INFORMANS
Solutions for e-business

eBusiness Protocol Hub For Ebics 2.4,2.5 SDK

Introduction

Le protocole de communication Ebics est utilisé en Allemagne sous l'égide du ZKA mais également en France sous l'égide du CFONB (Comite Français d'Organisation et de Normalisation Bancaire) afin de remplacer, entre autres et à terme, les protocoles des normes ETEBAC par des solutions innovantes permettant un déploiement simple, sécurisé et rapide sur TCP-IP.

Le protocole Ebics a été originellement défini par l'organisme de normalisation Allemand ZKA pour remplacer les standards MCFT® et BCS-FTAM. Ce standard est basé sur les technologies TCP-IP, TLS, HTTP et XML du W3C et de l'IEEE.

Le composant BPH Ebics est un élément de la suite des composants BPH (eBusiness Protocol Hub) Toolkit Suite. Ces composants sont destinés aux éditeurs et banques souhaitant intégrer ou tester ces protocoles dans/avec leurs applications ainsi qu'aux entreprises désireuses d'intégrer des fonctionnalités de communication rapidement et sans compétence métier particulière.

INFORMANS
Solutions for e-business

Solutions for EBICS 2.4,2.5

Le BPH Ebics distribué par **Informans** permet la mise en œuvre de la communication serveur dans une application tierce de manière simple et pratique par l'appel de fonctions de l'interface de programmation (API) fournie.

Il offre principalement les fonctions de communication en sens aller et retour avec les clients fonctionnant sous la norme Ebics

L'ensemble des fonctionnalités présentes dans le protocole sont disponibles ainsi que des fonctions avancées :

- Support du standard **2.4 Ebics H003 révision 1** et **2.5 Ebics H004 révision 1**.
- Support des recommandations Française du **CFONB**.
- Fonction cryptographique de chiffrement/déchiffrement selon la procédure **E002**, et de signature d'identification et d'authentification selon la procédure **X002**.
- Fonction de génération de bi-clés RSA via des certificats X509 auto-signé conforme à la version **X509 V3** et aux recommandations du **CFONB**.
- Vérification des signatures électroniques **A005** et **A006**.
- Encodage/ décodage Base64 conforme à la **RFC 1421** et **2045.**
- Compression/décompression **ZIP (deflate)** conforme à la **RFC 1950** et **1951**
- Support des couches de sécurisation **TLS1** et **HTTP 1.1** en mode serveur

Fort de son expérience et de sa compétence en matière de distribution et de normalisation de protocoles bancaires, **Informans** offre également des services complémentaires de tests et d'homologation (en partenariat avec des partenaires spécialisés) ainsi que la fourniture de fichiers de pré-configuration permettant la connexion (hors paramètres de sécurité) vers une sélection de banques.

INFORMANS
Solutions for e-business

Description fonctionnelle

BPH Solutions for EBICS est un composant prenant en charge la fonction serveur du protocole EBICS. Il n'intègre pas de logique métier d'un serveur bancaire comme décrite dans la spécification EBICS 2.4,2.5 : Le développement de cette logique est laissé à la latitude de l'application hôte.

BPH EBICS peut fonctionner suivant 3 modes :

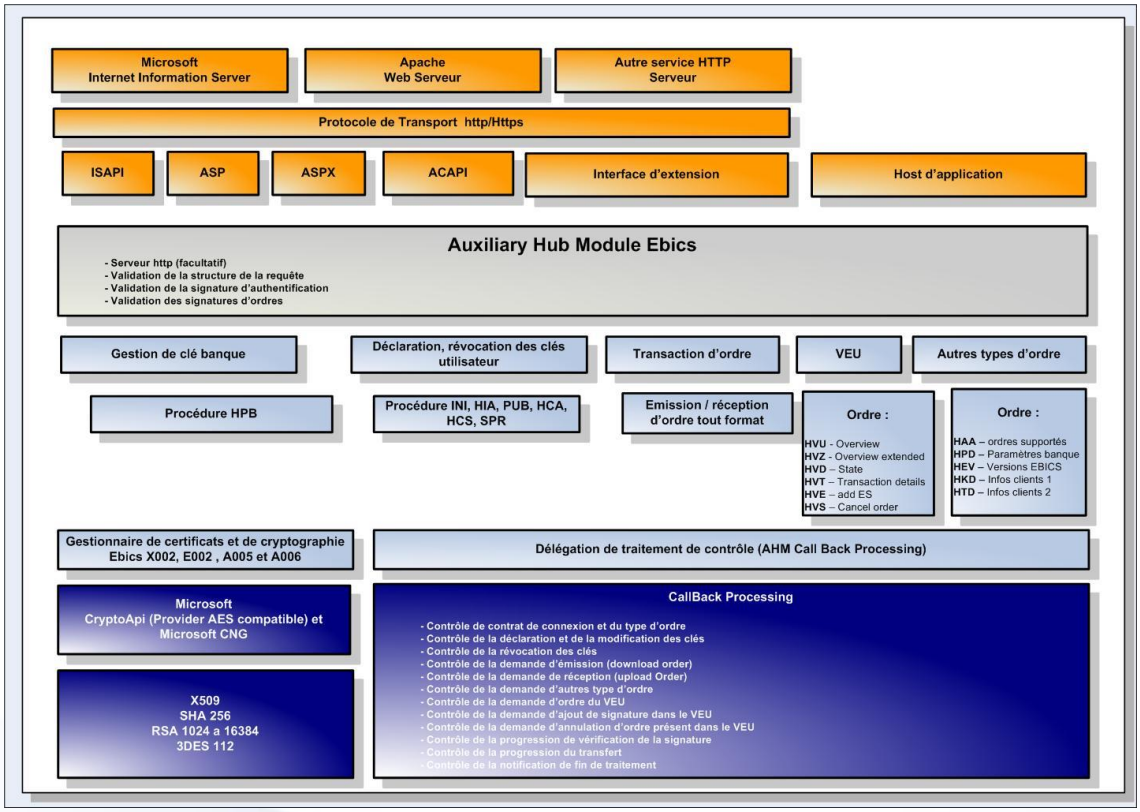
- **Support simple sans activation de la délégation des traitements de contrôle**. Ce mode de fonctionnement ne prend pas en charge le service http serveur, ni le support des ordres spécialisés et du VEU. Seuls les ordres de gestion des clés (INI, HIA, H3K, SPR, PUB, HCA, HCS, HPB) sont pris en charge ainsi que les transactions d'ordre standard et spécialisés FUL et FDL. Ce mode permet le développement rapide d'une fonction de test d'un client EBICS.

- **Support avancé avec activation de la délégation des traitements de contrôle**. En plus du support simple, ce mode de fonctionnement interroge la logique métier implémenté par l'application hôte en utilisant des procédures de rappel ; ces procédures de rappel sont au nombre de douze et permettent de sous traiter:

    - Le contrôle du contrat de connexion et du type d'ordre sollicité
    - L'autorisation de déclaration et de modification des clés du client
    - La révocation des clés du client
    - La sélection du fichier à émettre
    - La création du fichier à recevoir
    - Contrôle de la demande d'autre type d'ordre
    - Contrôle de la demande d'ordre du VEU
    - Contrôle de la demande d'ajout de signature dans le VEU
    - Contrôle de la demande d'annulation d'ordre présent dans le VEU
    - La progression de vérification de la signature
    - La progression du transfert
    - Notification de fin de traitement

- **Support avancé avec activation de la délégation des traitements de contrôle** ainsi que l'activation de la fonction serveur http/https.

L'organisation du composant est le suivant :



INFORMANS
Solutions for e-business

Fonctionnalités de base

Fonctionnalité	Description
Gestion des clés de la banque.	BPH Ebics permet le chargement des bi-clés RSA et des certificats X509 associé. Un trousseau de clé banque est composé de : ▪ la clé d'identification et d'authentification ▪ la clé de chiffrement de la clé de transaction L'accès à la clé publique de la banque est assuré par le support de la procédure **HPB**.
Gestion des clés utilisateurs.	BPH Ebics permet le chargement et la sauvegarde des trousseaux de clés utilisateurs. Un trousseau de clé est composé de : ▪ la clé d'identification et d'authentification ▪ la clé de chiffrement de la clé de transaction ▪ de la clé de signature dit ES (optionnelle) Ces opérations sont effectuée les procédures **INI, HIA,H3K, SPR, PUB, HCA, HCS**
Support de création de bi-clés RSA et certification X509 V3 des clés publique.	BPA Ebics permet la création de certificats X509 V3 auto-signées pour les modes cryptographiques **E002**, **X002** . BPA Ebics supporte les recommandations de génération de certificats X509 du CFONB : ▪ Utilisation d'une signature de certificat **RSASHA-256.** ▪ Mise en place des extensions **AuthorityKeyIdentifier**, **SubjectKeyIdentifier** et **KeyUsage**
Support des recommandations et adaptations locales.	BPA Ebics permet de s'adapter aux recommandations locales des banques. A l'heure actuelle les recommandations Allemandes (**ZKA**) et Françaises (**CFONB**) sont supportées.
Emission et réception des fichiers d'ordre standard et des ordres spécialisés FUL et FDL.	BPH Ebics permet d'émettre et de recevoir des fichiers d'ordres quelconques. ▪ En réception, il permet de déclarer les types d'ordres (ex : IZV) autorisés. ▪ En émission, il permet de déclarer les types d'ordres acceptés.
Vérification des signatures A005 et A006 (uniquement sur VISTA et Windows 2008).	BPH Ebics permet de vérifier les signatures des transactions d'ordre (ou fichier) de type Upload en appliquant les schémas de signature **A005** et **A006** Ebics. Le mode **A004** n'est pas supporté.

Support de politique de certification.	BPH Ebics permet de contrôler les certificats X509 utilisés suivant 4 niveaux : ▪ Aucun contrôle ▪ Niveau X509 sur le certificat terminal de la chaine de certification. ▪ Niveau X509 sur l'ensemble des certificats en excluant le certificat racine. ▪ Niveau X509 sur la chaine complète.
Ordres spécialisées.	BPH Ebics supporte tous les ordres spécialisés via la délégation de traitement de contrôle.
Support du VEU.	BPH Ebics supporte tous les ordres du VEU via la délégation de traitement de contrôle.

Fonctions avancées

Fonctionnalité	Description
Compatibilité multi-banque.	BPH Ebics est compatible avec une utilisation multi-banque.
Cryptographie.	BPH Ebics est compatible avec les providers de cryptographique compatible avec la technologie Microsoft CryptoApi. La version 2.4 d'Ebics impose de fait l'utilisation d'un provider de type AES compatible comme le « **Microsoft Enhanced RSA and AES Cryptographic Provider** ». ▪ Identification/authentification **X002** : Longueur de clé RSA de 1024 à 16384 bits, Algorithme de hashage SHA-256, Padding PKCS#1, Processus de canonisation REC-xml-c14n-20040315 ▪ Chiffrement **E002** : Longueur de clé RSA de 1024 à 16384 bits, Algorithme de chiffrement Triple DES 112 bits, , Padding PKCS#1 ▪ Vérification des signatures **A005/A006** : Longueur de clé RSA de 1536 à 4096 bits, Algorithme de hashage SHA-256, Padding PKCS#1 EMSA-PKCS1-v1_5 et EMSA-PSS. Les clés publiques servant à la réalisation des modes de cryptographie précédemment décrits sont contenus obligatoirement dans des certificats X509 V3 à l'exception de la vérification de la signature.
Délégation de traitement de contrôle.	BPH Ebics permet d'activer la délégation de traitement de contrôle qui permet à votre application d'affiner et de mieux gérer le comportement de votre serveur. Vous pouvez ainsi mieux effectuer le : ▪ contrôle du contrat de connexion et du type

	d'ordre ▪ contrôle de la déclaration et de la modification des clés ▪ contrôle de la révocation des clés ▪ contrôle de la demande d'émission (download order) ▪ contrôle de la demande de réception (upload order) ▪ contrôle des ordres dits « autres » ▪ contrôle des ordres du VEU ▪ contrôle de la progression de la vérification des signatures ▪ contrôle de la progression du transfert ▪ Contrôle de notification de fin de traitement
Serveur http/https.	BPH Ebics permet d'activer le support du service http/https serveur.
Ecriture de trace.	BPH Ebics permet de déclarer le fichier de traçage permettant d'archiver des données internes du composant et des données émis et reçu du réseau.

INFORMANS
Solutions for e-business

Condition d'utilisation

La solution est fournit sous la forme d'un SDK (Software Development Kit) complet :

- Procédure d'installation
- Documentation PDF
- Redistribuable
- Exemples en Vbscript, C# et C++

Il est disponible pour les plateformes Microsoft suivantes :

- BPH Ebics édition 32 bits pour **Windows XP SP3, Windows server 2003, Vista,Seven et Windows Server 2008,R2**
- BPH Ebics édition 64 bits pour **Windows Server 2003 x64, Vista,Seven x64 et Windows Server 2008 ,R2 x64**

Le tableau ci-dessous résume les informations de pré-requis nécessaires pour utiliser et déployer le SDK.

Prérequis	Minimal	Recommandé
Processeur	**Intel Pentium/Core duo toute version et compatible**	**Intel Core 2 duo**
Mémoire	**32 MB**	**64 MB**
Espace disque (NTFS obligatoire)	**20 MB**	**20 MB**
Système d'exploitation	▪ **Windows XP SP3, Windows server 2003, Vista, Seven et Windows Server 2008** ▪ **Windows Server 2003 x64, Vista x64, Seven x64, Windows Server 2008 x64 et Windows Server 2008 R2**	
Runtimes	▪ **DotNet 2.0**	
Langage	**Tous langages supportant la technologie COM de Microsoft.**	
Compilateur	**Tous compilateurs compatibles avec la technologie COM.**	

INFORMANS
Solutions for e-business

Informans diffuse ses produits sur son site spécialisé www.informans.com et à travers un réseau de partenariats non exclusifs avec des éditeurs et des intégrateurs.

Innovez avec INFORMANS grâce à son savoir-faire et son expérience dans la conception de briques logicielles d'E-Business et E-Banking.