TrustedX

Gestión de claves de cifrado

Descripción

Solución de gestión de claves de cifrado para la protección de datos y custodia de las claves de cifrado:

- Funciones de cifrado, disponibles como servicio web o desde una aplicación de escritorio
- Custodia centralizada de claves de cifrado, con control de acceso basado en roles
- Parametrización de algoritmos de cifrado y clasificación de la información basada en políticas
- Auditoría centralizada de los accesos a claves y la información

Beneficios

Gestión centralizada de las claves

El cifrado de datos es una necesidad creciente debido a las nuevas regulaciones y la externalización de centros de datos. TrustedX permite gestionar de forma centralizada todas las claves de cifrado, protegiendo contra los riesgos de pérdida de datos debidos a no disponer de las claves de cifrado.

Gestión de las políticas de cifrado

Permite determinar de forma centralizada, en todo momento, los parámetros criptográficos apropiados en base a políticas de cifrado y descifrado que se establecen, por ejemplo, en función del tipo de información, roles o aplicaciones.

Control y auditoría centralizados

Gestión centralizada de las políticas de protección de datos y del sistema de control y auditoría. De este modo, los mecanismos de protección y accesos a los datos son auditados, permitiendo la reacción rápida a problemas de seguridad y presentación de informes de auditoría.

Integración orientada a servicios

Los mecanismos de cifrado y de custodia de claves se integran en los sistemas de información corporativos como servicios. TrustedX está diseñado para Arquitecturas Orientadas a Servicios (SOA) y es accesible mediante protocolos SOAP/WS o REST/WS.

Integración con el escritorio de usuario

Los servicios de protección de datos de TrustedX pueden usarse de forma integrada con la aplicación KeyOne Desktop de Safelayer. De este modo, el cifrado de documentos situados en el escritorio de los usuarios se integra de forma transparente con el sistema de protección de datos de la plataforma.

TrustedX

Gestión de claves de cifrado

Funcionamiento

Cuando se cifra la información mediante los servicios de cifrado o custodia de TrustedX, se indican los grupos de receptores a los que se destinan dichos datos (mediante la selección de políticas de acceso) y, opcionalmente, el tipo de información protegida. Los algoritmos de cifrado de datos pueden ser simétricos o una combinación de simétricos y asimétricos.

Este funcionamiento soporta las siguientes variantes:

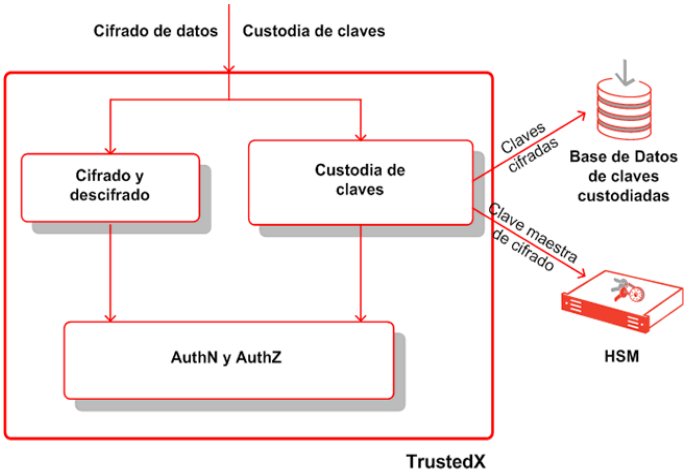
(i) Cifrado sin custodia de claves. Los datos se cifran y descifran aplicando las políticas de cifrado definidas en TrustedX (y para uno o varios receptores). Los documentos cifrados podrán ser descifrados por los titulares de los certificados digitales utilizados para el cifrado.

(ii) Cifrado con custodia de claves. Esta modalidad extiende el servicio de cifrado de datos mediante la custodia de las claves simétricas. De esta forma, cuando se requiera descifrar los datos se deberá obtener previamente la clave de cifrado custodiada por TrustedX. Para esto, la plataforma autenticará al solicitante y le entregará las claves en función de su rol.

La variantes (i) y (ii) se pueden invocar desde una aplicación empleando las interfaces que proporciona la plataforma TrustedX (SOAP/WS, REST/WS), o bien un API Java. Además, la variante (ii) se puede integrar con la aplicación de escritorio de Safelayer KeyOne Desktop.

Arquitectura

La siguiente figura muestra las interacciones de las aplicaciones con los servicios de cifrado y custodia de claves de la plataforma TrustedX.



Según se requiera cifrar datos o custodiar claves, las aplicaciones interactúan con el "servicio de cifrado y descifrado" o con el "servicio de custodia de claves" de TrustedX.

El servicio de "custodia de claves" dispone de un "almacén de claves seguro" sobre una base de datos protegida criptográficamente. Dicho almacén está protegido por una clave maestra de cifrado gestionada por un HSM FIPS 140-2 Nivel 3.

Tal como ilustra la figura, la gestión del control de acceso a todos los servicios es responsabilidad del "servicio de autenticación y autorización" de TrustedX (AuthN y AuthZ).

Características técnicas

- **Formato:** Software appliance. Consultar para más información sobre entornos hardware o virtuales homologados.
- **Infraestructura de servicios web:** WS/SOAP, WS/REST, OASIS WSS, OASIS SAML, SSL/TLS.
- **Estándares de PKI:** PKCS #7, IETF CMS, W3C XML-Enc y S/MIME. ITU-T X.509 v3 y verificación de certificados digitales mediante CRL, protocolo OCSP de IETF y otros mecanismos personalizables.
- **Bases de datos y directorio:** Oracle, Microsoft SQL Server o MySQL. Directorio basado en protocolo LDAP
- **Soporte de HSM:** Dispositivos PKCS #11 homologados por Safelayer.
- **Monitorización de eventos:** 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