INFORMANS
Solutions for e-business

eBusiness Protocol Adaptor 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 BPA Ebics est un élément de la suite des composants BPA (eBusiness Protocol Adaptor) 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 BPA Ebics distribué par **Informans** permet la mise en œuvre de la communication Ebics 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 serveurs bancaires fonctionnant sous la norme Ebics, ce qui permet l'émission signée et chiffrée de fichier d'ordres (paiement débit et crédit, opérations de recouvrement ou avis, ordres de gestion de compte, remise de taxes, etc.) ainsi que la récupération sécurisée d'informations bancaires (relevés de compte, relevés d'opérations et autres avis, rapports).

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**, de signature d'identification et d'authentification selon la procédure **X002**, de signature électronique (ES) selon la procédure **A005**.
- Support en externe des signatures électroniques **A004**, **A005** et **A006**.
- Fonction de génération de bi-clés RSA via des certificats X509 auto-signé conforme à la version **X509 V3** et aux recommandations du **CFONB**.
- 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**

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.

Description fonctionnelle

L'ensemble des fonctionnalités définies dans le protocole sont disponibles ainsi que des fonctions avancées.

Fonctionnalité Ebics	Description
Version et révision Ebics.	BPA Ebics supporte le versionnage EBICS. L'API contient deux propriétés permettant de spécifier la version et le numéro de révision de manière à adapter le comportement du composant.
Support de la déclaration du produit ou agent utilisateur.	BPA Ebics permet la déclaration du produit ou agent utilisateur du protocole.
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** et **A005**. 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.
Support de politique de certification.	BPA 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.
Gestion des trousseaux de clés multi-utilisateurs.	BPA Ebics permet l'initialisation, le chargement, la sauvegarde et la destruction 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)
Gestion des trousseaux de clés multi-	BPA Ebics permet le chargement et la sauvegarde des

banque.	trousseaux de clés banque. Un trousseau de clé banque est composé de : ▪ la clé d'identification et d'authentification ▪ la clé de chiffrement de la clé de transaction BPA s'appuie de préférence sur les certificats X509 du trousseau de la banque s'ils existent.
Déclaration, modification et révocation des clés de signature, d'identification/authentification et de chiffrement utilisateur.	BPA Ebics permet d'effectuer ces opérations via les procédures **INI, HIA, H3K,SPR, PUB, HCA, HCS** pour les modes cryptographiques **E002**, **X002** et **A005**.
Edition des clés de signature et d'identification/authentification et de chiffrement utilisateur.	BPA Ebics permet de générer l'édition au format texte des lettres d'initialisation.
Déclaration et modification de la clé de signature (ES) utilisateur provenant d'un logiciel tiers externe gérant la signature EBICS.	BPA Ebics permet d'effectuer la déclaration et modification de la clé de signature externe via les procédures **INI** et **PUB**. Cette procédure supporte les modes de signature **A004**, **A005** et **A006** ainsi que la déclaration de médium de signature et la nature de la clé publique (Raw, X509).
Téléchargement des clés d'identification/authentification et de chiffrement de la banque.	BPA Ebics permet d'effectuer cette via la procédure HPB.
Emission et réception de fichier d'ordre via les procédures standards et les ordres spécialisés FUL et FDL.	BPA Ebics permet d'émettre et de recevoir des fichiers d'ordres quelconques. ▪ En émission, il permet de déclarer le type d'ordre (ex : IZV), les paramètres de l'ordre et effectuer ou non une signature (ES) de l'ordre en mode A005. ▪ En réception, il permet de déclarer le type d'ordre et les paramètres de l'ordre.
Transport en émission de la signature d'ordre provenant d'un logiciel tiers externe gérant la signature Ebics.	BPA Ebics permet l'ajout, avant l'émission d'un ordre, d'une ou plusieurs signatures (ES) externes. Cette procédure supporte les modes de signature **A004**, **A005** et **A006**.
Gestion des codes de retour Ebics.	BPA Ebics met à disposition les codes de retour et leur description provenant de tous les types de procédures disponibles.
Support du gestionnaire de signatures distribuées (VEU).	BPA Ebics supporte les ordres **VEU** suivant : ▪ **HVU** Téléchargement des informations d'autorisation de signature. ▪ **HVZ** Téléchargement des informations d'autorisation de signature étendues. ▪ **HVD** Téléchargement de l'état du VEU. ▪ **HVT** Téléchargement du détail d'une transaction.

Ordres spécialisées.	▪ **HVE** Ajout d'une à plusieurs signature sur un ordre présent dans le VEU. ▪ **HVS** Annulation d'un ordre présent dans le VEU. BPA Ebics supporte les ordres spécialisés suivant : ▪ **HAA** Téléchargement des types d'ordres disponibles sur le serveur de la banque. ▪ **HPD** Téléchargement des paramètres de la banque ▪ **HKD** Téléchargement des informations société. ▪ **HTD** Téléchargement des informations société restreintes à l'utilisateur donné. ▪ **HEV** Téléchargement des versions Ebics supportées par le serveur de la banque.

Fonctionnalité avancée	Description
Compatibilité multi-utilisateur.	BPA Ebics est compatible avec une utilisation multi-utilisateur.
Cryptographie.	BPA 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 EMSA-PKCS1-v1_5**, 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 EMSA-PKCS1-v1_5** ▪ Signature **A005** : Longueur de clé RSA de 1536 à 4096 bits, Algorithme de hashage SHA-256, Padding **PKCS#1 EMSA-PKCS1-v1_5** Les clés publiques servant à la réalisation des modes de cryptographie précédemment décrits sont contenus obligatoirement dans des certificats X509 V3. Suivant le provider CryptoApi utilisé les clés privées sont contenues soit sur un médium de type software (fichier, registre, …) ou hardware (carte à puce, clé USB,…) Leur accès peut être également protégé par un Pin code (Il n'est pas conseillé d'utiliser un pin code d'accès pour les clés des modes **X002** et **E002**).
Support de l'ANM/AYM.	BPA Ebics supporte l'architecture **ANM/AYM** de la suite eBusiness Protocol Adaptor. Cette couche apporte le

	support direct ou proxisé d'un accès en TCP-IP à un partenaire distant et le support de TLS 1.
Délégation de transport.	BPA Ebics permet de redéfinir simplement la couche de transport via une déclaration d'activation d'une procédure de rappel. Cette procédure de rappel (callback) reçoit la trame Ebics de requête à émettre et attend en retour la trame de réponse.
Ecriture de trace.	BPA Ebics permet de déclarer le fichier de traçage permettant d'archiver des données internes du composant et des données émis et reçu du réseau.
Statistique de transfert.	BPA Ebics publie des statistiques de transferts.

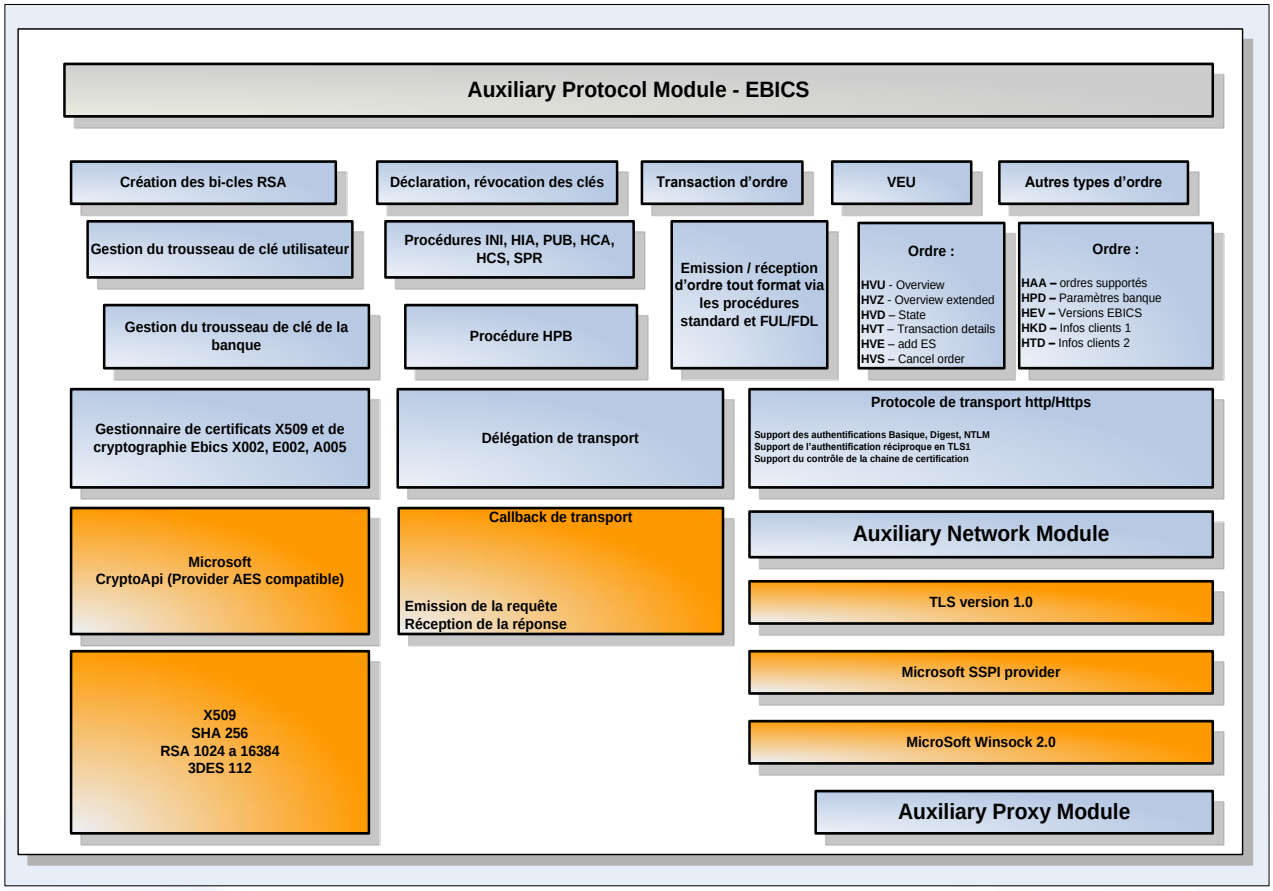
Architecture du composant

BPA Ebics est constitué de 3 composants :

- Le pilote du protocole Ebics ou **APM** (Auxiliary Protocol Module)
- Le pilote réseau ou **ANM** (Auxiliary Network Module)
- Le proxy réseau ou **AYM** (Auxiliary Proxy Module)

Le pilote du protocole EBICS (**APM** Ebics) est l'interface la plus haute et la seule accessible par l'application utilisatrice. Cette interface fait le lien entre l'application utilisatrice (désirant intégrer une couche Ebics) et l'institution financière distante.
Pour ce faire, elle s'appuie sur le pilote **ANM** qui négocie l'ensemble du dialogue réseau soit directement avec les dispositifs réseaux soit via le composant **AYM**.
L'**AYM** est un composant assurant un service de proxy réseau pour les déploiements nécessitant un haut niveau de sécurisation. L'utilisation de ce module est optionnelle.

INFORMANS
Solutions for e-business



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 :

- BPA Ebics édition 32 bits pour **Windows XP SP3, Windows server 2003, Vista,Seven et Windows Server 2008,R2**
- BPA 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	**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.

Copyright

Ce document a été crée par **Informans** et tous les droits de reproduction sont donc réservés. Tous les droits, également ceux de traductions, d'impression ou de reproduction de l'ensemble ou d'une partie du document exige l'accord préalable d'**Informans**.

Les logiciels et de matériels mentionnés dans ce document sont des marques déposées et sont soumises à la législation en vigueur.