TrustedX

eSignature Platform

Description

Web services platform for managing e-signature processes:

- Support for advanced e-signature standards and formats.
- Batch signatures and batch verification.
- Trust management for multiple CAs, both public and corporate.
- Optional signature archiving service that guarantees non-repudiation over time.
- Signature mechanisms are isolated from the applications to provide the centralized management of e-signatures.
- Extendable and centralized logging that can be easily integrated with SIEM tools.

Benefits

Advanced e-signature integration

TrustedX supports the various advanced e-signature standards and enables integrating generation and verification processes into applications. The platform acts as a centralized repository, which means the applications can remotely use the keys and certificates stored by TrustedX without having to store them locally. This approach provides greater, audited control over the use of keys and simplifies deploying, maintaining and using the PKI through centralized management. The authentication and access control provides a range of mechanisms and trust levels, and the system can be easily integrated with other repositories for managing identities.

Semantic interpretation of signatures

TrustedX is the most complete signature platform of its kind. Multiple CAs can be managed, all signature formats are supported and all complexity related to managing trust is removed from the applications. The incorporated semantic services support obtaining all signer/signature data along with a trust level indicated using discrete values (4 levels) and labels (i.e., Government, Corporate, Finance, etc.).

Cost saving and flexible integration

The product can be quickly deployed thanks to its standardization and multiple integration options. It can be used (i) from user applications through plug-ins, (ii) as a Web service and (iii) by means of watch folders. The product incorporates an integration gateway that uses pipelines for the straightforward integration of data and common-task processing.

Centralized management, auditing and non-repudiation

TrustedX provides the centralized management of all signature policies, the preservation of electronic signatures, and logging and auditing. This allows the corporate control of the use of the cryptography, the effective management of recognized CAs/VAs and the transparent maintaining of signatures when required owing to the expiration of certificates and the renewal of cryptographic material.

TrustedX

eSignature Platform

Functions

TrustedX incorporates functions that provide a set of security and trust mechanisms as services. These services can be used in different formats as they support different integration strategies:

- **Java or .NET APIs**: Allows easily integrating electronic signature services in native Java applications and .NET (*).
- **SOAP/WS:** Using the OASIS DSS standard as an access protocol for Web services.
- **REST/WS, SOAP/WS:** Using TrustedX's integration gateway, which supports configuring traffic and data processing with an XML pipeline language.

The platform includes a Java Applet for signature integration scenarios with user smartcards in Web environments.

Platform functions are grouped into the following services:

- **Authentication and authorization.** Supports native authentication mechanisms based on passwords and digital certificates. New mechanisms can be incorporated using agents or the validation can be delegated to third-parties via RADIUS or LDAP/AD. It also supports identity federation via SAML.
- **Object and entity management.** Manages platform entities and objects. External repositories, such as user LDAP/AD, databases, files and HSMs, can be added for protecting private keys.
- **Certificate validation.** Provides PKI functions for validating certification chains and querying certificate status. Supports OCSP/CRL and customized mechanisms (e.g., databases and @firma platform).
- **Signature generation and verification.** Generates and verifies signatures in most standard e-document formats, including email and Web messaging. Supported formats include multiple signatures, signatures with time-stamps and long-term signatures.
- **Non-repudiation.** Allows extending a signature's validity over time by preserving its cryptographic reliability and incorporating the certification chain, information on certificate status at the time of signing and a time-stamp.
- **Auditing and accounting.** Uniformly and securely centralizes e-signature log data. The log system supports incorporating specific entries, which facilitates management with third-party tools.

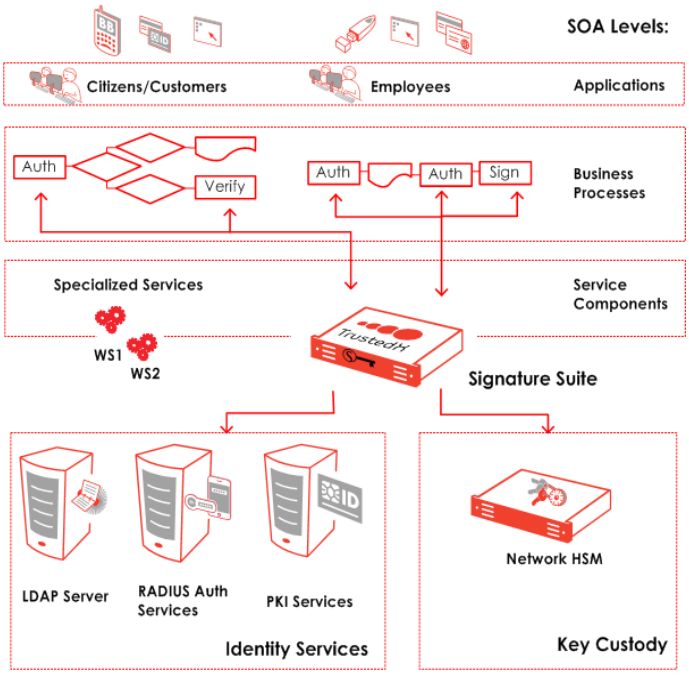
The following services can also be added:

- **Watched folders.** TrustedX watches the content of designated network folders and executes a series of actions (sign and verify) on all the files place in them.
- **Electronic signature custody.** Preserves the non-repudiability of the electronic signatures, by transparently interacting with the non-repudiation service and managing signature and e-document metadata.

(*) Please, check for availavility.

Architecture

The following figure illustrates the possible TrustedX architectures.



Technical specifications

- **Format:** Software appliance. Contact for more information about supported hardware or virtual machines.
- **Event monitoring:** Simple Network Management Protocol (SNMP).
- **Security services:** OASIS WS-Security, DSS (Digital Signature Service) and SAML, REST, SOAP and SSL/TLS.
- **Digital envelope standards:** PKCS #7, IETF CMS, ETSI TS 101733 - CAdES, W3C XML-DSig, W3C XML-Enc, ETSI TS 101903 - XAdES, Signature for PDF documents (IETF), S/MIME and ETSI TS 102 778) - PAdES.
- **Digital time-stamping support:** IETF TSP – RFC 3161.
- **Verification of digital certificate status:** Using CRLs, IETF OCSP protocol and customized mechanisms.
- **Database and directory access:** Oracle, Microsoft SQL Server and MySQL. LDAP directory access protocol.
- **Access to authentication services:** Authentication based on LDAP/AD and TMS compatible with RADIUS protocol.
- **Document manager support:** HTTP/WebDAV and XAM protocol.
- **HSM support:** PKCS #11 devices approved by Safelayer.
- **Network File Systems supported:** SMB / CIFS and NFS.
- **Integration with desktop applications:** Compatible with Microsoft CAPI and/or PKCS #11 for Windows environments.

Safelayer Secure Communications S.A.
Basauri, 17 Edif. Valrealty Edif. B Pl. Baja Izquierda Ofi. B
28023 Madrid (Spain)
Tel. +34 917 080 480 Fax +34 913 076 652

www.safelayer.com
World Trade Center (Edif. Sud- 4ª Planta). Moll de Barcelona s/n
08039 Barcelona (Spain)
Tel. +34 935 088 090 Fax +34 935 088 091

SAFELAYER