



I N F O R M A N S
Solutions for e-business

eBusiness Security Adaptor For Ebics 2.4 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 ZKA1 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 BSA Ebics est un élément de la suite des composants BSA (eBusiness Security Adaptor) Toolkit Suite. Ces composants sont destinés aux éditeurs et banques souhaitant intégrer ou tester des moyens de sécurisation moderne (signature, contrôle d'intégrité, statut,...) dans leurs applications ainsi qu'aux entreprises désireuses d'intégrer ces fonctionnalités rapidement et sans compétence métier particulière.



I N F O R M A N S
Solutions for e-business

Solutions for EBICS 2.4

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

L'ensemble des fonctionnalités de signature définies dans le protocole sont disponibles ainsi que des fonctions avancées :

- Support du standard **2.4 Ebics H003 révision 1**.
- Support des recommandations Française du **CFONB**.
- Fonction cryptographique de signature électronique **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**.

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 de signature définies dans le protocole sont disponibles.

Fonctionnalité	Description
Support de création de bi-clés RSA et certification X509 V3 des clés publique.	<p>BSA Ebics permet la création de certificats X509 V3 auto-signées pour le mode cryptographique de signature A005 et A006.</p> <p>BSA Ebics supporte les recommandations de génération de certificats X509 du CFONB :</p> <ul style="list-style-type: none">■ Utilisation d'une signature de certificat RSASHA-256.■ Mise en place des extensions AuthorityKeyIdentifier, SubjectKeyIdentifier et KeyUsage
Support des recommandations et adaptations locales.	<p>BSA Ebics permet de s'adapter aux recommandations locales des banques. A l'heure actuelle les recommandations Allemandes (ZKA) et Françaises (CFONB) sont supportées.</p>
Ouverture et fermeture du dispositif de signature.	<p>BSA Ebics permet l'ouverture et la fermeture du dispositif de signature à l'aide du Distinguished Name du certificat X509 associé.</p>
Récupération et extraction d'information sur le dispositif de signature.	<p>BSA Ebics permet de récupérer des informations techniques sur les clés cryptographiques et les mécanismes de stockage.</p>
Signature A005 et A006 (à partir de Windows VISTA).	<p>BSA Ebics permet d'effectuer des signatures d'ordre (ou fichier) en appliquant les schémas de signature A005 et A006 Ebics. Le mode A004 n'est pas supporté.</p> <p>Rq : Le mode A006 n'est supporté que si le provider CryptoApi utilisé autorise la technique de translation vers CNG (Cryptographic Next Generation).</p>



Condition d'utilisation

La solution est fournie 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 :

- BSA Ebics édition 32 bits pour **Windows XP SP3, Windows server 2003, Vista, Seven et Windows Server 2008, 2008 R2**
- BSA Ebics édition 64 bits pour **Windows Server 2003 x64, Vista 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	<ul style="list-style-type: none">■ 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	
Langage	Tous langages supportant la technologie COM de Microsoft.	
Compilateur	Tous compilateurs compatibles avec la technologie COM.	



I N F O R M A N S
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 créé 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.