zBackTrust

Electronic Signature System

This solution is a SOA electronic sig... central resource that allows to n... electronic evidences in a company wide ...

It delivers valid long term legal ele... signatures in any document, bas... advanced or qualified electronic certif... through the use of cryptographic ha... already equipped in mainframes compu... with a high reliability and scalability.

CONTENTS

zBackTrust

Electronic signatures in mainframe environments, Linux on System z and z/OS

- **zBackTrust** is a web service based on the standard OASIS DSS with centralized installation. It offers remote electronic signing and verification and can extend the signing capability throughout the entire organization.

- Likewise, thanks to its API, it allows Linux on System z and z/OS applications to directly access the signature and verification functionalities without the need of a DSS connection.

- **zBackTrust** speeds up the centralized electronic fractions at enterprise level.

- **zBackTrust** adheres to the legally required standards: TS 101 903 (complete long term XAdES-XL electronic signatures). It als support TS 102 778 PAdES (PDF signatures)

- **zBackTrust** adheres to European Directives.

Main Characteristics

- *Fast generation and checking of electronic signatures through API and DSS (Digital Signature Service)*
- *Generation of complete XAdES-XL signatures*
- *Support for PDF signatures (PAdES).*
- *Validation of certificates and electronic signatures*
- *Generation of electronic proof for digital custody of signed electronic documents*
- *Compatible with the IBM 4764 and IBM 4765 (CEX2 & CEX3) cryptographic processors*
- *Compatible with different middleware: WebSphere, Weblogic and Tomcat*
- *z/OS y z/Linux environments*
- *Adheres to ETSI and OASIS standards*

At a moment in which a **paradigm change** is occurring from "paper centered document management" to "electronic centered document management", stimulated by both legislation and market forces, it is important to have a component with both of these characteristics. Consequently, for electronic document management systems, the **signature and validation** component is a **key piece in the architecture**, as is the **custody** of documents (e.g. the IBM DR-550 system), as well as document **transformation/routing** management.

From the applications perspective, **zBackTrust** must be considered an **"architecture" component** that allows universal integration with any application given that it is a web service. In this manner, this component, which offers signature and validation services, adheres to the necessary characteristics to be integrated into a service oriented architecture (**SOA**).

The zBackTrust solution allows electronic signing integrated into business processes to be quick, easy and independent, providing maximum security in document exchange using SOA services integrated into the company architectures. It facilitates high performance electronic signature processes in multiple environments: electronic communication, electronic invoicing, electronic authenticated comparison, signing of contracts, etc.

Thanks to the compatibility with the IBM 4764 cryptographic processor zBackTrust improves criptografic reliability and processing speed.

zBackTrust, (or BackTrust for System z) is a product developed under the J2EE technology for mainframe environments which facilitates electronic signature integration for applications developed in both mainframe and external systems using the DSS protocol. The services deployed are part of the paradigm of "cloud computing "

Maximum security guarantee

Advantages of the Solution

- Optimized solution for Linux on System z and z/OS
    - A P I JAVA for Linux on System z
    - Linux on System z with Tomcat or WebSphere
    - API JAVA for z/OS
    - z/OS with WebSphere or Weblogic

- zBackTrust separates security services from business processes with a common electronic signing infrastructure for all of the applications that require these functionalities.

- zBackTrust unifies the implementation of security functions and centralizes security management according to corporate policies

- zBackTrust guarantees system growth with new functionalities without affecting the development of the rest of the applications.

- zBackTrust guarantees the interoperability between applications because it closely follows the standards.

- zBackTrust minimizes development and maintenance costs, avoiding the repetition of programming code in multiple applications and platforms

- zBackTrust guarantees the ability to accept certificates from any European certification service provider

- zBackTrust allows recent regulations to be followed:
    - Electronic invoicing (Directive 2006/112/CE)
    - Electronic commerce (Directive 2000/31/CE)
    - Electronic signature (Directive 1999/93/EC)
    - eProcurement (Directive 2004/18/EC)

Standards

Platform Uses

Certificate Validation

It is common for a company to have different environments that must verify the validity of certain electronic certificates. zBackTrust (which includes a VA – Validation Authority) can be the common point for managing this functionality.

One specific case of this is shown by the new automatic tellers. Different banks are adapting their automatic tellers so that they can be used with a citizen electronic identification card, checking whether it has been revoked or not by accessing the OCSP services of the issuer.

In order to prevent the automatic tellers from directly accessing the Internet (with its associated risk), the preference is to have them access the centralized validation service of the entity, implemented with zBackTrust, where the OCSP revocation information or CRL from different certification service providers can be accessed.

eGoverment

eGoverment development laws establish a number of rights for citizens which translate into obligations for the public administrations, who shall implement infrastructures related to electronic documents management, which relay on the security and evidential proof of electronic signature and digital custody.

Electronic signatures and qualified certificates are required in all of these infrastructures. Therefore it is essential to use appropriate services such as those provided by zBackTrust for proper management of the electronic signatures of the citizens, government employees and the automated signature systems.

Electronic Commerce

Contracts can and be signed electronically preserving the value of proof in court. When managing electronic documents in the private sector, the use of electronic is key and deserves dedicated infrastructure in corporations, such as zBacktrust which manages most aspects of electronic documents.

Specifications

SOA service is based on the standard OASIS DSS (Digital Signature Services), AdESv1.0

Implementation of profiles:

- Digital Signature Service Core Protocols, Elements, and Bindings
- XML Timestamping Profile
- XML Advanced Electronic Signature Profiles (XAdES)
- Extension to manage PDF signatures

Implementation of XAdES ETSI TS 101 903 V1.3.2 (2006-03) standards with their formats XAdES BES-EPES, T, C, X, XL and A.

Support for PDF signature and TS 102 778

HSM

The use of **IBM 4764** and **IBM 4765** Signature Creation Secure Devices (already installed in zEnterprise systems) allows the creation of qualified electronic signatures. Other HSM are also supported.

Integration

Source code of zBacktrust Client supplied for developers is available in **.net** and **Java** environments, so they can deploy applications in any kind of workload (PowerPC, Linux on x86, Windows,…) accessing the centralized signature services.

Characteristics

Integration with other **BackTrust** products and **EADTrust** timestamping and validation services.

Access through standard **WebServices** (DSS) and **API BackTrust** for Linux on System z and z/OS.

Requests for **remote signatures, signature validation and completion of signatures (XAdES-XL)**.

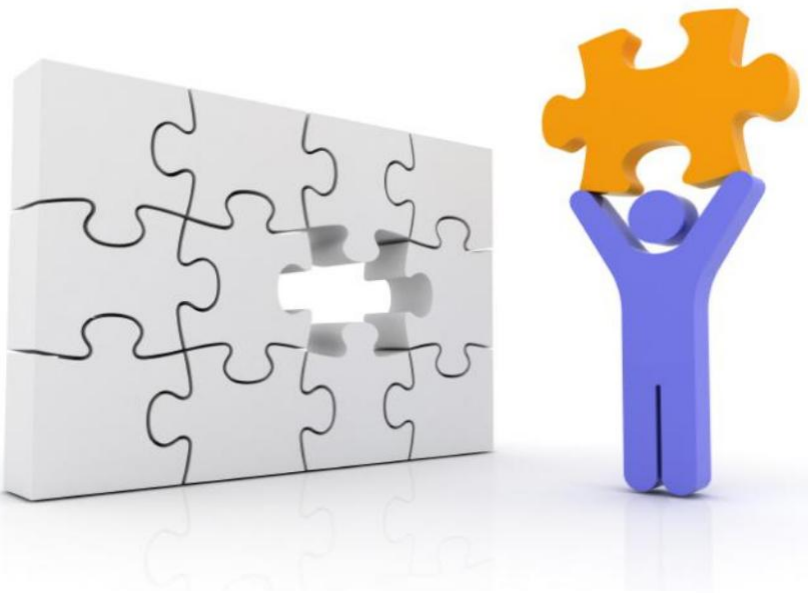Supported signature formats: **XMLDsig, XAdES (TS 101 903)**
Option for electronic signature in **PDF and PAdES (TS 101 778)**

Certificates

zBackTrust allows any Digital Certificate Service Provider to be used. Support for TSL TS 102 231 (Trust-service Status List)

Allows validation through CRLs and OCSP.

Note: Validation services with some Certification Service Providers are not free of charge.

Experience and professionalism

IBM and Albalia pool their experience to present a reliable and high performance solution that preserves the security and legal value of your company's documents at all times.

We have the necessary equipment and references to provide our customers with dynamic and effective solutions capable of meeting your needs and guaranteeing your success.

Our many years of experience in applications development and maintenance for leading companies, both in Spain and abroad, guarantees our reliability.

Available Through Selected partners

http://www.albalia.com
http://www.backtrust.net
+34902365612

http://www.insags.com
soluciones@insags.com
+34901116376