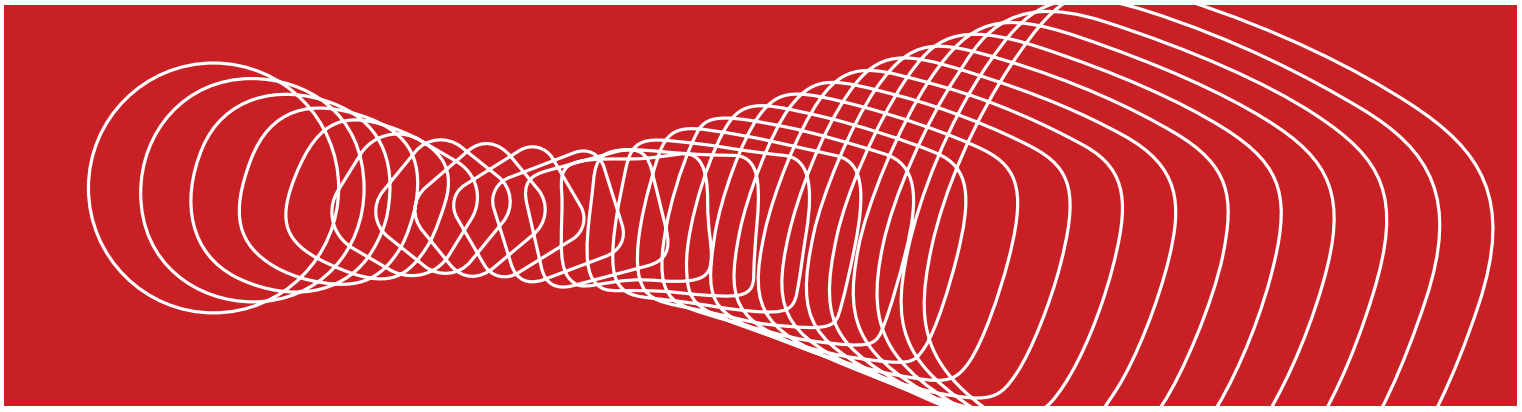


TrustedX

Encryption Key Management

Description

Encryption key management solution for data protection and encryption key custody:

- Encryption functions available as a Web service or in a desktop application
- Centralized custody of encryption keys with role-based access control
- Parameterization of encryption algorithms and policy-based data classification
- Centralized auditing of key and data accesses

Benefits

Centralized key management

Data encryption is becoming increasingly important owing to the new regulations and the externalization of data centers. TrustedX supports centrally managing all the encryption keys, protecting against the risk of losing data because due to unavailability of the encryption keys.

Encryption policy management

Allows centrally determining, at all times, the cryptographic parameters suitable for the encryption and decryption policies that are defined according to, for example, the type of information, roles or applications.

Centralized control and auditing

Centralized management of the data protection policies and the auditing and control system. Data accesses and data protection mechanisms are audited, which allows reacting quickly to security problems and preparing auditing reports.

Service-oriented integration

The encryption and key custody mechanisms are integrated in the corporate information systems as services. TrustedX is designed for service-oriented architectures (SOA) and is accessible via the SOAP/WS and REST/WS protocols.

Integration with the user's desktop

TrustedX's data protection services can be used via Safelayer's KeyOne Desktop application. Encrypting documents located in the user's desktop is transparently integrated into the platform's data protection system.

TrustedX

Encryption Key Management

Operation

When information is encrypted using TrustedX's custody or encryption services, the groups of recipients to receive the data are specified (by selecting access policies) and, optionally, the type of data protected is specified. The data encryption algorithms can be symmetric or a combination of symmetric and asymmetric.

The following options are supported:

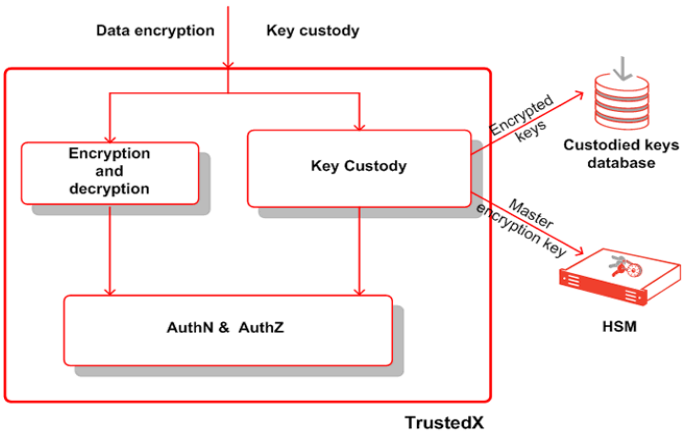
(i) **Encryption without key custody.** Data is encrypted and decrypted by applying the encryption policies defined in TrustedX (and for one or more recipients). The encrypted documents can be decrypted by the owners of the digital certificates used in the encryption.

(ii) **Encryption with key custody.** This mode extends the data encryption service with symmetric key custody. To decrypt data, the encryption key protected by TrustedX is required. Requesters need to authenticate in the platform to obtain the keys associated to their roles.

Options (i) and (ii) can be invoked from an application using the interfaces provided by the TrustedX platform (SOAP/WS, REST/WS) or by a Java API. Option (ii) can also be integrated in the desktop application, Safelayer KeyOne Desktop.

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 (encrypt data or store keys), the applications interact with the TrustedX encryption and decryption or key custody service.

The key custody service uses a secure keystore based on a cryptographically protected database (custodied keys database). That keystore is protected by a master encryption key managed by a NIST FIPS 140-2 level 3 HSM.

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

Technical Specifications

- **Format:** Software appliance. Contact for more information about supported hardware or virtual machines.
- **Web service infrastructure:** SOAP/WS, REST/WS, OASIS WSS, OASIS SAML, SSL/TLS.
- **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 and other customizable mechanisms.
- **Databases and directory:** Oracle, Microsoft SQL Server and MySQL. LDAP-based directory.
- **HSM support:** PKCS #11 devices approved by Safelayer.
- **Event monitoring:** Simple Network Management Protocol (SNMP).

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