



www.safelayer.com

TrustedX

TRUSTED SERVICES PLATFORM

Description

TrustedX is a Web Services platform that provides trust and security mechanisms in Service-Oriented Architectures (SOA).

TrustedX is designed to:

- Make the security and trust services independent from business processes
- Provide a complete and uniform group of authentication, electronic signature and encryption functions
- Provide a common interoperability framework for the external security domains (e.g., for all the recognized CAs)
- Allow the classification and interpretation of the information trust level
- Centrally control event auditing
- Incorporate electronic signature archive and custody services to guarantee the non-repudiation of data

Benefits

• Focus on Service-Oriented Integration

TrustedX offers a solution to integrate the security functions in Service-Oriented Architectures (SOA) and XML. This is in line with the current trend in corporate information systems that is marking the end of the predominance of rigid software architectures.

• Centralized auditing and control

TrustedX centralizes trust policies as well as registration log and control. This approach allows forcing the appropriate use of cryptography in critical business processes and transparently managing and auditing the Certification and Validation Authorities (CAs and VAs).

• Greater business-process orientation

In decision-making processes, it is vital to determine the level of trust of the information, as well as its authors and their attributes. TrustedX takes the concept of business-orientation to a new level, greatly reduces the complexity of the processes, provides increased reliability and reduces the integration costs. All of which means TrustedX is faithful to the approach of recognizing new trust services and authentication mechanisms.

• Flexible integration of applications

As all integration methods are supported, different strategies can be used with TrustedX. TrustedX services can be invoked in three ways: (i) as Web services (SOAP or REST); (ii) via a Java API (integrated in the applications) that transparently consumes TrustedX services; or (iii) by accessing them from an integration gateway that does not require to modify applications and supports processing data in a queue (using the XML-Pipeline language).



TrustedX



www.safelayer.com

TrustedX

TRUSTED SERVICES PLATFORM

Functions

The TrustedX functions allow the management of security and trust in a standard and service-oriented way. These functions (accessible from the SOAP/WS or REST/WS protocols) are grouped in different services:

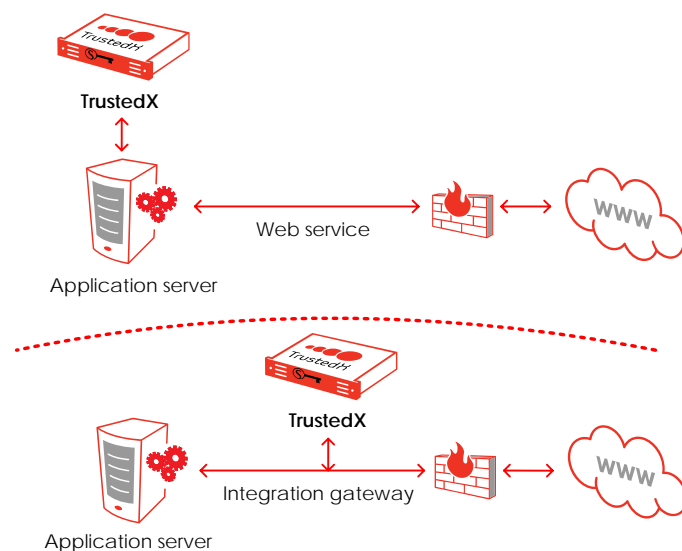
- Via the **authentication** and **authorization** services, the corporate applications and the external security domains exchange authentication and authorization information. This provides a single sign-on (SSO) mechanism under the OASIS defined standards.
- Thanks to the **digital certificate validation** service, multiple certification service providers can be recognized and the digital certificates information is made uniform. Standard certificate validation and customized mechanisms are also supported.
- The **electronic signature** service supports most signature formats for electronic documents, emails and web messaging. Supported formats include: multiple signatures, signatures with time stamps and long-term signatures (for validating a signature past the expiry date of the digital certificates).
- The **integration gateway** defines and connects successive XML data transformations (through interacting with platform services). The platform acts then as a trust gateway (between processes, application and networks) integrating applications in a non-intrusive manner.
- The **key management** service guarantees the secure administration of user/application keystores (on disk or HSM). This administration includes generating and importing keys, generating the certification requests and importing certificates.
- The **auditing and accounting** service uniformly and securely centralizes log information (generated by the platform's service components and through the consumption of services).
- The **entity and object management** service provides a uniform view (in XML format) of the objects and entities managed by the platform. Therefore, the data formats (XML, ASN.1, Text, etc.) and the information sources (LDAP, SQL, files, etc.) used by the platform are completely masked.

The following services can also be added:

- The **data encryption** service provides asymmetric key encryption for protecting electronic documents, e-Mails and Web Messaging. This service can also incorporate the key custody function to control access to encrypted data.
- The **archiving** and **electronic signature custody** component protects documents and maintains cryptographic reliability for later verification and retrieval. The archiving functions automatically process electronic signature metadata.

Architecture

The following figure illustrates the possible TrustedX architectures. The TrustedX functions can be used as a (i) trusted Web Service, (ii) a trusted gateway between applications (iii) or a combination of (i) and (ii) (this option is not shown in the figure).



Technical Specifications

- * **Format:** Hardware Appliance or Virtual Appliance. Contact Safelayer for more information.
- * **Web service infrastructure:** WSDL, UDDI and SOAP.
- * **Security services:** OASIS WSS, SSL/TLS, OASIS SAML and OASIS DSS electronic signature service. XKMS-based key management. Later versions will incorporate the OASIS XACML and WS-Trust/WS-Federation standards.
- * **Digital envelope standards:** PKCS #7, IETF CMS, ETSI TS 101733 - CAAdES, W3C XML-DSig, W3C XML-Enc, ETSI TS 101903 - XAdES, Signature for PDF documents (IETF) and S/MIME.
- * **Digital time-stamping support:** IETF TSP.
- * **Verification of the status of the digital certificates:** Via CRLs, IETF OCSP protocol and customized mechanisms.
- * **Database and directory access:** Oracle, Microsoft SQL Server and MySQL. LDAP directory access protocol.
- * **Custody service access:** Based on IETF RFC 4810.
- * **Document manager support:** HTTP/WebDAV and XAM protocol.
- * **HSM support:** PKCS #11 devices homologated by Safelayer.

Specifications subject to change without notice. All brand names are registered trademarks of their respective owners. Updated May 2009.



SAFELAYER SECURE COMMUNICATIONS S.A.

c/Basauri, 17 Edif. Valreality Edif. B Pl. Baja Izquierda Ofi. B 28023 Madrid (SPAIN) Tel.: +34 917 080 480 Fax: +34 913 076 652
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