



www.safelayer.com

TrustedX

DATA PROTECTION PLATFORM

Description

The TrustedX data protection platform is an EKM (Enterprise Key Management) solution that guarantees information protection and avoids data loss. Its main features are:

- Centralized custody of data encryption keys
- Key access control based on roles and policies
- Data encryption integrated with key custody functions
- Encrypted data archival in corporate or external repositories
- Parameterization of digital certificates and encryption algorithms. Classification of information based on policies
- Centralized auditing of access to keys and data
- Additional data authentication services using electronic signature functions

Benefits

• Centralized encryption key management

Regulations and the externalization of data centers increases the need for data encryption. Losing encryption keys can represent the loss of valuable assets. TrustedX avoids the risk of data loss by protecting encryption keys over time and monitoring access based on roles and policies.

• Encryption policy management

The level of data protection depends on the strength of the cryptographic algorithms and the keys used for encryption. TrustedX centrally and continually determines the required cryptographic parameters based on the encryption and decryption policies defined according to things such as the type of information, roles and applications.

• Centralized control and auditing

As TrustedX centralizes data protection, the control system and logs, the protection mechanisms and protected data access are always audited. These mechanisms are accessible from the platform's console or from a third party application connected to the TrustedX information system.

• Service-oriented strategic integration

TrustedX mechanisms for key custody, data encryption and archiving can be integrated as services in corporate information systems. The TrustedX platform is designed for Service-Oriented Architectures (SOA) and can be accessed via the SOAP and REST protocols.

• Flexible platform use

As TrustedX data protection services can be used via the Safelayer KeyOne Desktop application, the documents users have in their desktops can be encrypted and transparently integrated in the platform's data protection system.



TrustedX



www.safelayer.com

TrustedX

DATA PROTECTION PLATFORM

Functions

When information is encrypted using the TrustedX encryption, custody and archiving services, the data recipient groups are specified (by selecting access policies). The type of information being protected can also be specified. Data encryption algorithms can be symmetric or a combination of symmetric and asymmetric.

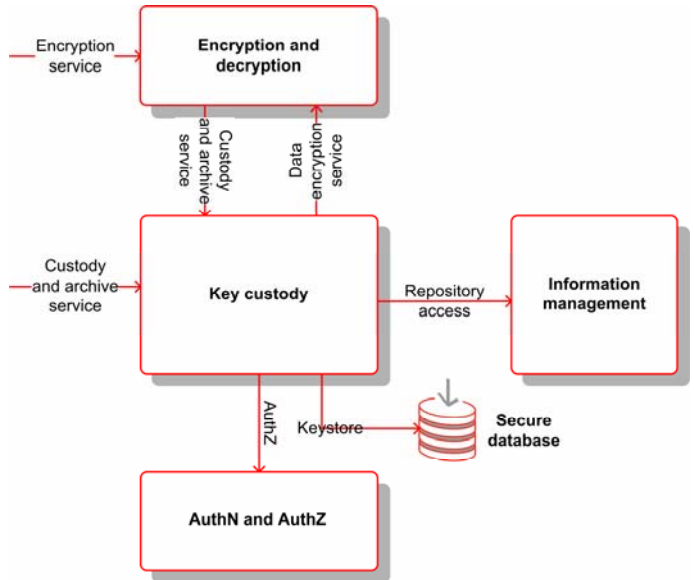
The following options are supported:

- (i) **Data encryption.** The encryption policies defined in TrustedX are applied to encrypt and decrypt data (for one or more recipients). The encrypted documents can be decrypted by the owners of the digital certificates used in the encryption process.
- (ii) **Key encryption and custody.** This option extends the data encryption service by protecting the encryption keys and using a data access control mechanism. It solves the problem arising from the expiry of encryption certificates in option (i). When the data is to be decrypted, authentication in TrustedX is required. The platform determines if requesters have the necessary access privileges. If they do, they are returned the decryption keys.
- (iii) **Encryption, key custody and data archiving.** This option, *to be incorporated in future versions of TrustedX*, integrates the key custody service with the archiving of encrypted documents in an external repository. Requesters authenticate in TrustedX to read, extract or delete archived data. The platform determines whether requesters have the necessary access privileges. If it finds they do, the requested operation is executed (e.g., data reading).

Before generating cryptographic material (as defined in the selected encryption policies) TrustedX downloads and transparently validates the digital certificates. Options (i), (ii) and (iii) can be invoked from an application. Option (ii) can be integrated with the Safelayer KeyOne Desktop application.

Architecture

The following figure illustrates how the applications interact with the encryption and key custody services of the TrustedX platform.



Depending on the operation required (data encryption, key custody or document archiving), the applications interact with the TrustedX 'encryption and decryption service' or 'key custody service'.

The 'key custody' service uses a cryptographically-protected database as a 'secure keystore'. This keystore, which can be kept on a HSM (not shown in the figure), protects all the encryption keys. The key custody service interacts with the TrustedX 'information management service' to access the HTTP/WebDAV/XAM or SQL document repositories (not shown in the figure).

As shown in the figure, the TrustedX authorization and authentication service (AuthN and AuthZ) controls the access to all the services.

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. Future versions will incorporate the OASIS XACML and WS-Trust/WS-Federation standards.
- * **PKI standards:** PKCS #7, IETF CMS, W3C XML-Enc and S/MIME. ITU-T X.509 v3 and digital certificate verification using CRL, IETF OCSP protocol and other customized mechanisms.
- * **Databases and directory:** Oracle, Microsoft SQL Server and MySQL. LDAP protocol based directory.
- * **Document manager support:** External DMS/ECM using 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. Valrealty 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