et quand les anciens standards de communication seraient-ils abandonnés ? Cela vaut aussi bien pour l'Allemagne que pour la France.

1.2 Structure de la spécification

En conclusion de cette introduction, voici un aperçu de la structure de la spécification et des autres textes d'accord et de spécification y afférents. Depuis le 27/11/2018, la spécification EBICS V3.0 est en vigueur. Parallèlement, la version précédente 2.5 restera également valable.

Étant donné que ces versions se distinguent non seulement par leur contenu, mais aussi par leur structure, les deux variantes seront discutées ici.

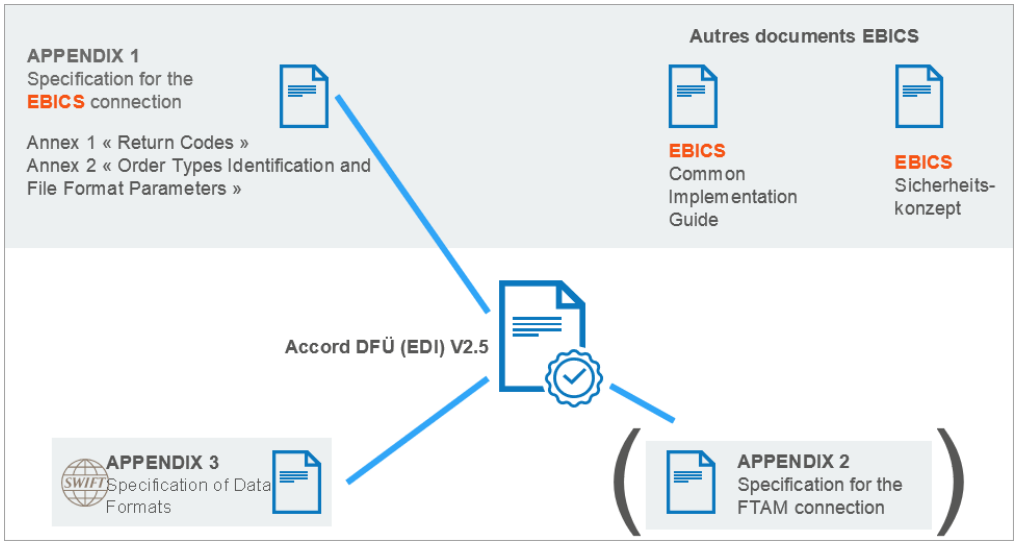


Figure 1 : Structure de la spécification EBICS V2.5 et intégration dans l'accord DFÜ (EDI) allemand

L'annexe 1 « EBICS » et les deux appendices sont rédigés sous l'égide de la société EBICS et publié sur ebics.org. En conséquence, la spécification [1] même est rédigée nativement en anglais et des retraductions en allemand et en français sont effectuées. Ces documents se trouvent sur ebics.de ou cfonb.org.

En plus de la spécification dans l'annexe 1, il est possible de recevoir un « Guide d'implémentation » pour EBICS et en Allemagne [4] – sur demande

auprès du DK – également un concept de sécurité [5]. Avec la version 2.5, les versions allemande et française du guide d'implémentation ont été combinées dans un document commun. Pour la Schweizer Kreditwirtschaft, SIX Payment Services a défini l'utilisation d'EBICS pour la Suisse dans un guide d'implémentation qui est disponible sur six-group.com. En outre, un autre document définit les règles commerciales pour l'utilisation des paiements ISO 20022 en Suisse. Cela permet de répondre aux exigences demandées d'une mise en œuvre et d'une migration facile ainsi qu'une exploitation sûre.

L'annexe 3 de l'accord DFÜ (EDI) à la spécification est consacré aux formats de données [3] SWIFT ou SEPA, restera une standardisation allemande et ne concerne pas les activités EBICS à l'échelle internationale.

L'annexe 2 de la spécification de la procédure FTAM [2] est désormais obsolète et ne figure plus que par soucis d'exhaustivité. Sa place a été prise à partir de 2019 par la nouvelle annexe 2 de la spécification sur les Notifications en temps réel [9].

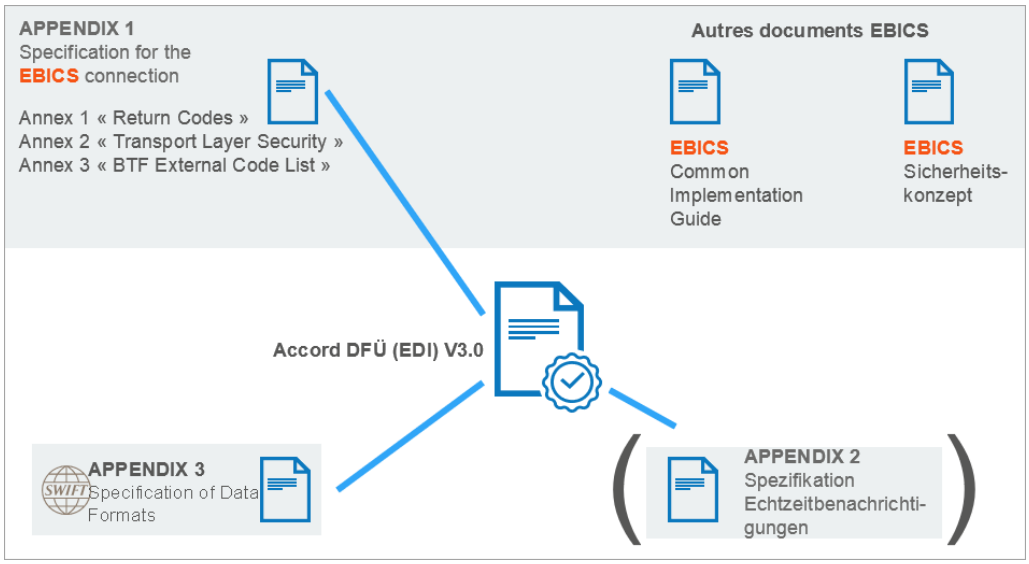


Figure 2 : Structure de la spécification EBICS V3.0 et intégration dans l'accord DFÜ (EDI) allemand

À première vue, la structure de la spécification EBICS version 3.0 ne diffère guère de la version 2.5. Comme prévu, la liste des codes BTF remplace l'ancienne liste des types d'ordre, cependant les listes de référence pour les deux sens sont disponibles sous *ebics.de*.

Une étape majeure constitue l'externalisation de la Transport Layer Security ce qui résulte en une concentration de la spécification EBICS sur des contenus du protocole spécifiques à l'application.

1.3 Documents supplémentaires

En supplément à la spécification EBICS officielle, il existe encore des documents supplémentaires spécifiques se référant à différents cas d'utilisation d'EBICS.

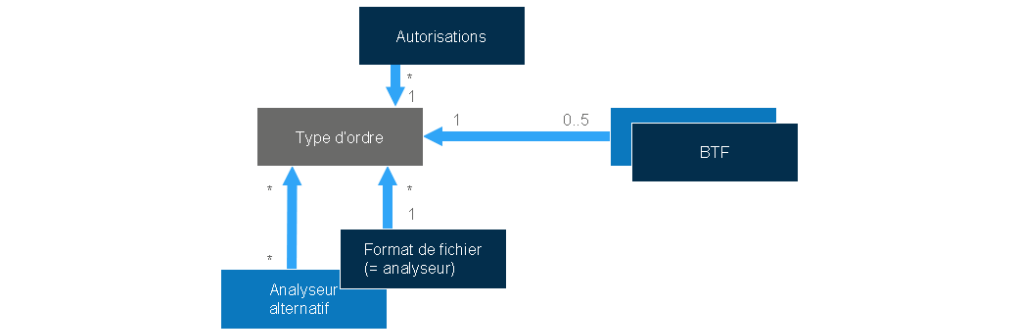
Auteur	Document
Bundesbank	« Accord de transfert de paiement relatif à la communication via EBICS avec les institutions de crédit et les institutions de paiement » ■ Valeur de hachage ■ Empreinte digitale ■ Guide d'implémentation disponible sur Internet
EBA Clearing	EBA STEP2 EBICS Procedural Rules
EBA Clearing	RT1 System – SCT Inst Service Network Interfaces
EBA Clearing	R2P System – Pan-European Request to Pay (R2P) Service
Berlin Group	EBA Cards Clearing (ECC)
Die Deutsche Kreditwirtschaft	Datenaustausch unter Einbindung von Service-Rechenzentren (SRZ) www.die-dk.de
CFONB	EBICS Guide de mise en œuvre en France (Implementation Guideline) : version 2.1.5 www.cfonb.org
SIX Group	Swiss Market Practice Guidelines EBICS 3.0 https://www.six-group.com/dam/download/banking-services/standardization/ebics/market-practice-guidelines-ebics3.0-de.pdf

2 Scénario d'ensemble EBICS

Dans cette section, un scénario complet est présenté à titre d'exemple. Cette approche doit aider à comprendre, comment il est possible de migrer de manière souple et sans interruption une infrastructure existante et stable, tout comme une plateforme Internet déjà établie sur base de produits standards, vers un système ciblé EBICS.

2.1 Interaction entre EBICS 3.0 et ses versions précédentes

La mise en œuvre d'EBICS 3.0 entraîne des exigences aux implémentations, car les clients qui utilisent la version EBICS 2.5 en parallèle doivent être pris en charge pendant la période de transition. L'objectif de la mise en œuvre doit être la couverture complète des exigences, conformément à la spécification EBICS version 3.0, afin d'atteindre en étapes l'harmonisation souhaitée. Cependant, il fallait que les conséquences pour les contrats de clients finaux soient minimes et l'effort de changement soit aussi faible que possible pour les institutions et les fabricants.



Service Nom	Service Scope	Service Option	Service MsgName	Type de conteneur	Type d'ordre
SCC	DE	B2B	pain.008	XML	C2C

Figure 3 : Rapport/mise en correspondance entre BTF et types d'ordre

Les sujets suivants sont importants pour le rapport :

- Uniformité des formats de certificat
- Compatibilité des versions dans un contrat
- Mise en correspondance BTF nationale
- Cas particulier : VEU et indicateur de signature
- Exigence pratique : maintien des interfaces
- Exigences cryptographiques

Uniformité des formats de certificat

Avec EBICS 3.0, X.509 est le seul format de certificat autorisé. Cela signifie qu'au moins la syntaxe X.509 doit être prise en charge dans le cadre du schéma

H005. Du fait qu'il n'existe pas d'infrastructure PKI, les certificats validés par une AC ne seront pas vérifiés par l'AC qui a émis le certificat dans le cas d'un profil DK pendant une période de transition. Indépendamment de ce fait, la date de validité est vérifiée et comparée à la date actuelle au niveau local.

Compatibilité des versions dans un contrat/mise en correspondance BTF

Outre les types d'ordre et formats de fichier connus, BTF est introduit comme nouveau format. Cela signifie pour un institut que des ordres peuvent être remis dans les différentes versions EBICS 2.5 et 3.0 en fonction des installations du client. Une mise en correspondance entre BTF et type d'ordre permet, sous réserve de certaines conditions cadre, d'utiliser la structure d'autorisation existante qui est basée sur un type d'ordre, également pour des ordres BTF, afin d'assurer ainsi la compatibilité.

Cas particulier : VEU et indicateur de signature

Commande VEU

Contrat client	Ordre	VEU
Permis	Permis	Oui
Permis	Non permis	Non
Non permis	Permis	Non
Non permis	Non permis	Non

Indicateur de signature

Configuration du type d'ordre	Ordre	Traitement
Fichier O	Indicateur disponible	Vérification de signature électronique
Fichier O	Indicateur non disponible	Refuser
Uniquement fichier D	Indicateur disponible	Refuser
Uniquement fichier D	Indicateur non disponible	Validation alternative

Figure 4 : Commande VEU et indicateur de signature

La figure montre que le contrat client, l'ordre et l'indicateur de signature influence si un ordre remis ayant une autorisation insuffisante sera refusé ou transféré au traitement VEU.

Exigence pratique : maintien des interfaces

La spécification EBICS 3.0 ouvre la voie à une harmonisation considérable du paysage EBICS européen et augmente ainsi l'attractivité pour d'autres pays à intégrer le standard.

À l'inverse, il vaut veiller à ce que les interfaces aux systèmes d'application soient maintenues lors de l'introduction d'EBICS 3.0 dans les implémentations existantes, afin que l'objectif qui consiste en la migration à faible coûts de ressources soit atteint.

Prise en considération des exigences cryptographiques

Les sections suivantes expliqueront que la transmission vers EBICS 3.0 signifie que certains protocoles cryptographiques ne sont plus pris en charge. Cela concerne la signature d'authentification X001, la procédure de signature A004 et la procédure de chiffrement E001.

L'objectif est aussi d'utiliser que des clés RSA ayant une longueur minimum de 2 048 bits.

Pour l'Allemagne, le DK a publié sur le site www.ebics.de le document « Krypto LifeCycle EBICS » [6]. Ce document définit les directives pour les composants cryptographiques utilisés dans la procédure EBICS en tenant compte des recommandations de l'Office fédéral de la sécurité des technologies de l'information (Bundesamtes für Sicherheit in der Informationstechnik ou BSI). Le document est mis à jour de manière indépendante de la spécification EBICS.

Après cette brève description du rapport entre les différentes versions, les prochaines sections ne traitent que la version actuelle 3.0 d'EBICS.

2.2 Prise en considération des produits

Dès la première lecture, on s'aperçoit que la spécification EBICS n'a pas été conçue de manière improvisée, mais qu'elle décrit de façon optimale les scénarios rencontrés dans la pratique. Cela est dû au fait que la spécification a pu faire ses preuves dans les produits standards disponibles sur le marché, offrant ainsi une preuve de concept. Le point commun de tous ces produits étaient qu'ils présentaient des options pour traiter les paiements de masse pour les entreprises clientes sur les plateformes Internet. De plus, chaque produit a également mis en œuvre ses propres idées en matière d'extensions d'application. De cette manière, le standard EBICS a pu puiser les meilleures solutions dans ce portfolio et éviter les erreurs typiques de débutant. Ceci explique pourquoi, lors de l'introduction d'EBICS, des problèmes tels que la segmentation de grands messages avaient déjà été résolus, ou pourquoi le concept de la signature électronique disjointe était déjà disponible et ne nécessitait pas d'être complété ou optimisé après la phase de déploiement.

2.3 Portails

Depuis quelques années, chaque banque propose dans sa gamme de services des portails professionnels basés sur navigateurs Internet. Du fait qu'EBICS s'appuie également sur une technologie Internet, il est évident que ce protocole de transfert peut bien s'accorder avec un portail web d'entreprise. Cela est le cas tant qu'on communique avec le portail web propre à l'institution.

3 Communication et protection de l'infrastructure

Ce paragraphe se consacre à la pièce maîtresse du standard EBICS : la communication via Internet.

Dans les ouvrages d'introduction à l'Internet sur les protocoles de communication, on cherche toujours à situer le protocole TCP/IP dans le modèle OSI (Open Systems Interconnection) afin d'établir une comparabilité historique. Jusqu'à un certain degré, cette comparaison est possible et justifiée, mais elle est sans intérêt dans le cas du standard EBICS. Cette orientation vers des plateformes Internet est décisive pour l'utilisation des infrastructures disponibles, aussi bien du côté client que du côté banque, et également parce qu'elle fournit un degré de performance bien plus élevé qu'avec les solutions précédentes.

De plus, l'utilisation de la technologie Internet permet à EBICS de se rapprocher d'autres applications. Du fait que les clients-entreprises ont de nombreux champs d'application en dehors des paiements de masse dans le domaine des transactions ou dans l'interface graphique, une interaction avec d'autres services est indispensable comme par exemple le deuxième standard significatif du DK, le FinTS (Financial Transaction Services – en Allemagne [7]). Ce qui est fortement simplifié par l'usage de plateformes communes.

3.1 HTTPS et TLS – Transport Layer Security

Alors que le protocole TCP/IP est dédié par exemple au routage dynamique en cas de défaillance d'une section de ligne, HTTP contrôle la session entre deux partenaires. EBICS n'utilise que la variante sécurisée HTTPS, ce qui se reconnaît, par exemple, à l'affichage d'un cadenas dans le coin inférieur du navigateur. La protection est fournie par le dispositif TLS (Transport Layer Security) qui prend la relève de SSL (Secure Socket Layer).

Le remplacement de SSL par TLS indique un problème de base du raccordement des technologies Internet ayant des standards d'application. Selon une déclaration de l'Office fédéral de la sécurité des technologies de l'information, les versions 1.0 et 1.1 du protocole TLS sont obsolètes et à relever. Jusqu'ici la situation était plutôt inflexible, en raison de l'intégration de ces standards dans la spécification EBICS. Avec l'introduction d'EBICS 3.0, les protocoles de sécurité de la couche de transport ont été transférés dans un propre document, qui peut maintenant être maintenu à l'écart des standards métier.

TLS garantit une transmission sécurisée entre le système client et le premier serveur HTTP ou le serveur Web de l'institution. Actuellement, la version 1.2 est recommandée au minimum. Bien que ce dispositif remplisse cette fonction tout à fait correctement et de manière sûre, cela ne suffisait pas aux responsables du standard EBICS, comme nous le verrons dans une des sections suivantes.

3.2 XML – Extensible Markup Language

Pour faciliter la compréhension des sections suivantes, le langage XML est expliqué dans ce qui suit. Avec BCS, les tâches des comptes-rendus pouvaient

être cachées dans le nom du fichier, mais avec EBICS, une enveloppe de compte-rendu séparée est générée, en raison de la diversité des tâches. Dans le cadre de la technologie Internet, il est judicieux d'utiliser le langage de description des données XML – Extensible Markup Language.

Dans EBICS, chaque requête (request) ou réponse (response) est composée d'un ordre qui est analogue aux types d'ordre définis, ou bien à un conteneur BTF et à une enveloppe XML. Il s'agit donc d'un genre de système hybride, dont le noyau demeure les formats bancaires SEPA ou SWIFT, mais qui est complété par des structures XML. La surcharge d'information engendrée par cette technique est minimale, car il s'agit typiquement de paiements de masse et le fichier de paiement représente un multiple de l'enveloppe XML.

La figure suivante illustre tous les schémas XML définis dans EBICS. Vous les trouverez – conformément au concept namespace XML – aux adresses respectives http://www.ebics.de.

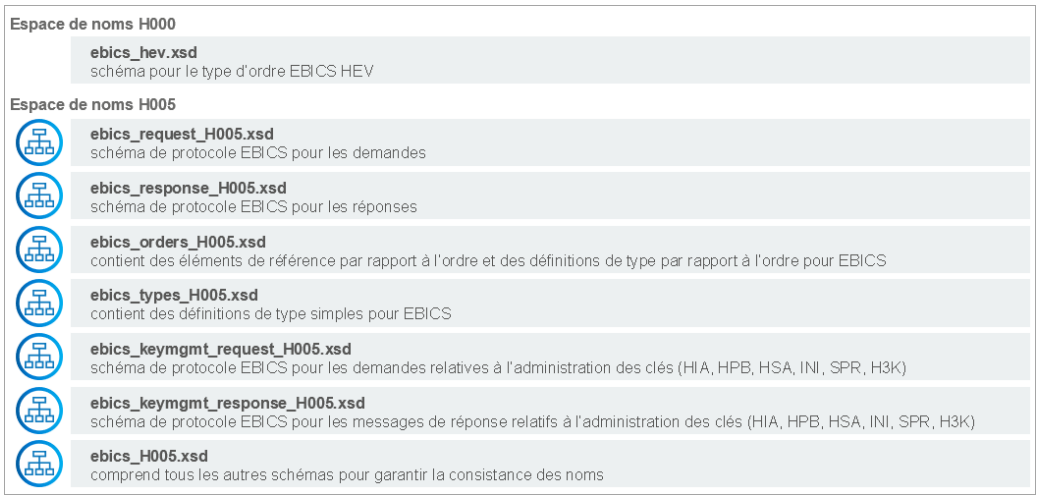


Figure 5 : Schémas XML EBICS V3.0

Vous pouvez constater que les schémas sont structurés de manière claire, et que les définitions de type sont séparées des schémas de comptes-rendus métier.

Le premier schéma présente une particularité. H000 sert à la gestion des versions et permet au produit client de savoir quelles versions de compte-rendu la banque supporte.

Le namespace S001 contenant le schéma de signature EBICS ne figure pas dans la liste. Les versions actuelles des schémas EBICS se trouvent sur les pages officielles ebics.org et ebics.de.

3.3 Optimisation de la communication

Une série d'optimisations dans le domaine de la communication a permis de prendre en compte les propriétés spécifiques à l'Internet.

EBICS permet de comprimer les données de transfert. Pour ce faire, EBICS utilise un algorithme ZIP gratuit et largement répandu.

Afin d'éviter de bloquer les capacités des instances Internet du côté banque, le protocole EBICS offre la possibilité de segmenter de grandes quantités de données.

La capacité optionnelle de récupération de ce protocole permet aussi une reprise intelligente de la transaction lorsqu'un transfert de fichiers a été interrompu. Des segments déjà transmis ne doivent donc pas être doublement envoyés.

Par l'intermédiaire de `Nonce` et `Timestamp`, EBICS met aussi à disposition un procédé qui permet de détecter les doubles remises (replays). Pour cela, un produit client génère une valeur fortuite « Nonce » (valeur « ad hoc ») qui est reprise avec la date/l'heure dans l'enveloppe EBICS. Une liste des valeurs déjà utilisées par le participant pour Nonce et Timestamp est présentée du côté banque, ce qui permet de vérifier le caractère unique d'un ordre.

4 Modèle de données

La section suivante traite spécifiquement le modèle de données utilisé par EBICS. Ce modèle est intégré dans la gestion des données de base des produits utilisés et ne diffère que peu du modèle BCS, comme cela a déjà été mentionné dans les caractéristiques de la migration.

De manière schématique, le modèle de données présente les entités suivantes :

- Client
- Compte
- Participant
- Opération métier

Dans la nomenclature, un `client` constitue le point de départ. C'est le terme générique pour une entreprise qui, d'une part, possède plusieurs comptes dans une banque et qui, d'autre part, autorise l'accès à ces comptes à plusieurs participants.

Un `participant` peut, par exemple, être un employé d'une entreprise qui agit sur ordre du client. Une classe de signature lui est attribuée, déterminant si le participant a le droit d'autoriser des ordres, en agissant seul ou avec d'autres participants.

Les classes de signature suivantes sont prises en charge :

- Classe de signature E Signature unitaire

  Aucune autre signature n'est requise pour l'autorisation de l'ordre.

- Classe de signature A Première signature

  Au moins une autre signature de la catégorie B est requise. La séquence des classes de signature est arbitraire.

- Classe de signature B Seconde signature

  L'ordre doit en plus disposer d'une signature au moins de la classe A. Pour cette raison, la séquence des classes de signature est arbitraire.

- Classe de signature T Signature transport

  Indique qu'il s'agit d'une signature d'authentification, par exemple, d'un participant technique.

Un participant avec classe de signature E, A ou B obtient le droit de signature pour certains comptes de l'entreprise et on lui attribue les types d'ordre pour lesquels il est autorisé.

Ainsi, un système de compétence flexible est créé qui est ensuite reproduit du côté client et du côté banque dans les produits respectifs.

La figure suivante est une représentation simplifiée du modèle de données :

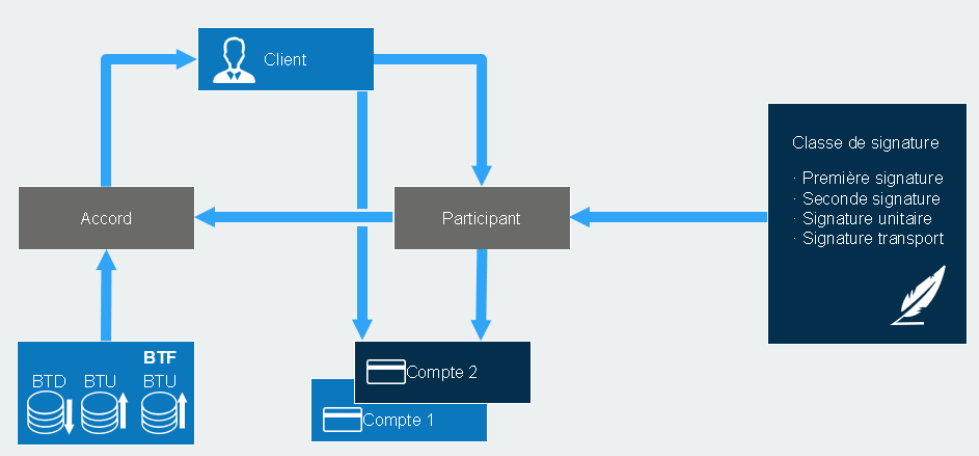


Figure 6 : Modèle de données

Lorsqu'on évoque le modèle de données, il ne faut pas oublier de mentionner les données des paramètres bancaires et les données de l'utilisateur. Toutes les informations concernant l'accès bancaire ainsi que les fonctions optionnelles proposées par la banque sont mentionnées dans les données des paramètres bancaires qui vous sont fournies par le serveur EBICS. Par exemple, on y trouve l'adresse de communication (URL). Les données de l'utilisateur proposées en option par la banque contiennent des informations spécifiques au client et au participant comme les comptes ou les types d'ordres autorisés ou les noms de messages.

5 Sécurité

La version EBICS 2.4 avait déjà introduit de nouvelles procédures de sécurité A005 et A006 ou X002 et E002. Mais plus important encore sont les définitions concernant l'obligation de mettre en place ces procédures – une nouveauté avec l'introduction du standard EBICS.

Les dispositifs de sécurité en soi, comme la carte à puce ou la disquette ou bien la clé USB aujourd'hui, ne sont pas pris en compte. À ce sujet, le standard EBICS ne donne aucune consigne et laisse les clients ou éditeurs des produits client faire leur choix. À l'aide de la classification suivante, le système client peut déterminer le dispositif de sécurité utilisé par le client :

- Aucune indication
- Disquette
- Carte à puce
- Autre dispositif de sécurité
- Dispositif de sécurité non interchangeable

La France pose des exigences particulières au profil TS : le guide d'implémentation impose pour le profil TS l'utilisation de jeton HW spécifiques qui ont été émis par une autorité de certification (AC). Le transfert s'effectue de manière implicite par le biais du certificat X.509 (voir ci-dessous).

5.1 Sécurité de l'infrastructure

Pour obtenir un haut niveau de sécurité de l'infrastructure, EBICS a mis en place un concept global pour la signature et le chiffrement. Avec EBICS, les signatures de client sont obligatoires. Les signatures bancaires sont prévues et seront définies de manière concrète une fois que les questions légales auront été résolues (une signature bancaire se rapportant à des personnes par opposition à un cachet de l'entreprise). De plus, la signature d'authentification X002 est requise.

Au niveau du chiffrement, là aussi, EBICS ne fait pas les choses à moitié : à l'exception du chiffrement impératif avec TLS sur le plan du transport, la procédure de chiffrement propre au standard EBICS ou E002 est obligatoire pour garantir une sécurité de bout en bout.

Dans une étape d'initialisation spéciale, au cours de laquelle des examens préalables optionnels peuvent être effectués, un ID de la transaction est notamment attribué pour l'ensemble de la transaction. Cela permet de créer une parenthèse de transaction, condition préalable à la segmentation lors du transfert de quantités importantes de données.

Ces définitions permettent d'obtenir un degré de sécurité conforme à l'exploitation sur Internet et dont la fiabilité a été analysée et prouvée dans un concept de sécurité correspondant.

Vous trouverez plus de détails sur les propriétés de protocole dans la section *Séquences EBICS* à la page 41.

5.2 Procédures de signature

EBICS connaît deux signatures différentes :

- Signatures d'authentification pour l'identification du remettant
- Signatures pour autoriser un ordre, signature électronique pour l'autorisation bancaire des ordres

Les deux types de signature se distinguent nettement comme vous pouvez le constater dans la figure suivante :

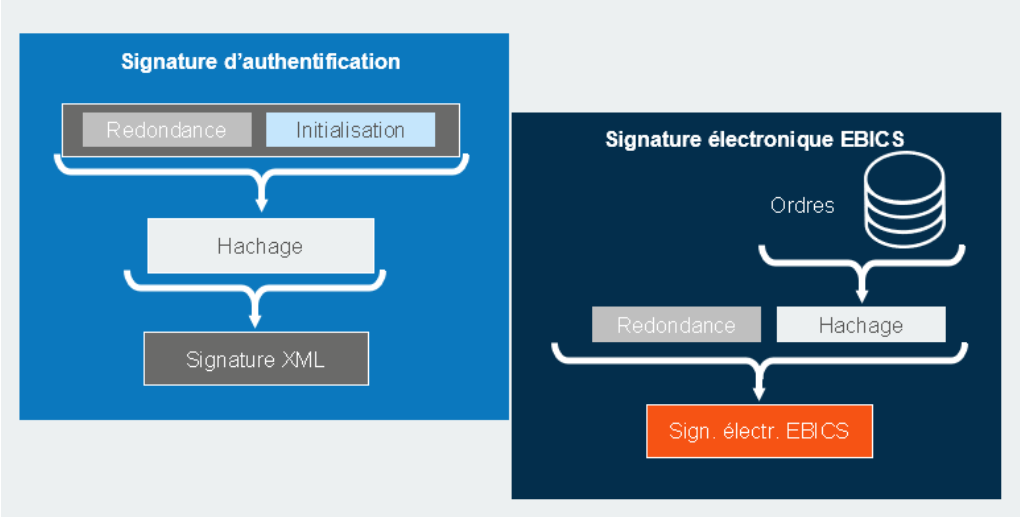


Figure 7 : Procédure de signature EBICS

5.2.1 Signature d'authentification X001 ou X002

La signature d'authentification sert à identifier le remettant sans ambiguïté. La signature d'authentification est vérifiée dans le cadre de l'étape d'initialisation ainsi que dans toute autre étape de la transaction, à savoir avant même que les données de l'ordre ne soient transmises (voir section *Séquences EBICS*, page 41).

Les participants, qui sont exclusivement chargés de la remise des ordres, peuvent avoir la classe de signature T avec laquelle il est également possible de configurer de simples « participants techniques » qui sont uniquement autorisés à remettre des ordres.

La signature d'authentification est créée selon une marche à suivre courante dans le domaine des transactions. Les ordres sont complétés par des informations dynamiques (par exemple, ID de session, heure/date ou informations similaires) qui permettent ainsi d'obtenir différentes signatures correspondant à une situation spéciale avec les mêmes données d'utilisateur. Les spécialistes du chiffrement de données appellent cela la redondance. Une somme de

contrôle chiffrée, la valeur de hachage, est établie sur toute la structure. La principale caractéristique de la valeur de hachage est de générer précisément une valeur avec les données qui sont fournies ; cette valeur ne peut être générée à partir d'aucune autre combinaison de données. Il existe donc une conformité parfaite entre les données et la valeur de hachage.

Sur la base de cette valeur de hachage et à l'aide d'une clé de signature, une signature numérique est créée. Pour être précis, il faut mentionner qu'avant la formation de la valeur de hachage, les données sont complétées selon un algorithme prédéfini jusqu'à une longueur minimum déterminée (padding), afin que ce mécanisme fonctionne également pour les petites quantités de données.

Comme ce procédé est courant dans le monde des transactions, il est aussi supporté sous cette forme dans le standard W3C de signature XML. Par conséquent, EBICS prend en charge la signature d'authentification de la même manière que la signature XML comme standard X002 et X001 (obsolète), et à partir d'EBICS 3.0 uniquement X002.

5.2.2 Signatures d'ordre selon A004 ou A005/A006

La signature électronique d'un ordre du côté client (à l'avenir aussi du côté banque) est rendue obligatoire depuis la version EBICS 2.4 par les nouvelles procédures A005 et A006. Contrairement à la génération de la signature d'authentification, les étapes pour la génération de redondance et de valeur de hachage sont ici inversées. L'utilisation de la valeur de hachage du fichier comme « représentant » direct et important des données d'origine permet de créer cette valeur sans redondance directement depuis le fichier d'ordre et peut ainsi être vérifiée de manière directe, quel que soit sa position.

Pour des raisons de migration, EBICS requière la signature RSA selon A004 comme point de départ (les anciennes variantes de signature de l'accord DFÜ (EDI) n'étant pas prises en charge). La version A004 était déjà conçue pour l'utilisation de la carte de signature de la Deutschen Kreditwirtschaft avec SECCOS comme système d'exploitation, mais comme déjà mentionné, l'utilisation de disquettes ou de clés USB était également possible.

Des procédés supportés par SECCOS un profil a été supporté pour A004, composé des algorithmes suivants :

- Signature RSA avec longueurs de clé de 1 024 bits
- Padding selon ISO 9796-2
- Procédure de valeur de hachage RIPEMD160

Aujourd'hui tout à fait courant et depuis EBICS 2.4 rendu obligatoire, les procédures de SE A005 et A006 ont les attributs suivants :

	A005	A006
Longueur de clé	(1 536)–4 096 bits	(1 536)–4 096 bits

	A005	A006
Procédure de valeur de hachage	SHA-256	SHA-256
Procédure de padding	PKCS#1	PSS

Le tableau montre qu'A005 et A006 se distinguent uniquement dans la procédure de padding.

Sur la base de la présentation des protocoles de sécurité et de la référence au système d'exploitation des cartes à puces SECCOS, on pourrait penser que cette partie de la spécification EBICS reste plutôt un standard allemand. Cela n'est pourtant pas le cas. La stratégie de cartes adoptée par la DK, qui respecte strictement les normes du catalogue crypto de l'Office fédéral de la sécurité des technologies de l'information et s'oriente ainsi aux normes européennes pour l'usage de la signature, garantie donc son utilisation au niveau international.

La version EBICS 3.0 impose une longueur de clés d'au moins 2 048 bits. Il est prévu de modifier également les clés A004 existantes.

5.3 Initialisation

Avant de pouvoir utiliser une paire de clé, l'authenticité des partenaires doit d'abord être établie sur la base d'une procédure adaptée. Pour cela, on utilise soit des certificats soit des procédés alternatifs suivants d'autres voies. La prise en charge de certificats selon X.509 est certes prévu par EBICS, mais, actuellement en Allemagne, on utilise la lettre d'initialisation. En France, une infrastructure PKI existait déjà à l'introduction du standard EBICS. Il est possible d'utiliser des certificats dans le cadre de l'initialisation, ce qui est pris en charge par le standard depuis la version 2.5 d'EBICS.

Les deux concepts seront présentés dans les sections suivantes, donnant la possibilité de mixer les deux concepts, comme le montre le scénario de repli utilisé en France.

5.3.1 Certificats en France

Une politique de sécurité appropriée constitue la base d'une procédure basée sur des certificats. Cela signifie, qu'il faut définir dans quelle mesure les émetteurs de certificats peuvent être considérés comme sécurisés. En France, il existe des définitions claires et publiées pour l'utilisation des certificats dans EBICS. Le niveau le plus élevé est représenté par les émetteurs de certificats qualifiés selon la directive européenne sur la signature électronique. En France, il est également possible d'échanger des fichiers de paiements à un degré de sécurité moins élevé comme expliqué ci-après.

En France, les classes de signature utilisées sont T et E. Pour le moment, la signature électronique disjointe n'est pas supportée. Au lieu de cela, il existe deux profils pour la remise (T) et l'autorisation (E).

Pour la remise de certificats, il est possible d'utiliser le nouveau type d'ordre H3K, disponible à partir de la version 2.5. Le reste des processus d'initialisation d'un client n'a pas été modifié.

- Profil de remettant T sur base de certificats déjà à partir d'EBICS 2.4

  Il n'est pas impératif que l'initialisation se fasse par une autorité de certification (AC) listée. Il est également possible d'utiliser des certificats auto-signés par la banque avec lettre INI.

  Cependant, si le certificat a été délivré par une autorité de certification, celui-ci doit faire partie d'une liste de confiance.

- Profil d'autorisation TS

  On utilise dans ce cas les signatures électroniques pour le transport et la signature. La procédure correspond en gros au standard ETEBAC-5. Dans ce cas, le certificat pour la clé de signature doit être délivré et signé par une autorité de certification et également faire partie d'une liste de confiance. Les certificats pour les clés d'authentification et de chiffrement peuvent également être auto-signés.

  La vérification du certificat est obligatoire pour la clé de signature, pour les certificats pour les clés d'authentification et de chiffrement, la vérification se fait par une AC, si les certificats ont été délivrés par une AC.

- Lettre INI comme scénario de repli

  En France, l'utilisation de certificats n'exclue pas pour autant l'envoi de lettres INI pendant le processus d'initialisation. Indépendamment de l'utilisation de certificats, le client doit au départ envoyer une lettre INI.

  Les certificats qui ne sont pas délivrés par une AC ne sont activés que par lettre INI. Les certificats délivrés par une AC doivent toujours être vérifiés par une AC. Quand la vérification du certificat par l'AC est positive, les données du certificat doivent également être comparées aux indications transmises par le remettant. Si des différences sont constatées, l'activation manuelle peut toujours se faire sur la base d'une lettre INI.

Après vérification et activation réussite, le certificat du client est sauvegardé dans le système de l'application. Les futures demandes de blocage seront effectuées sur cette base – le client n'a besoin de remettre le certificat qu'une seule fois.

Indépendamment des profils d'autorisation et de remise courants en France, l'introduction d'EBICS 3.0 engendre l'utilisation du format de certificat pour clés. Cependant, l'application restera dans un premier temps différent de manière à ce que l'effet d'harmonisation ne se manifeste pas.

5.3.2 Lettre INI en Allemagne

Lors de la procédure de validation par lettre INI, un participant génère une paire de clés et communique à la banque sa clé publique avec le type d'ordres INI (ou HIA s'il s'agit d'une clé publique pour la signature d'authentification ou pour le chiffrement). Parallèlement à cela, une lettre d'initialisation est imprimée,

contenant les données administratives, la clé publique et la valeur de hachage correspondante. Cette lettre d'initialisation est signée manuellement par le participant, puis envoyée par courrier ou par fax à la banque avant d'être comparée avec les données transmises par voie électronique. Lorsque les données sont identiques, la clé est activée et peut être alors utilisée par le participant. Le même procédé peut être exécuté dans le sens inverse si la signature de la banque est introduite à une date ultérieure. Le participant a donc pour mission de comparer les données de clé transmises par voie électronique et postale et de confirmer qu'elles sont identiques.

5.4 Procédure de chiffrement

EBICS utilise un double chiffrement selon TLS ainsi que le chiffrement EBICS actuel E002 (E001 est l'ancienne version) afin de permettre à la fois un chiffrement standard dans HTTPS et un chiffrement de bout en bout. À partir de 2009, le procédé AES recommandé par BSI sera introduit pour E002.

5.4.1 TLS – Transport Layer Security

TLS est le successeur de SSL. Ces deux protocoles de chiffrement ont pour caractéristique de garantir à la fois l'authentification et le chiffrement sur une voie de transport. Des implémentations correspondantes se font du côté client dans le navigateur Internet, par exemple, et du côté banque dans les serveurs Web courants.

Lorsqu'une connexion TLS est établie, les partenaires échangent certificats et procédés pris en charge, ce qui sert alors de base à la création d'une session.

Selon un principe communément admis, EBICS utilise uniquement l'authentification de serveur à partir de TLS et ne prend en charge actuellement aucun certificat de client TLS. Les certificats Internet employés généralement par les banques sont utilisés comme certificats de serveur (qui sont, par exemple, certifiés par VeriSign).

Le chiffrement a lieu dans les deux sens. Seules les procédures de chiffrement puissantes ou suites de chiffrement sont prises en charge. Les suites de chiffrement valables peuvent être consultées sur le site Web de la Bundesbank allemande et sous ebics.de.

Ici, encore, l'information que la Transport Layer Security a été écartée dans un propre document avec la nouvelle version d'EBICS 3.0.

5.4.2 Chiffrement E001 et E002

Pour le chiffrement E001/E002, il s'agit d'une procédure hybride ainsi nommée car elle est composée d'algorithmes asymétriques et symétriques. Le principe de base consiste à utiliser une clé RSA asymétrique en tant que clé de chiffrement. Pour des raisons de performance, le message même est crypté symétriquement. Comme clé, on utilise une clé dynamique qui est échangée (sécurisée avec la clé de chiffrement).

E001 utilise une clé de chiffrement longue de 1 024 bits et l'algorithme Padding PKCS#1. La prise en charge d'E001 dans les implémentations sera supprimée au plus tard avec l'introduction d'EBICS 3.0. L'introduction d'EBICS 3.0 et la version précédente V2.5 a pour conséquences qu'EBICS 2.4 devient obsolète et également E001, X001 et A004.

Avec EBICS 2.4, E002 a été introduit comme évolution. C'est ici que s'effectue le passage de triple DES à AES (recommandation de BSI depuis 2009).

6 Fonctions métier d'EBICS

EBICS ouvre aux clients de nouveaux champs d'application.

6.1 Types d'ordres

L'accord DFÜ (EDI) pour l'Allemagne, les lignes directrices d'implémentation pour la Suisse, ainsi que les standards de formats du CFONB en France supporteront avec EBICS, entre autres, les domaines d'application suivantes par le biais des types d'ordre opératifs et des paramètres FileFormat ou bien à partir de la version EBICS 3.0 harmonisé par le biais des spécifications BTF concernées :

- Opérations de paiement SEPA et autres opérations de paiement nationaux
- Opérations de paiement internationales
- Opérations sur valeurs mobilières
- Opérations accréditives
- Les informations de relevé de compte journalier et d'autres informations pour les écritures comptabilisées et les avis des opérations de compte (entre autres dans les formats MT940/MT942 ou camt XML)

De nouveaux types d'ordre pour BTF sont en plus introduits avec la version EBICS 3.0 :

- BTD : type d'ordre administratif pour télécharger un fichier qui est plus caractérisé par une structure BTF
- BTU : type d'ordre administratif pour envoyer un fichier qui est plus caractérisé par une structure BTF

6.1.1 Paiements SEPA

EBICS prend en charge des types d'ordres et aussi des paramètres FileFormat pour les paiements SEPA client-institution financière et institution financière-institution financière (Bundesbank allemande et interbanque STEP2). Voici les messages SEPA qui sont pris en charge actuellement pour l'interface client-institution financière :

- SEPA Credit Transfer Initiation
- SEPA Direct Debit Initiation
- Restitution avant règlement (Rejects)

Ces messages se reflètent dans les types d'ordres EBICS correspondants, bien que la particularité suivante doive aussi être prise en compte.

Lors de la conversion des messages SEPA pour le DK, on a constaté l'utilité d'introduire, en plus du format SEPA, des formats élargis pouvant être utilisés en fonction de l'institution financière ou du cas d'application. Plus précisément, il s'agit d'ordres collectifs avec plusieurs formations de groupe, par exemple, des comptes du donneur d'ordres ou des données d'exécution qui peuvent être

Version du document 9 du 05/04/2023

traitées différemment (exemple, le traitement de plusieurs comptes de donneur d'ordres) :

- Format standard SEPA

  Utilisation du format standard SEPA avec une restriction : seuls les ordres pour un compte de donneur d'ordre sont possibles. Pour pouvoir exécuter les ordres de plusieurs comptes de donneur d'ordres avec cette option, il faut remettre plusieurs ordres dans le format standard SEPA.

- Container SEPA

  Élargissement du protocole conformément aux normes de la DK pour permettre la remise de plusieurs formats SEPA pour plusieurs comptes de donneur d'ordres dans le cadre d'un type d'ordres

- Options de groupage élargies

  Format standard SEPA pour lequel, en profitant des options de groupage élargies dans le format SEPA, il est possible de remettre des ordres pour plusieurs comptes de donneur d'ordre

Cette répartition sur plusieurs variantes se justifie par le mode de traitement optimisé des différentes sociétés de service en informatique.

Quelques-uns des types d'ordres SEPA utilisés en Allemagne sont énumérés dans le tableau suivant en tenant compte de certaines variantes :

Option	Type d'ordre EBICS 2.x	Dénomination SEPA
Formats des données SEPA	CRZ	Payment Status Report for Credit Transfer
	CDZ	Payment Status Report for Direct Debit
Container	CCC	Credit Transfer Initiation
	CRC	Payment Status Report for Credit Transfer
	CDC	Direct Debit Initiation
	CBC	Payment Status Report for Direct Debit
Option de groupage élargie	CCT	Credit Transfer Initiation
	CDD	Direct Debit Initiation

En plus des types d'ordres SEPA mentionnés, d'autres types d'ordres ont été développés avec des caractéristiques différentes de format pour traiter les opérations métier spécifiques de la Deutschen Kreditwirtschaft. Il s'agit notamment des types d'ordres pour le traitement de la procédure prestataires nationale.

Pour être tout à fait complet à ce sujet, il faut ajouter que pour la transmission des données SEPA dans le cadre des relevés de compte quotidiens SWIFT avec le type d'ordre STA, les formats SWIFT MT940 et MT942 ont été adaptés.

Pour reproduire les opérations de paiement des ordres SEPA sans perte, de nouveaux types d'ordres de téléchargement pour les formats camt (C52, C53 et C54) ont été introduits comme équivalent aux messages MT94x (STA et VMK) et les informations sur le chiffre d'affaires DTAUS (DTI).

Pour obtenir plus de détails sur les formats de données SEPA et leur utilisation en Allemagne, veuillez consulter l'annexe 3 de l'accord DFÜ (EDI).

Selon le pays, de différents formats de paiement nationaux sont utilisés en dehors de SEPA, ayant des types d'ordre et paramètres FileFormat définis à cet effet.

6.1.2 ISO 20022

Le standard *ISO 20022: Financial Services – Universal financial industry message scheme*, à la fois libre et ouvert, joue un rôle significatif dans les transactions financières électroniques d'aujourd'hui à l'échelle internationale. L'objectif de ce standard est la simplification est l'harmonisation de la communication globale au sein du secteur financier. Les sujets de la standardisation sont, entre autres, la terminologie, les processus et les formats de messages. Cela sert à permettre un échange à l'échelle mondiale des informations financières entre les systèmes. Les messages échangés entre le client et la banque ou bien entre la banque et la banque se présentent dans un document XML (Extensible Markup Language).[1] Cette manière de présentation constitue une différence aux anciens formats, comme le format DTA.

Grâce à l'ISO 20022, une importante quantité de types de message a été standardisée (à trouver sous : https://www.iso20022.org/iso-20022-message-definitions). Pour chaque type, il existe une spécification formelle des éléments et structures disponibles sous format de fichier de schéma XML. Afin de permettre une identification sans ambiguïté, chaque type dispose d'un Identifier (identifiant) ou bien d'un nom. Les descriptions des messages contiennent de plus une version de manière à ce que des versions divergentes de la description de message, qui est à la base de la version, puissent être distinguées. Chaque type de message peut représenter un ou plusieurs opérations métier (par exemple la remise d'un virement SEPA).

Les messages importants pour la communication client-institution financière sont décrits dans ce qui suit :

Nom	Message
pain.001	Virements

[1] Voir aussi ISO 20022 : https://www.iso20022.org/ comme page d'accueil et pour un aperçu d'informations par exemple le site https://www.iso20022.org/faq.page

Nom	Message
pain.002	Rapports de statut
pain.008	Prélèvements
pain.007	Retour de client (customer to bank payment reversal)
camt.052	Écritures de compte intraday
camt.053	Relevés de compte journaliers
camt.054	Informations de comptabilisation
camt.029	Information concernant l'annulation/retour (Resolution of investigation)
camt.055	Annulation par client (customer payment cancellation request)

Des messages pour la communication interbancaire sont également disponibles (par exemples des messages pacs). Les messages ISO 20022 sont également utilisés pour les paiements instantanés.

En raison de la norme ISO 20022, il existe une forme de description harmonisée pour l'échange de messages dans le secteur financier. La quantité d'élément disponible au total par message est décrite à ce niveau global.

En raison de limitations des spécifications générales et par le biais des règles de remplissage supplémentaires (technique et/ou métier), les organisations peuvent définir leurs propres sous-types des messages ISO 20022 pour certains domaines d'application.

L'une des organisations qui a défini de telles concrétisations et règles supplémentaires est la CGI Group (Common Global Implementation Group). Elle se focalise sur l'échange de message dans les opérations de paiements globaux et transnationaux. Au même temps de divers types d'ordre de paiement peuvent être reproduits. Aucune spécialisation sur les paiements SEPA n'a lieu, par exemple.[2]

Une autre organisation ayant ses propres spécifications pour les messages ISO 20022 est le European Payments Council (EPC).[3] L'EPC publie des lignes directrices d'implémentation spécifiques, expliquant l'application des paiements SEPA par ISO 20022, comme par exemple des virements (ISO 20022

[2] Voir CGI Group/SWIFT : https://www.swift.com/standards/market-practice/common-global-implementation

[3] Voir European Payments Council (EPC) : https://www.europeanpaymentscouncil.eu

dénomination pain.001).[4] Les documents décrivent une limitation des spécifications générales ISO 20022, comme par exemple les éléments autorisés ainsi que les règles supplémentaires à respecter qui sont spécifiques au paiement. De cette manière, le format EPC ne contient que des éléments, qui sont nécessaire pour les paiements SEPA. La description de formats qui concerne, entre autres, les valeurs autorisées n'est disponible que dans une description textuelle pour le format EPC.

Les différents pays, eux-aussi, ont leurs propres variantes ISO 20022. Le DK a défini des prescriptions spécifiques pour l'Allemagne, comme la structure des messages XML conformément à la norme ISO 20022 et les règles à prendre en considération pour les informations transportées. Les différents formats de données et processus sont décrits, les fichiers de schéma XML correspondants sont publiés.[5] Le marché financier en Suisse connaît également de telles spécifications. La SIX (Swiss Infrastructure and Exchange) a publié des spécifications et recommandations de mise en œuvre dans leurs Swiss Payment Standards, pour la réalisation des messages ISO 20022. Ils contiennent des spécifications concrètes, comme la manière dont les ordres de virement peuvent être échangés. Il existe également des spécifications pour les ordres de paiement suisses, comme les prélèvements suisses.[6]

Tant les prescriptions de la DK, que celles de la SIX appliquent de différentes spécifications des prescriptions EPC, mais mettent en œuvre les spécifications ISO 20022 de manière spécifique au pays. Les prescriptions de la DK et de SIX représentent ainsi des concrétisations des prescriptions EPC. Cela concerne en particulier les descriptions des formats qui sont parfois décrit de manière plus détaillée que des composants de schéma XML, au contraire du format EPC. Ce procédé permet de nombreuses vérifications à l'aide du schéma XML (par exemple en ce qui concerne le format DK). Leur point commun est la base ISO 20022 sous forme d'une description XML universelle.

Les prescriptions SIX offrent en plus aux institutions financières la possibilité de créer des variations individuelles, par exemple en fonction du portefeuille de services proposés par l'institution.

En France, il existe en outre un guide d'implémentation, publiée par le CFONB concernant l'utilisation d'ISO 20022 pour, par exemple, les paiements pain.001, [7] (SEPA, non-SEPA,…) ou les prélèvements SEPA pain.008 [8]. Les différentes variantes sont décrites dans les documents.

---

4 Voir European Payments Council (EPC) : https://www.europeanpaymentscouncil.eu/document-library/implementation-guidelines/sepa-credit-transfer-inter-psp-implementation-guidelines

5 Voir DK, SIZ : https://www.ebics.de/de/datenformate

6 Voir SIX : https://www.six-interbank-clearing.com/de/home/standardization/iso-payments/customer-bank/implementation-guidelines.html

7 Voir CFONB : https://www.cfonb.org/index.php/instruments-de-paiement/virement

8 Voir CFONB : https://www.cfonb.org/instruments-de-paiement/prelevement

Partant de la description générale du standard ISO 20022, les différentes variantes deviennent de plus en plus concrètes et spécifiques ou bien restrictives.

Les messages ISO 20022 sont communiqués via EBICS sous forme de transactions d'émission ou de téléchargement (voir section *Séquences EBICS*, page 41). Le message pain.001 (virement) est par exemple envoyé du système client à la banque via EBICS (voir section *Paiements SEPA*, page 27). Il en est de même pour l'ordre de téléchargement du rapport de statut pain.002 qui est également accordé via EBICS (voir section *Paiements SEPA*, page 27).

Selon la variante du standard ISO 20022, les messages pain.002 peuvent contenir des messages positifs et/ou négatifs quant aux ordres de paiement. Cela permet à une institution financière d'utiliser un message pain.002, qui est lisible par machine par le système client traitent, afin de signaler les causes d'erreurs pour le rejet des ordres de virement. Le système client peut prendre en considération ces erreurs, le cas échéant. Les différents codes de statut informent sur le statut de l'ordre complet ou d'une partie d'une transaction individuelle. Peut être traité en partie notamment un ordre de virement, qui est composé de plusieurs transactions individuelles erronées ou sans erreurs. Seules les transactions sans erreurs sont traitées, les transactions erronées seront écartées et signalées au client. Les informations sur les erreurs et la réaction sont ainsi très détaillées et également basées par machine.[9]

6.1.3 Opérations de paiement internationales et informations sur le chiffre d'affaires

L'aperçu suivant montre certains exemples des formats de types d'ordre standardisés et groupés, utilisés en Allemagne et en Suisse :

- AZV Envoyer un ordre AZV au format disquette (DTAZV en Allemagne)
- STA Télécharger des relevés quotidiens SWIFT (SWIFT MT940)
- VMK Télécharger des annonces à court terme (SWIFT MT942)
- VML Télécharger des annonces à long terme (SWIFT MT942)
- C52 Télécharger le Bank-To-Customer Account Report
- C53 Télécharger le Bank-To-Customer Statement Report
- C54 Télécharger le Bank-To-Customer Debit Credit Notification
- ESR Télécharger des informations BVR (spécifique en Suisse)

En Europe, de différents formats nationaux sont en outre utilisés pour le traitement des paiements internationaux. De plus en plus, les formats basés sur ISO 20022 gagneront en importance (par exemple ISO Global, CGI) (voir section *ISO 20022*, page 29).

[9] Par exemple standard DK, voir DK, SIZ : https://www.ebics.de/de/datenformate

6.1.4 Types d'ordre standard pour l'émission (FUL) et le téléchargement (FDL)

Ces types d'ordre sont surtout utilisés en France et servent au transfert transparent de fichiers de quelque format qu'ils soient. Cela a pour conséquences que le nom du type d'ordre n'indiquera plus le format transporté, ce qui est jusqu'ici un procédé courant en Allemagne. Un paramètre de format plus long est ajouté au type d'ordre FUL ou FDL, permettant la commande. Ces types d'ordre sont disponibles depuis la version 2.4 d'EBICS. Le type d'ordre FUL (File Upload - émission de fichier) est destiné à la remise, le type d'ordre FDL (File Download - téléchargement de fichier) est utilisé pour le téléchargement. La structure et les paramètres de format à utiliser, conjointement avec les types d'ordre, sont documentés dans l'annexe à la spécification EBICS.

6.1.5 Autres types d'ordres

En plus des types d'ordre standards, il est possible d'effectuer la classification suivante concernant l'utilisation dans EBICS :

- Types d'ordre déterminés par le système – spécialement pour EBICS
  - Par exemple : types d'ordre en rapport avec la signature électronique disjointe (VEU)
- Autres types d'ordre pris en charge par le système
  - Par exemple HAC, PTK pour le téléchargement de comptes-rendus client
- Types d'ordre réservés pour l'échange de fichiers inter-entreprises
  - Par exemple : envoyer FIN pour EDIFACT-FINPAY
- Autres types d'ordre réservés utilisant des formats non standardisés, par exemple :
  - FTB pour l'envoi/le téléchargement de fichiers quelconques
  - FTD pour l'envoi/le téléchargement de fichiers de texte libre
- Types d'ordre EBICS optionnels
  - Par exemple : HVT pour consulter des détails de transaction VEU

6.2 Business Transaction Format – BTF

BTF est l'abréviation de Business Transaction Format. En raison de l'introduction d'EBICS 3.0, BTF harmonise la description des formats à transférer en Allemagne, en France et en Suisse. Au lieu d'échanger des types d'ordre ou des paramètres de format, la communication avec le serveur bancaire par le biais de BTF prévoit un échange d'une structure qui identifie une opération métier.

Afin d'assurer la compatibilité avec les versions EBICS précédentes, les adaptations des paramètres de format et des types d'ordre pour répondre au standards BTF ont été facilitées par des aperçus d'affectation (mise en correspondance). Les aperçus d'affectation sont définis à l'échelle nationale pour les

types d'ordre et les paramètres de format. Les clients EBICS doivent respecter ces affectations. Pendant la période de transition, il peut y avoir des formes mixtes des versions EBICS prises en charge :

- Côté client

  L'institution financière A prend en charge déjà BTF, tandis que l'institution financière B ne propose qu'EBICS 2.x. Les accès bancaires dans un client EBICS doivent être adaptés à la version concernée du serveur bancaire.

- Côté serveur

  Les employés d'un client utilisent les clients EBICS avec différentes versions. Tandis que le remettant remet un ordre avec une ancienne version via le type d'ordre, un autre employé signe l'ordre dans la VEU avec un client EBICS 3.0 par BTF.

6.3 Signature électronique disjointe (VEU)

La signature électronique disjointe (VEU) est la fonction la plus importante dans EBICS. Sous l'influence des différents produits disponibles sur le marché, cette évolution fit son apparition dans la spécification EBICS.

La signature électronique disjointe permet de séparer la remise d'un ordre, qui est éventuellement déjà porteur d'une première signature, de la validation effective. La remise d'un fichier de signature peut avoir lieu à un autre moment et en un autre endroit que la remise de l'ordre. Un numéro d'ordre ou un ID d'ordre permet d'établir la liaison entre les deux fichiers.

Le procédé se déroule comme suit :

- Un participant remet un ordre de type CCT, par exemple, et il ajoute, le cas échéant, sa propre signature électronique bancaire de catégorie A.
- L'institution financière examine l'ordre et vérifie si d'autres signatures sont requises. Si oui, l'ordre y compris la valeur de hachage est mis en cache du côté banque.
- Un deuxième participant souhaite désormais valider l'ordre et il a obtenu les données requises telles que le numéro d'ordre et la valeur de hachage par un autre moyen (la restitution du numéro d'ordre et de la valeur de hachage est externe à EBICS et ne fait pas partie intégrante des composants du serveur du côté banque).

  Il a désormais les options suivantes :

  - Il consulte avec le type d'ordre HVU ou HVZ la liste d'ordres en attente de sa signature et obtient un aperçu indiquant entre autres le type d'ordre, les signatures portées et manquantes et la longueur de l'ordre non compressé.
  - À partir du type d'ordre HVD, il peut obtenir des détails supplémentaires comme les informations de l'abrégé et la valeur de hachage concernant les ordres.

Cette étape n'a pas lieu lorsque l'aperçu a été téléchargé avec le type d'ordre HVZ, car HZV fournit déjà toutes les informations détaillées nécessaires.

- Le type d'ordre optionnel HVT permet à l'institution de fournir au participant toutes informations, par exemple les transactions individuelles de l'ordre, le motif de paiement et l'intégralité de l'ordre.

- Après l'analyse des ordres existants, le participant a désormais les possibilités suivantes :
  - Signature avec type d'ordre HVE
  - Annulation par HVS

La figure suivante est inspirée de la représentation dans *Specification for the EBICS connection* [1] et donne une vue d'ensemble compréhensible de cas d'utilisation pourtant assez complexes :

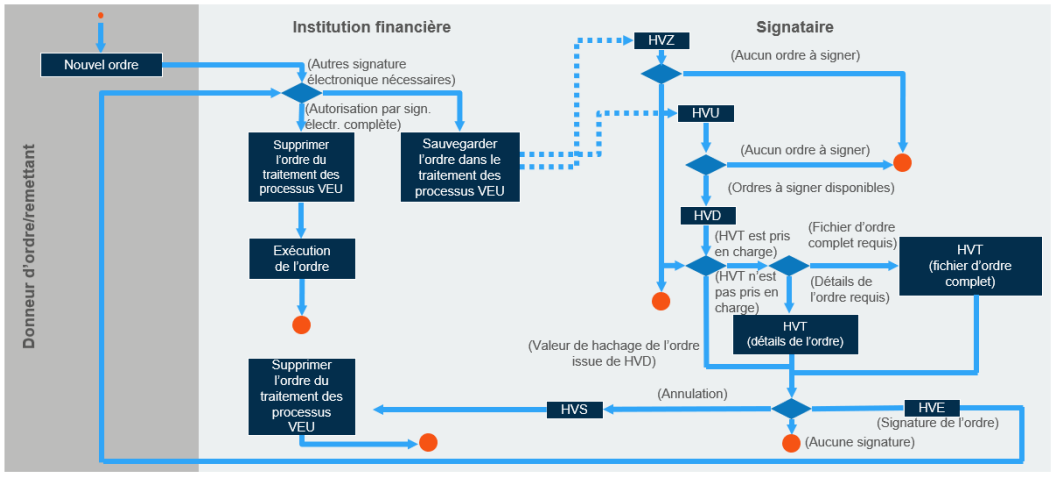


Figure 8 : Procédure VEU

Alors que la VEU est très répandue en Allemagne, elle n'est pas courante en France et en Suisse, mais elle devrait être introduite également dans ces pays avec EBICS 3.0.

En France, il est courant d'envoyer les signatures avec l'ordre. Avec le profil EBICS TS, le traitement d'un ordre est le suivant, en fonction du nombre de signatures :

- Une signature : l'ordre est entièrement autorisé avec une seule signature et est exécuté.
- Deux signatures : le système d'application décide si une deuxième signature est requise et si l'ordre est suffisamment autorisé. Il est décidé par exemple, si un ordre peut être exécuté dans le cas où un des deux signataires n'est pas autorisé.

- Une signature sur l'ordre, deux signatures suivant le plafond : le système d'application décide, si l'ordre est suffisamment autorisé ou si en fonction du plafond une deuxième signature est nécessaire.

Avec l'introduction d'EBICS 3.0, il peut y avoir des contrats mixtes de type d'ordre et BTF pendant la phase de migration. Afin de pouvoir utiliser des modèles d'autorisation existants comme point de départ, il faut respecter certaines conditions cadre des ordres BTF (ici BTU pour la remise), par exemple :

- BTU ne doit pas correspondre au modèle d'autorisation de l'ordre, mais doit être configuré sur le même type d'ordre.
- BTU est utilisé pour le téléchargement du dossier de signatures.
- Les champs vides dans le filtre BTF sont des caractères génériques, selon la spécification :

  Tous les ordres adaptés du dossier de signatures sont fournis (il n'est pas possible d'adresser un BTU spécifique avec un champ vide).
- Un BTU d'un HVx n'est pas signalé en plus du BTU de l'ordre dans des exits.

6.4 Systèmes de portail

Bien que le terme portail n'apparaisse pas de manière explicite dans la spécification EBICS, l'utilisation de la signature d'authentification permet d'intégrer des tiers lors de la remise d'ordres. EBICS ne va pas aussi loin que le standard FinTS dans lequel les opérateurs de portail ou les intermédiaires sont pourvus d'un rôle qui leur est propre – la séparation du remettant (participant technique) et du/des donneur(s) d'ordre permet toutefois de construire des scénarios de portails simplifiés. En utilisant la catégorie de signature T, cette instance de transport est aussi accompagnée de règles adaptées à ces systèmes.

6.5 Fonctions optionnelles

Dans les sections précédentes, nous avons évoqué le fait que certaines fonctions telles que la récupération ou la demande détaillée avec VEU présentent un caractère optionnel. Certaines des fonctions appartenant à ce portefeuille sont brièvement décrites dans les paragraphes suivants.

6.5.1 Vérification préalable

Comme il est expliqué de manière détaillée dans la section *Séquences EBICS* à la page 41, une transaction EBICS se déroule en deux étapes. Dans la première étape, un transfert de fichier (éventuellement très volumineux) est préparé au moyen d'un bref message pour l'initialisation.

Dans cette étape, il est possible d'effectuer des vérifications préalables optionnels pour des transactions d'émission à volume défini et d'éviter ainsi qu'un transfert non justifié soit autorisé. Les détails suivants peuvent être vérifiés dans le cadre de la vérification préalable :

- Vérification de l'autorisation du compte
- Vérification de limite
- Vérification de la signature électronique sur base de la valeur de hachage du fichier

Le volume possible pour la vérification préalable dépend de savoir lesquelles de ces vérifications sont concrètement prises en charge par l'institution et quelles informations sont livrées ou peuvent être livrées par le produit du client. Il ne s'agit donc pas de se défendre contre des attaques mais d'une fonctionnalité permettant d'augmenter la sécurité de fonctionnement et d'optimiser les besoins en ressources puisque les émissions de fichiers incorrectes ne sont même pas démarrées.

6.6 Données du participant

Les types d'ordre suivants permettent au produit du client de télécharger des informations concernant les accords conclus avec l'institution financière :

- HAA télécharger les types d'ordre téléchargeable
- HPD télécharger les paramètres bancaires
- HKD télécharger les données du client et du participant à partir du client
- HTD télécharger les données du client et du participant à partir du participant

Grâce à ces types d'ordre optionnels, un participant peut configurer son produit client pour l'accès bancaire ou bien adapter localement le produit client à un environnement adapté au participant, en affichant par exemple seulement les types d'ordre supportés.

Lors du transfert, les fonctions optionnelles (comme la vérification préalable ou la récupération) prises en charge par l'institution sont également transmises, en plus des paramètres d'accès comme l'URL et le nom de l'institution.

Les données du client et du participant informent sur les détails suivants des accords commerciaux :

- Informations sur le client, son adresse, par exemple
- Informations sur les comptes, numéros de compte et devises, par exemple
- Types d'ordre autorisés
- Attributs du participant, ID participant et catégorie de signature, par exemple

À partir de ces informations très détaillées, un produit client peut réaliser une configuration entièrement automatisée de l'environnement local. Des informations sur le statut permettent une analyse précise même en cas d'erreur.

6.7 Notifications en temps réel

Il s'avère que les entreprises clientes ont plus souvent besoin des notifications en temps réel sur la réception du paiement. Cette tendance est notamment due au processus des paiements instantanés. Dans le cas de la communication EBICS, c'est toujours l'entreprise cliente (client EBICS) qui prend l'initiative. Le serveur EBICS d'une institution financière réagit uniquement aux demandes entrantes (inbound), mais il ne lance pas un échange. Mais comment une information peut-elle être transférée rapidement de l'institution financière au client ? À cette fin, le DK s'est mise d'accord sur la mise en œuvre d'une interface pour notifications en temps réel permettant de lancer côté banque un processus de téléchargement par le système client, en respectant le modèle des rôles EBICS (voir *Annexe 2 : Spécification „Notifications en temps réel"* [9]). La communication sortante (outbound) de l'institution financière au client entreprise utilise un service push sur base de WebSocket agissant en tant que composant central pour l'envoi actif des notifications aux clients et aux participants EBICS.

6.8 EBICS pour l'exploitation interbancaire

EBICS est également utilisé pour l'exploitation interbancaire dans l'échange du trafic des paiements de masse (paiement SEPA) ainsi que pour les paiements instantanés.

6.8.1 Connexion au SEPA-Clearer de la Bundesbank allemande

En Allemagne, les solutions de producteur sont de plus en plus remplacées par EBICS comme standard ouvert dans la compensation bilatérale.

Un champ d'application dans les échanges interbancaires est la connexion des instituts à la Bundesbank allemande. La Bundesbank ne propose avec SEPA plus que deux interfaces :

- EBICS avec messages SEPA pacs
- SWIFT FileAct

La Bundesbank a introduit ses propres types d'ordres dans EBICS et spécifié des formats, par exemple pour PTK.

6.8.2 Connexion à la plateforme STEP2 d'EBA CLEARING

Un autre champ d'application dans les échanges interbancaires pour les paiements SEPA est la connexion des institutions financières à STEP2 de l'EBA CLEARING. Depuis fin 2013, l'EBA CLEARING fournit cet accès aux institutions financières connectées également via EBICS comme alternative à l'accès SWIFT (à partir d'EBICS 2.5). L'EBA CLEARING a également introduit ses propres types d'ordre dans EBICS et spécifié des formats pour l'échange de données via EBICS.

6.8.3 Échange interbancaire bilatéral

Pour l'échange bilatéral entre institutions financières, il n'y a pas de définition dans la spécification EBICS. Les partenaires font leurs accords de manière bilatérale. Ces accords concernent, outre le traitement des retours (transactions R), également des questions au niveau commercial, comme le transfert de responsabilité ou des SLA spécifiques (par exemple taille du fichier maximale).

Pour les types d'ordre et les régularisations techniques, ce sont normalement les règles de l'EBA CLEARING pour la connexion de STEP2 qui s'appliquent.

6.8.4 Paiements instantanés

Les paiements instantanés représentent la prochaine étape de l'harmonisation des paiements au sein de l'espaces SEPA, ayant comme objectif de promouvoir la compétitivité et la croissance économique de l'Europe. Après avoir presque terminé le passage aux virements et prélèvements SEPA, et pendant une période pendant laquelle la numérisation de l'économie entière amène nouvelles attentes du côté client et du côté distributeur, les paiements instantanés représenteront le thème central de European Payment Council (EPC) des prochaines années.

La pièce maîtresse est le nouveau schéma SEPA Instant Credit Transfer (SCTInst). Ce système offre, en raison d'une affectation spécifique du schéma de virement SEPA standard, une connexion forte au transfert de paiement SEPA existant et les processus et implémentations déjà établis. Même si le schéma ne supporte que l'euro, les comptes de débit et de crédit peuvent être tenus dans une autre devise.

Depuis novembre 2017, l'EBA CLEARING offre, sur base de SCTInst, un service paiements instantanés (RT1) à l'échelle européenne. La BCE prévoit le Target Instant Payments Service (TIPS) à partir d'automne 2018. En dehors de cela, il existe aussi des procédures locales dans certains pays.

L'une des caractéristiques principales des paiements instantanés est la durée entre le transfert d'un ordre SCT Inst validé par l'institution financière du donneur d'ordre jusqu'à la réponse de l'institution financière du bénéficiaire. Cette durée ne doit normalement pas dépasser 10 secondes. Si un timeout apparaît exceptionnellement, le rulebook prévoit des règles pour la demande de statut. Dans tous les cas, la banque du bénéficiaire part du principe que le paiement a été effectué avec succès, sauf si un retour négatif est envoyé. La condition préalable pour ce procédé est une disponibilité 24/7/365 de tous les systèmes concernés.

Pour des raisons de sécurité, un paiement instantané individuel est limité à 15 000 euros. En revanche, il est possible de conclure des accords bilatéraux sur des montants plus élevés. Les paiements instantanés SEPA existent dans les 34 pays de l'espace SEPA. Le support de SCT Inst n'est actuellement pas obligatoire pour les institutions financières. Pour la génération d'un paiement instantané, il est indispensable que l'institution financière du bénéficiaire offre cette fonction.

L'EBA CLEARING offre SiaNet et EBICS (à partir d'EBICS 2.5) en tant que canal d'accès au service RT1. Comparable à celle de la connexion à STEP2, l'EBA Clearing met en œuvre un guide d'implémentation pour la connexion à EBICS. Les messages de paiements instantanés sont transférés en une étape via EBCIS, les rapports basés sur des fichiers sont transférés via EBICS, comme il est usuel pour STEP2. Pour l'utilisation en une étape, basée sur des messages d'EBICS 3.0 au service RT1, une propre spécification sous forme d'un document delta a été créée (voir *Use of EBICS for the Clearing & Settlement of Instant Payment Transactions (Delta - Concept)* [8]) et sur le site web d'EBICS (www.ebics.de et www.ebics.org).

7 Séquences EBICS

Suite à cette description des fonctionnalités d'EBICS, le dernier paragraphe technique s'intéresse aux séquences réelles du protocole.

Une unité de traitement achevée est qualifiée de transaction. EBICS fait la distinction entre les transactions « émission » et « téléchargement ». Les transactions upload servent, par exemple, à remettre des ordres alors que les transactions download sont utilisées pour télécharger les relevés de compte.

Les transactions sont divisées en phases et étapes de transaction. Les phases de transaction suivantes sont possibles :

Transaction upload	Transactions download
Initialisation	Initialisation
Transfert de données	Transfert de données
–	Validation

Les phases de transaction peuvent être composées de plusieurs étapes, chacune d'elles consistant d'une requête EBICS (EBICS request) et d'une réponse (EBICS response) correspondante. Alors que la phase d'initialisation est constituée d'une seule étape, la phase de transfert de données peut, pour des raisons de segmentation, contenir plusieurs étapes.

Une transaction est généralement initiée par le produit client. Le système du côté banque peut seulement intervenir par initiation, par exemple, en communiquant une récupération au système du client après une annulation.

La connexion entre les différentes phases de transaction se fait à partir d'un ID transaction qui est générée par le système bancaire et communiquée dans la réponse (response) de l'initialisation.

Chaque requête EBICS (EBICS request) et chaque réponse EBICS (EBICS response) incluent la signature d'authentification du client/participant ou de l'institution.

La figure suivante présente les étapes d'une transaction EBICS :

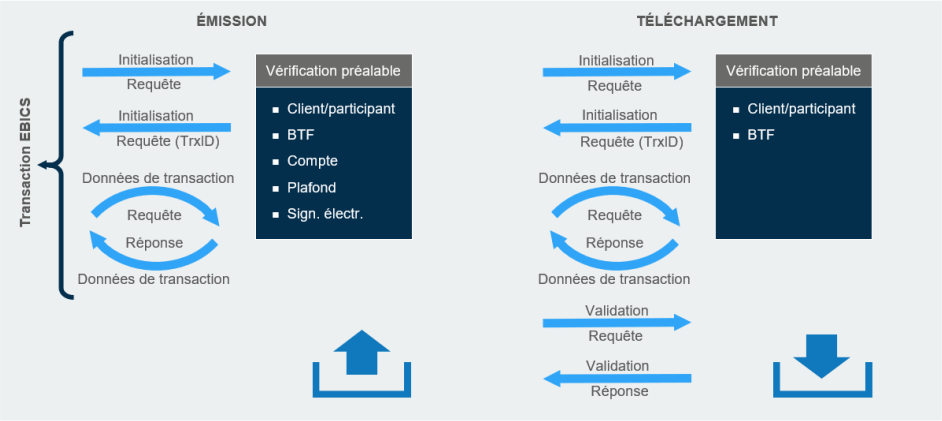


Figure 9 : Processus d'une transaction EBICS

8 Positionnement à l'échelle internationale

EBICS en tant qu'extension de l'accord DFÜ (EDI) décrit les définitions concernant la communication et la sécurité pour les paiements de masse dans les offres de services bancaires aux entreprises. Tant au niveau national qu'au niveau international, on trouve des standards qui viennent compléter ou bien qui se recoupent avec EBICS. Certains de ces standards seront brièvement présentés par la suite et seront mis en relation avec EBICS.

8.1 FinTS

FinTS (Financial Transaction Services, avant HBCI – Homebanking Computer Interface) est également un standard DK, qui cependant met l'accent sur la banque en ligne avec les clients privés et professionnels. Dans sa forme classique, FinTS reproduit donc des dialogues entre le client et la banque et traite des transactions individuelles qui sont orientées sur les messages. FinTS inclut des fonctionnalités telles que données de paramètres bancaires ou d'utilisateur qui sont comparables à celles d'EBICS.

Dans sa version la plus récente 4.1, FinTS mise aussi de manière conséquente sur les standards Internet comme HTTP ou XML. Quant aux procédés de communication, ils ont été enrichis par des datagrammes sans dialogue et la communication banque-client.

Dans le domaine de la sécurité, FinTS supporte à la fois les signatures électroniques ainsi que le procédé PIN/TAN dans diverses variantes.

Comme dans EBICS, les formats courants des opérations de paiements (SEPA, camt, DTAZV et SWIFT) sont aussi pris en charge par FinTS ; ils sont qualifiés d'opérations métier. FinTS contient aussi paiements instantanés. La DK veille à ce que les versions et les contenus de ces formats soient utilisés de la même manière par les deux standards. En outre, FinTS a la possibilité de définir de nombreuses opérations métier allant de l'ordre de virement permanent, en passant par l'argent à terme, jusqu'aux messages libres avec l'institution. Ces opérations métier permettent (au moins) d'établir un standard national là où il n'existe aucune définition internationale.

Dans le domaine des clients professionnels, le client de FinTS dispose par exemple de sa propre implémentation de la signature électronique disjointe (VEU), outre les opérations métier identiques à EBICS pour lots ou opérations de compte. Ce qui manque actuellement au standard, ce sont toutes les possibilités de paiements de masse comme la segmentation ou la récupération.

En résumé, il faut considérer FinTS comme un complément à EBICS. Cela est valable pour tous les contextes où clients professionnels et clients entreprises sont un groupe cible commune, étant donné qu'ils réalisent leurs transactions financières dans les deux mondes. Ainsi une entreprise réalisera des paiements de masse mais sera aussi active dans le négoce de valeurs ou les opérations sur titre. Pour certains types d'opération, le lieu de l'opération sera même déterminant (dans le service de la comptabilité ou par un gérant de société en déplacement, par exemple).

Les nouveaux produits clients se sont déjà adaptés à cette situation et proposent avec EBICS et FinTS deux protocoles de communication.

Pour un examen plus profond du standard FinTS, nous recommandons la lecture du compendium FinTS qui peut être téléchargé sous *fints.org* :

8.2 SWIFT

Dans l'interaction entre EBICS et SWIFT, les structures suivantes sont à mentionner :

- Les formats classiques FIN pour les opérations de paiement internationales
- Les activités XML et ISO de SWIFT
- SWIFTNet comme propre standard de communication
- SWIFT FileAct comme standard de transfert de fichiers

Il y a peu à dire sur les formats FIN classiques tels que MT940. Ils sont stables et seulement soumis à des modifications légales ; ils sont intégrés de manière identique dans le protocole respectif des deux principaux standards allemands EBICS et FinTS. Cela engendre une certaine indépendance de SWIFT, dans la mesure où le travail s'effectue seulement à partir de référencements.

Le fait qu'une version des formats basée sur XML soit disponible avec SWIFT XML ne modifie en rien la séparation stricte des tâches entre les standards. Avec la création des formats XML, SWIFT a procédé de manière très abstraite et a quasiment effectué un « Reverse Engineering » du monde existant. Suite à un travail méticuleux sur plusieurs années utilisant UML, des modèles de processus pour les opérations de paiement internationales ont été confectionnés ; aujourd'hui, ils ne servent qu'à générer les formats FIN et XML. Grâce à cette approche méthodique, SWIFT s'est hissé vers le haut dans le domaine des standards internationaux de transaction financière et a réussi à positionner les composantes centrales de ces modèles comme standard ISO 20022.

Alors que les efforts ISO de SWIFT devraient influencer très fortement l'évolution des formats de paiement, le protocole de transport correspondant, servant de base à SWIFTNet est plutôt d'importance secondaire et doit être considéré comme une évolution propriétaire. SWIFTNet possède certainement un taux de pénétration stable dans les opérations interbancaires, mais ne joue quasiment aucun rôle dans la relation client-banque.

Ainsi, la principale caractéristique du standard SWIFT est d'agir en tant qu'instance pour la publication et la mise à jour des formats de paiements. Cela décrit sa position par rapport à EBICS, qui devrait rester stable dans les années à venir.

Vu que la France est engagée dans la société SEPA, le réseau SWIFT a également une certaine influence en France, car ce standard joue un rôle significatif en France. SWIFT FileAct est également de plus en plus utilisé comme protocole de transfert de fichiers. Cependant, on peut conclure que SWIFT (voir *swift.com*) et EBICS peuvent aisément cohabiter.

8.3 PeSIT-IP

Le standard français PeSIT peut être considéré comme un standard complémentaire à EBICS, particulièrement dans le trafic interbancaire, mais aussi en partie pour les grandes entreprises. PeSIT permet aussi de remettre des paiements de masse et de livrer des données d'écriture. Les entreprises clientes en France utilisent souvent des produits qui disposent d'EBICS et d'un module PeSIT-IP.

8.4 SFTP et FTP(S)

Les protocoles de transfert de fichiers basés sur FTP sont utilisés de manière isolée dans les transactions financières en Europe. Outre des protocoles présentés jusqu'ici, ils ne règlent que le transport et non pas un type quelconque de traitement métier. Au niveau de sécurité, les protocoles ne correspondent pas aux exigences actuelles des transactions financières. En raison de la vaste disponibilité comme logiciel système, SFTP ou FTPS sont souvent utilisés lors du transfert général de fichiers.

8.5 Perspective

Cette description des standards explique qu'il n'existe au jour d'aujourd'hui aucun standard industriel comparable (pas même sur le plan international).

On peut donc en déduire que EBICS sera le standard de référence pour les opérations de paiement de masse en Europe et à l'international. Cela est souligné du fait qu'outre les partenaires existants de la société EBICS (Allemagne, France, Suisse), EBICS est de plus en plus pris en charge par des institutions financières dans d'autres pays comme l'Autriche, l'Espagne, l'Italie, le Portugal et l'Irlande. Ce développement est encore facilité par l'introduction d'EBICS 3.0 et l'harmonisation y liée.

Les paiements instantanés peuvent servir de motivateur à l'introduction d'EBICS dans d'autres pays de l'UE, car un traitement uniformisé à l'échelle européenne amène des avantages à toutes les instances impliquées.

La dernière section illustre à titre d'exemple l'implémentation d'EBICS et sa migration sur base d'une gamme de produit concrète.

9 Mise en œuvre

Après l'aperçu des fonctionnalités d'EBICS et la représentation du scénario d'ensemble, cette dernière section s'attache à illustrer une mise en œuvre du standard et de quelle manière l'ancien et le nouveau standard interagissent.

À cet effet, la gamme de produit TRAVIC (Transaction Services), dont les différents modules peuvent servir à structurer un tel scénario d'ensemble, est présentée.

TRAVIC est composé des éléments suivants, qui peuvent être combinés suivant le besoin :

Composant	Description
TRAVIC-Corporate	Comprend toutes les fonctionnalités côté banque pour EBICS et EBICS interbancaire et en outre les canaux PeSIT et SFTP/FTP(S).
TRAVIC-Port	Implémentation d'un portail EBICS pour l'exécution d'opérations de paiement
TRAVIC-Interbank	Permet de remettre des paiements via EBICS auprès des institutions de clearing européennes, ou dans le cas des paiements instantanés via EBA Clearing
TRAVIC-Link	Met à disposition un portefeuille de transfert de fichiers qui permet, par exemple de transférer automatiquement des ordres (dotés de signatures électroniques bancaires) à une banque via EBICS ou d'autres protocole de transfert de fichiers
TRAVIC-EBICS-Mobile	Permet aux utilisateurs de valider/signer en déplacement des fichiers d'ordre pour des opérations de paiement nationales et internationales qui sont disponibles auprès de l'institution financière
TRAVIC-Push-Server	Information active du client concernant des ordres EBICS à l'application, par courriel, WebSocket ou d'autres chemins
TRAVIC-Retail	Complète la structure et met à disposition toutes les fonctionnalités centrales pour un système FinTS du côté banque.
API des services TRAVIC pour EBICS	Aide à la mise en œuvre d'EBICS dans les produits client par l'API des services TRAVIC pour EBICS et TRAVIC-EBICS-API, qui met à disposition une suite EBICS complète et ergonomique pour une parfaite intégration côté client.

Composant	Description
Target Instant Payment Settlement (TIPS)	Contient des fonctions de compensation et de règlement pour paiements instantanés

À l'exception de TRAVIC-Retail qui n'est pas pris en considération dans ce contexte, les différents modules sont présentés de manière plus détaillée dans ce qui suit.

9.1 TRAVIC-Corporate

TRAVIC-Corporate met à disposition toutes les fonctions décrites dans EBICS, aussi les fonctions opérationnelles. Des outils fournis séparément permettent également l'adoption de données de base et de clés cryptographiques provenant des produits d'autres fabricants dans le cadre d'une migration :

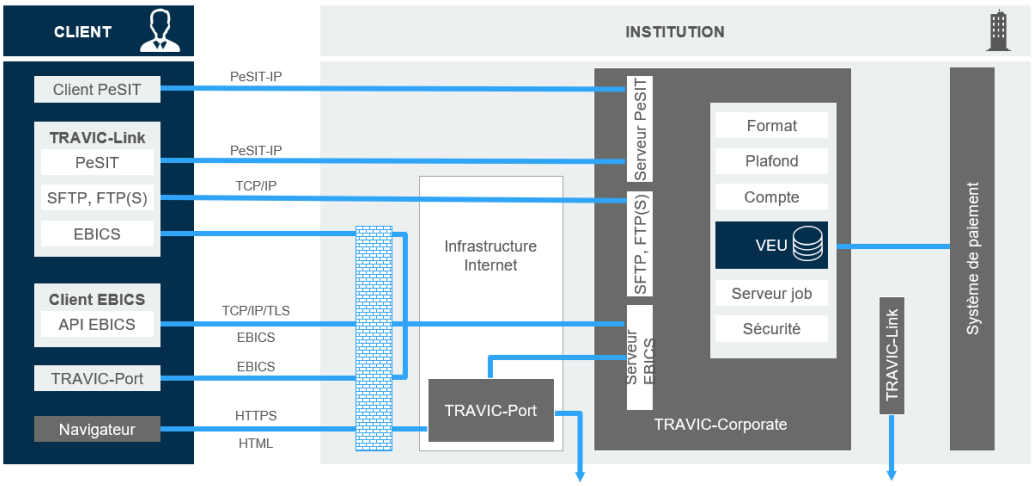


Figure 10 : Composants de la gamme de produits TRAVIC

TRAVIC-Corporate est disponible sur plusieurs plateformes Unix et Linux afin de pouvoir sélectionner l'environnement optimal pour chaque type d'utilisation.

9.2 TRAVIC-Port

Dans le domaine de la signature disjointe et lorsque le nombre d'ordres à saisir et à remettre est faible, une intégration de type portail avec EBICS est le complément idéal d'une gamme de prestation proposée par une institution financière. Par conséquent, il n'est pas étonnant que de plus en plus de banques intègrent des portails de clients entreprises dans leur portefeuille de la banque en ligne.

TRAVIC-Port utilise EBICS-Kernel comme noyau central de la communication multibancaire pour mettre en place le protocole EBICS. Ces fonctions principales sont enrichies par des services web pour mettre en place la structure

métier permettant de réaliser des opérations de paiement et de gérer le profil des utilisateurs, ce qui permet aux clients d'effectuer les tâches administratives.

Pour faciliter l'intégration dans des solutions de la banque en ligne déjà installées, la visualisation des fonctions du portail a lieu par des interfaces de services web. Cela signifie que la présentation peut être effectuée par la banque ou son prestataire de technologie de l'information. TRAVIC-Port dispose aussi de la fonctionnalité Single-sign-on qui permet l'intégration de portails dans TRAVIC-Port et inversement.

Avec ces moyens, il est possible d'édifier, avec peu d'efforts d'implémentation, la partie transactionnelle d'un portail d'entreprises clientes et de l'enrichir par d'autres fonctions métier.

9.3 TRAVIC-Interbank

Dans les opérations interbancaires EBICS se caractérise en particulier par les rôles similaires des deux partenaires de communication. Chaque partenaire dispose d'un serveur EBICS et d'un client EBICS. TRAVIC-Interbank dispose des composants pour les deux rôles. L'autorisation de l'échange des données s'effectue conjointement avec le transfert de données. TRAVIC-Interbank prend en charge les scénarios d'application suivants :

- Les procédures interbancaires, les procédures de la Bundesbank, l'échange des opérations de paiement de masse électroniques, le SEPA-Clearer de la Bundesbank ou STEP2 de l'EBA CLEARING via EBICS
- TRAVIC-Interbank pour paiements instantanés RT1 de l'EBA CLEARING
- TRAVIC-Interbank pour la demande de paiement R2P de l'EBA CLEARING

9.4 TRAVIC-Link

TRAVIC-Link est un produit de transfert de fichiers universel pouvant être intégré dans divers scénarios.

Dans le cadre des opérations de paiement électroniques pour les clients-entreprises, TRAVIC-Link occupe le rôle du système client conformément au DFÜ (EDI) agreement avec les clients. Dans ces scénarios, TRAVIC-Link supporte les standards BCS et EBICS. TRAVIC-Link complète les systèmes de comptabilité financière au niveau du transfert automatique des ordres et du téléchargement automatique et de la redirection des relevés. Les fichiers d'ordre à transmettre à une banque peuvent être porteurs de signatures électroniques avant même que le transfert n'ait eu lieu.

Le protocole de communication ONGUM-IP intégré dans TRAVIC-Link permet des transferts de fichiers à contenus quelconques entre plusieurs systèmes TRAVIC-Link.

Une autre fonctionnalité de TRAVIC-Link est la communication par l'intermédiaire de ce qu'on appelle logiciel standard. TRAVIC-Link propose les interfaces correspondantes.

Les procédés ou modules de communication suivants sont actuellement supportés par TRAVIC-Link.

Banque en ligne dans l'environnement des entreprises clientes

- EBICS
- PeSIT-IP

Protocoles de transfert de fichiers intégrés

- ONGUM-IP
- Secure-FTP
- HTTP
- JMS
- FTP(S)

Logiciel standard intégrable via interfaces :

- Connect:Direct (Sterling Commerce)
- UDM (Stonebranch)

9.5 TRAVIC-EBICS-Mobile, TRAVIC-Push-Server

TRAVIC-EBICS-Mobile est une application mobile pour la signature d'ordres de paiement qui ont été soumis auprès des institutions financières par protocole EBICS.

Les informations sur les comptes (soldes et écritures) continuent d'être affichées.

L'application est destinée aux institutions financières et aux grandes entreprises qui veulent offrir à leurs clients ou leurs salariés la possibilité de valider des ordres de paiement de façon mobile, c'est-à-dire en dehors du site de l'entreprise.

TRAVIC-EBICS-Mobile

- Est une solution multi-banques car elle est équipée d'interfaces standardisées et du protocole d'échange EBICS sur le serveur Gateway
- Peut être configuré individuellement
- Offre une sécurité d'exploitation par des signatures électroniques et des transferts de messages chiffrés
- Intègre une fonction push pour les banques qui opèrent TRAVIC-Corporate avec TRAVIC-Push-Server

TRAVIC-Push-Server assure la communication sortante (outbound) de l'institution financière à l'entreprise cliente. Le système agit en tant que composant

central pour l'envoi actif des notifications via les canaux de communication préférés des clients et des participants EBICS. Outre les canaux push mobiles et courriel, TRAVIC-Push-Server dispose de la notification des informations en temps réel via une interface WebSocket, conformément au nouveau document *Annexe 2 : Spécification „Notifications en temps réel“* [9].

9.6 TRAVIC-EBICS-API

Alors que les fabricants d'ordinateurs bancaires s'appliquent ardemment à adapter leurs produits au standard EBICS, les fabricants de produits du client doivent faire face au problème suivant :

Des centaines de pages de documentation doivent être modifiées et intégrées, par exemple, seulement dans le but d'ajouter une nouvelle voie de transport à un produit de paiement. À l'heure actuelle, nous ne savons pas dans quelle mesure les caractéristiques optionnelles d'EBICS seront utilisées et donc si on doit les prendre en compte dès le départ.

TRAVIC-EBICS-API, l'API des services pour EBICS aide à résoudre ce problème. Ce progiciel met à disposition une suite EBICS complète et ergonomique pour une parfaite intégration côté client.

Bibliographie

[1] DFÜ agreement (accord EDI)
Appendix 1 : Specification for the EBICS connection
Version 3.0.2 du 27/06/2022
Die Deutsche Kreditwirtschaft

[2] DFÜ agreement (accord EDI)
Appendix 2 : FTAM connexion
- obsolète -
Die Deutsche Kreditwirtschaft

[3] DFÜ agreement (accord EDI)
Appendix 3 : Specification of Data Formats
Version 3.6 du 06/04/2022
Die Deutsche Kreditwirtschaft

[4] EBICS-Implementation Guide (anglais)
basée sur la version EBICS 3.0 du 27/06/2022
EBICS Working Group

[5] EBICS-Sicherheitskonzept (concept de sécurité EBICS, uniquement sur demande)
Version 1.6 du 03/02/2021
Die Deutsche Kreditwirtschaft

[6] Krypto LifeCycle EBICS
Version 1.2 du 29/04/2022

[7] FinTS V4.1
Version 4.1 du 12/09/2019
Die Deutsche Kreditwirtschaft

[8] Use of EBICS for the Clearing & Settlement of Instant Payment Transactions (Delta - Concept)
du 30/10/2019
EBICS Working Group

[9] Accord DFÜ (EDI)
Annexe 2 : Spécification „Notifications en temps réel“
Die Deutsche Kreditwirtschaft (Comité allemand pour le secteur bancaire, DK)
Version 1.0 du 17/07/2019

Liste des abréviations

BCS	Banking Communication Standard
BPD	Données des paramètres bancaires
BSI	Bundesamt für Sicherheit in der Informationstechnik (Office fédéral de la sécurité des technologies de l'information)
BTD	Type d'ordre administratif pour télécharger un fichier qui est plus caractérisé par une structure BTF
BTF	Business Transaction Formats
BTU	Type d'ordre administratif pour envoyer un fichier qui est plus caractérisé par une structure BTF
CFONB	Comité Français d'Organisation et de Normalisation Bancaire
DFÜ	Datenfernübertragung (télétransmission de données)
DK	Die Deutsche Kreditwirtschaft (Comité allemand pour le secteur bancaire, avant → ZKA)
EBICS	Electronic Banking Internet Communication Standard
EDS	Electronic Distributed Signature (voir aussi →VEU)
ETEBAC	Echange TElematique BAnque-Clients
SE	Signature électronique
FTP	Filetransfer Protocol
HTTP	Hypertext Transport Protocol
FinTS	Financial Transaction Services
FTAM	Filetransfer Access and Management
HBCI	HomeBanking Computer Interface
IP	Instant Payments (paiements instantanés)
TI	Technologie de l'information
ISO	International Standards Organisation
OAGi	Open Application Group

OSI	Open Systems Interconnect
PSA	Payment Services Austria GmbH
RT1	Service de paiements instantanés de l'EBA CLEARING
SEPA	Single European Payment Area
SIX	Swiss Infrastructure and Exchange
SRZ	Prestataire
SSL	Secure Socket Layer
TCP/IP	Transport Communication Protocol/Internet Protocol
TLS	Transport Layer Security
UML	Unified Modelling Language
TWIST	Transaction Workflow Innovation Standards Team
VEU	Verteilte Elektronische Unterschrift (voir aussi →VEU)
W3C	World Wide Web Consortium, Organe de normalisation des techniques sur Internet
XML	Extensible Markup Language
ZKA	Zentraler Kreditausschuss (Organisme de normalisation bancaire allemand → aujourd'hui DK)

Liste des illustrations

Moorfuhrtweg 13
22301 Hambourg
Tel. : +49 40 227433-0
Fax : +49 40 227433-1333

E-Mail : info@ppi.de
Internet : www.ppi.de