TrustedX - Gestión de claves de cifrado

Whitepaper

CONTENIDO

Introducción

Actualmente, las organizaciones utilizan cada vez más el cifrado, como mecanismo para proteger los datos que utilizan las aplicaciones. Las razones que están impulsando el uso creciente de esta tecnología son básicamente las siguientes:

- **Una mayor exposición al riesgo** de los datos debida, por ejemplo, a la progresiva externalización de los centros en los que estos datos se almacenan.
- **La necesidad de cumplir regulaciones** que obligan a proteger la confidencialidad de determinados datos.

La protección de datos mediante claves simétricas, plantea el problema de la gestión y custodia de las claves utilizadas. Por ejemplo:

- En el supuesto de pérdida de una clave de cifrado quedarán inutilizados los datos que se hubieran cifrado con ella, que ya no podrán recuperarse en claro.
- Cuando el control de acceso a la clave de cifrado no es adecuado la clave está expuesta a copias, por lo que los datos cifrados están desprotegidos con independencia de la fortaleza de los algoritmos criptográficos utilizados.

Cifrado y gestión de claves simétricas con TrustedX

La protección de datos de TrustedX abarca el cifrado y descifrado de datos y la gestión centralizada de claves simétricas.

El cifrado y el descifrado de datos pueden ser de dos tipos:

- **Simétrico**: los datos se cifran y descifran con una clave secreta.
- **Asimétrico**: los datos se cifran con una clave secreta y ésta, a su vez, se cifra con las claves públicas de uno o varios destinatarios (digital envelope). De este modo, los destinatarios podrán descifrar los datos, descifrando la clave secreta previamente, con sus respectivas claves públicas

La gestión de claves simétricas incluye, por lo tanto, la generación, el almacenamiento de las claves (custodia) y la recuperación de las claves cuando sea necesario acceder a los datos cifrados.

El principal valor de TrustedX reside en que permite realizar todas estas operaciones de forma centralizada, constituyendo una solución para la protección de datos que las aplicaciones pueden usar como servicios SOAP/WS y REST/WS.

La centralización de estas operaciones, accesibles como servicios de seguridad, proporciona las siguientes ventajas:

- **Posibilita el control de acceso dinámico (basado en roles) a los datos que sean cifrados de forma simétrica por los diferentes sistemas de la organización**. Al centralizar el almacenamiento y

recuperación de las claves simétricas que se emplean en las operaciones de cifrado, los sistemas que realizan estas operaciones quedan liberados de tener que distribuir las claves a todos los destinatarios a quienes se autoriza a leer los datos. Simplemente basta con que utilicen la operación de almacenamiento (custodia). A partir de entonces, el servicio de gestión de claves simétricas es quien controla el acceso a las claves basado en su rol corporativo, en consecuencia, cualquier usuario que quiera recuperarlas, deberá acreditar una identidad a la que se haya asignado el rol requerido.

- **Posibilita el gobierno de la gestión de claves simétricas y de todos los procesos de cifrado y descifrado de datos**. La centralización permite aplicar políticas de alcance corporativo que regulen cómo deben realizarse cada uno estos procesos. Se puede establecer, por ejemplo, el tipo de clave con la que se deberán proteger las claves simétricas custodiadas. Del mismo modo, se puede establecer el algoritmo de cifrado que tendrá que utilizarse para proteger unos datos en función del grado de confidencialidad que se atribuya a los mismos mediante etiquetas de seguridad.
- **Posibilita la auditoría de la gestión de claves simétricas y del cifrado y descifrado de datos.** La centralización permite que los eventos correspondientes a la generación, custodia y recuperación de claves simétricas queden anotadas en los mismos registros de log, al igual que los eventos correspondientes a la realización de operaciones de cifrado y descifrado de datos. Esto permite supervisar el uso que hace la organización de estas operaciones y, por tanto, someterlas a vigilancia de un modo efectivo.

CAPÍTULO 1

Descripción de la gestión de claves de cifrado

TrustedX proporciona una plataforma para la protección de datos y la gestión de claves de cifrado que está disponible en formato appliance, que puede ser físico (hardware) o virtual (software). Dispone de una consola de administración gráfica y de un intérprete de comandos (shell) que permiten administrar la configuración de todo el sistema.

Esta plataforma consta de los siguientes servicios:

- Servicio de cifrado y descifrado de datos
- Servicio de gestión de claves simétricas

Las funciones que ofrecen estos servicios se pueden invocar desde una aplicación empleando las interfaces Web que proporciona la plataforma (SOAP/WS, REST/WS), o bien un API Java.

Por otra parte, el acceso al servicio de gestión de claves simétricas se puede realizar de forma transparente desde el escritorio de usuario con la aplicación de cifrado de datos KeyOne Desktop de Safelayer.

Autenticación y autorización

Todos los servicios de TrustedX están protegidos mediante control de acceso (autenticación y autorización), para lo cual TrustedX se apoya en el servicio de autenticación y autorización que incorpora la plataforma.

Utilizando la consola de administración gráfica se puede establecer el conjunto de mecanismos de autenticación que son aceptados. Con respecto al empleo de estos mecanismos se distinguen los siguientes escenarios:

- **La validación de las credenciales es realizada por el servicio de autenticación y autorización de TrustedX** (e.g. nombre de usuario y contraseña, certificados de cliente recibidos en conexiones TLS/SSL establecidas directamente con TrustedX).
- **El servicio de autenticación y autorización recibe unas credenciales que no han sido validadas y delega su validación en un servicio o validador de autenticación externo** (RADIUS, LDAP, Active Directory). Un ejemplo de este caso es la autenticación en TrustedX mediante la validación de contraseñas de un sólo uso (OTP) accediendo a un servidor de autenticación RADIUS.
- **La validación de las credenciales es realizada total o parcialmente, y de manera previa, por un agente de autenticación externo**. A continuación, el agente proporciona la identidad del cliente al servicio de autenticación y autorización (en el caso de que el agente haya validado totalmente las credenciales) o las credenciales mismas, para que el servicio de autenticación y autorización las termine de validar (en el caso de que el agente las haya validado sólo parcialmente).

Servicio de cifrado y descifrado de datos

El servicio de cifrado y descifrado de datos sirve para cifrar y descifrar datos de forma centralizada (en servidor).

Los mensajes de interacción con el servicio tienen una estructura deliberadamente flexible que varía dependiendo del formato en el que se quieran representar los datos cifrados o del que se quieran extraer los datos en claro. De este modo, se distinguen los siguientes perfiles de acceso al servicio:

- **Perfil CMS/PKCS#7**: permite cifrar unos datos cualesquiera y encapsularlos dentro de una estructura CMS/PKCS#7 del tipo EnvelopedData (si el cifrado es asimétrico) o EncryptedData (si el cifrado es simétrico). También permite descifrar los datos que encapsule una estructura CMS/PKCS#7 de cualquiera de los tipos anteriores.
- **Perfil XML-Enc**: permite cifrar unos datos que estén en formato XML y representar el resultado también en XML, encapsulándolos dentro de un elemento <EncryptedData>, tal como se define en [XML-Enc]. Del mismo modo, permite recuperar en claro, los datos en formato XML que encapsule un elemento <EncryptedData>. Soporta tanto el cifrado simétrico como el asimétrico.
- **Perfil S/MIME**: permite cifrar una entidad MIME (e.g. un mensaje de correo electrónico) y encapsularla dentro de otra que se devuelve como resultado. Concretamente, la entidad MIME original se encapsula primero dentro de una estructura CMS (S/MIME v3) o PKCS #7 (S/MIME v2) del tipo EnvelopedData y, a continuación, dicha estructura se representa en formato S/MIME. Es decir, se codifica en base64 y se pone en el cuerpo de una entidad MIME que tenga los siguientes campos en su cabecera:

  Content-Type: application/pkcs7-mime; smime-type=enveloped-data.
  Content-Transfer-Encoding: base64

  Del mismo modo, permite recuperar, en claro, una entidad MIME que se encuentre cifrada dentro del cuerpo de otra que la encapsula.
- **Perfil WS-Security**: permite cifrar cualquier elemento de un mensaje SOAP (o su contenido) y devolver como resultado otro mensaje SOAP cuyo formato cumpla con la especificación [WSS]. De este modo, en el mensaje SOAP que se devuelva como resultado, el elemento (o el contenido) que se haya cifrado estará encapsulado dentro de un elemento <EncryptedData>. Además, la cabecera <Security> de dicho mensaje incluirá un elemento <EncryptedKey> que contendrá la clave simétrica que se haya utilizado para realizar el cifrado, protegida, a su vez, por la clave pública del destinatario del mensaje. Del mismo modo, permite recuperar, en claro, un mensaje SOAP que tenga uno o varios de sus elementos (o el contenido de éstos) cifrados y, por lo tanto, encapsulados cada uno de ellos, dentro del correspondiente elemento <EncryptedData>.

Servicio de gestión de claves simétricas

El servicio de gestión de claves simétricas es un servicio que permite generar, almacenar (custodiar) y recuperar claves simétricas de forma centralizada.

Las claves se gestionan de acuerdo a los criterios que establece una determinada política. Por ejemplo:

- El tipo de clave que debe utilizarse para proteger las claves custodiadas.
- Si la clave de custodia se tiene que proteger mediante un HSM.
- Si se tiene que utilizar un HSM para generar las claves simétricas

Utilizando este servicio, una entidad cualquiera (usuario, aplicación) puede cifrar un documento con una clave simétrica y enviarla después al servicio de gestión de claves simétricas para que la custodie y la entregue sólo a los usuarios de un determinado círculo de confianza. Esto proporciona las siguientes ventajas:

- La entidad no tiene que preocuparse de custodiar la clave de cifrado. Es TrustedX quien realiza esta labor.
- La entidad no tiene que preocuparse de enviar la clave de cifrado a los destinatarios del documento. TrustedX se encarga de gestionar quién puede recuperar la clave para descifrar el documento y se apoya, para ello, en el servicio de autenticación y autorización de la plataforma, el cual proporciona un control de acceso a las claves basado en la pertenencia a grupos.

En referencia a las claves simétricas de cifrado, éstas pueden ser generadas por una aplicación externa o por la propia plataforma TrustedX.

KeyOne Desktop

KeyOne Desktop es una aplicación de escritorio que permite realizar diferentes operaciones criptográficas sobre los ficheros del sistema de archivos. Estas operaciones aparecen como opciones del menú contextual que se muestran cuando se hace clic con el botón derecho del ratón encima de un fichero concreto.

En particular, KeyOne Desktop permite cifrar ficheros, tanto de forma simétrica como asimétrica. Cuando cifra de forma simétrica, la clave de cifrado puede ser generada por KeyOne Desktop o por TrustedX, dependiendo de cuál sea la configuración de KeyOne Desktop.

En cualquier caso, KeyOne Desktop solicitará a TrustedX que custodie la clave que vaya a utilizar y obtendrá como resultado un identificador que le permitirá recuperarla más adelante para realizar el descifrado.

Este identificador se guarda dentro de la estructura CMS mediante la que KeyOne Desktop codifica los datos cifrados. Así, cuando el usuario solicite la operación de descifrado, KeyOne Desktop será capaz de obtener el identificador de la clave correspondiente y solicitar la clave de descifrado a TrustedX.

CAPÍTULO 2

Arquitectura y funcionamiento

Las aplicaciones que quieren cifrar o descifrar datos acceden a las operaciones del servicio de cifrado y descifrado de datos de la plataforma (encrypt, decrypt). En el caso de que deseen realizar un cifrado asimétrico deberán indicar en el mensaje de acceso al servicio los destinatarios para quienes se quiere cifrar la información. Cada uno de ellos podrá recuperar posteriormente la información en claro solicitando la operación de descifrado del servicio. En el caso de que las aplicaciones deseen realizar un cifrado o descifrado simétrico, deberán indicar en el mensaje de acceso al servicio la clave simétrica que tenga que utilizarse para realizar la operación.

Por lo que respecta a la gestión de claves simétricas, se soporta la generación (genKey), el almacenamiento (putKey) y la recuperación (getKey) de claves simétricas. Las claves custodiadas se almacenan en una base de datos (u otro tipo de repositorio) cifradas con la clave de una determinada política de gestión de claves simétricas (clave de custodia), y a cada una de ellas se le asocia un recurso que deberá estar registrado en TrustedX. A su vez, cada clave de custodia se guarda en el almacén de claves de la política a la que pertenece y éste se basa, habitualmente, en un dispositivo HSM (Figura 3-1).

Tanto el acceso a las operaciones del servicio de cifrado y descifrado (encrypt, decrypt) como a las operaciones del servicio de gestión de claves simétricas (genkey, putkey, getkey), está controlado por el servicio de autenticación y autorización de TrustedX (authn, authz). En el caso particular de la recuperación de las claves custodiadas, el servicio de autenticación y autorización controla no sólo que el usuario, en función de su rol, tenga permisos para ejecutar la operación del servicio (getKey), sino que también tenga acceso a la clave simétrica que pretenda recuperar.

La plataforma genera un log detallado con todos los eventos que ocurren en ella como consecuencia del consumo de los servicios y la administración de la configuración. La información de este log se puede guardar en bases de datos y en servidores Syslog.

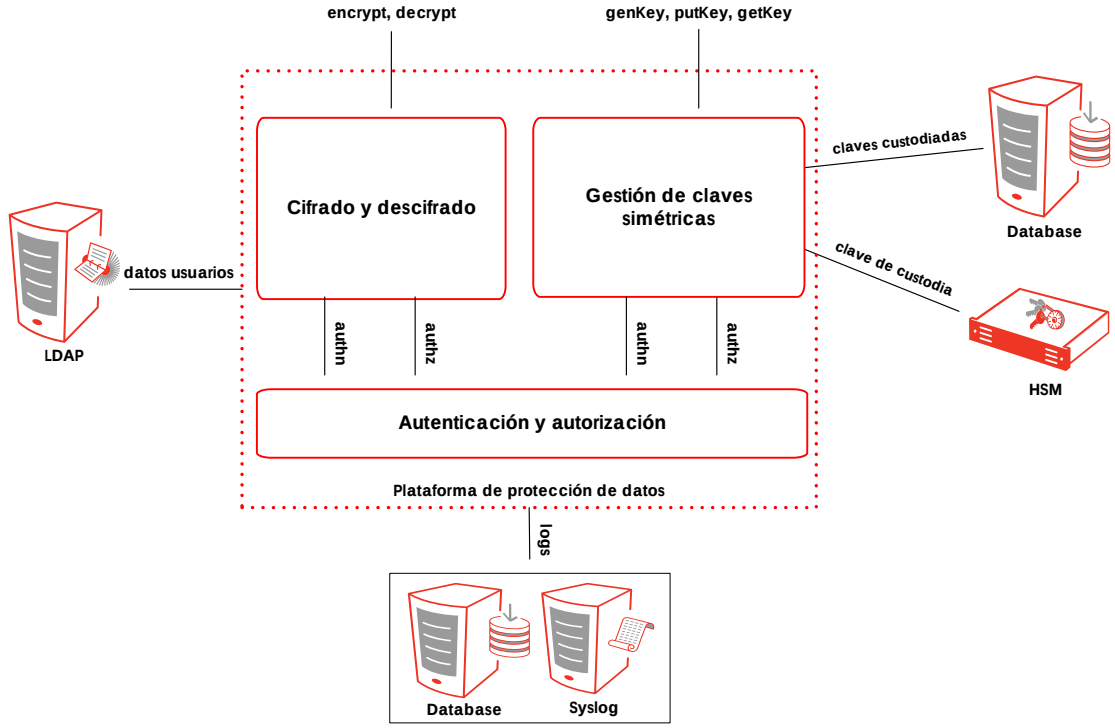

Figura 2-1. Cifrado, descifrado y gestión de claves simétricas

CAPÍTULO 3

Administración

La administración de TrustedX abarca dos dominios claramente diferenciados. Por un lado, la administración de la configuración del sistema propiamente dicha y el acceso a los logs que generan los servicios. Por otro lado, la administración "del appliance", es decir, de la plataforma de ejecución sobre la que funciona TrustedX:

- Con respecto a la primera, se realiza mediante una aplicación web que forma parte del sistema y que dispone de una interfaz gráfica desde la que se puede gestionar la configuración de TrustedX y consultar sus logs.
- Con respecto a la segunda, se realiza mediante una aplicación que se denomina intérprete de comandos (o simplemente shell) a la que se puede acceder desde el terminal físico del appliance o desde un terminal remoto que se conecte al mismo por SSH.

Consola de administración gráfica

La consola de administración gráfica es una aplicación web que permite administrar y acceder a toda la información que maneja TrustedX, utilizando un navegador.

- **Gestión de entidades finales:** permite registrar usuarios, aplicaciones y servicios como entidades finales y administrar sus datos. También permite definir grupos de entidades finales.
- **Gestión de políticas de autenticación y autorización:** permite definir las políticas de autenticación y autorización con las que se controlará el acceso de las entidades finales a los servicios de TrustedX.
- **Gestión de políticas de cifrado y descifrado:** permite definir y modificar las políticas que se aplicarán para cifrar y descifrar datos.
- **Gestión de políticas de gestión de claves simétricas:** permite definir y modificar las políticas que se aplicarán para administrar las claves simétricas que se custodien (Figura 4-2).

Figura 3-2. Gestión de políticas de gestión de claves simétricas.

- **Gestión de la configuración de los servicios:** permite definir la configuración de los distintos servicios de la plataforma.
- **Gestión de la configuración de las conexiones con repositorios:** permite definir la configuración de las conexiones mediante las que se accederá a los distintos repositorios (bases de datos, servidores LDAP) que utiliza el sistema.
- **Gestión de la configuración de acceso a dispositivos HSM:** permite definir la configuración que se utilizará para acceder a los dispositivos HSM que utilice la plataforma.
- **Consulta de logs y auditoría:** permite consultar los eventos que generan por todos los componentes de servicio de la plataforma.

Intérprete de comandos

Esta aplicación que, como su nombre indica, tiene un interfaz de usuario en línea de comandos, sirve para administrar el sistema sobre el que se ejecuta TrustedX (Figura 4-3). Se trata de un componente que entre otras cosas, permite lo siguiente:

- Instalar el archivo de licencia en el sistema de archivos del appliance.
- Configurar la interfaz de red del appliance
- Instalar los drivers y establecer la configuración de cliente que permitan a TrustedX acceder a los elementos que conforman su entorno operacional (bases de datos, dispositivos HSM, etc).

Los comandos que reconoce esta aplicación están organizados jerárquicamente según una estructura de varios niveles. Todos los comandos tienen una sintaxis muy similar y ésta se puede consultar mediante el comando help. Por otro lado el tabulador permite autocompletar los distintos comandos y mostrar sus opciones.

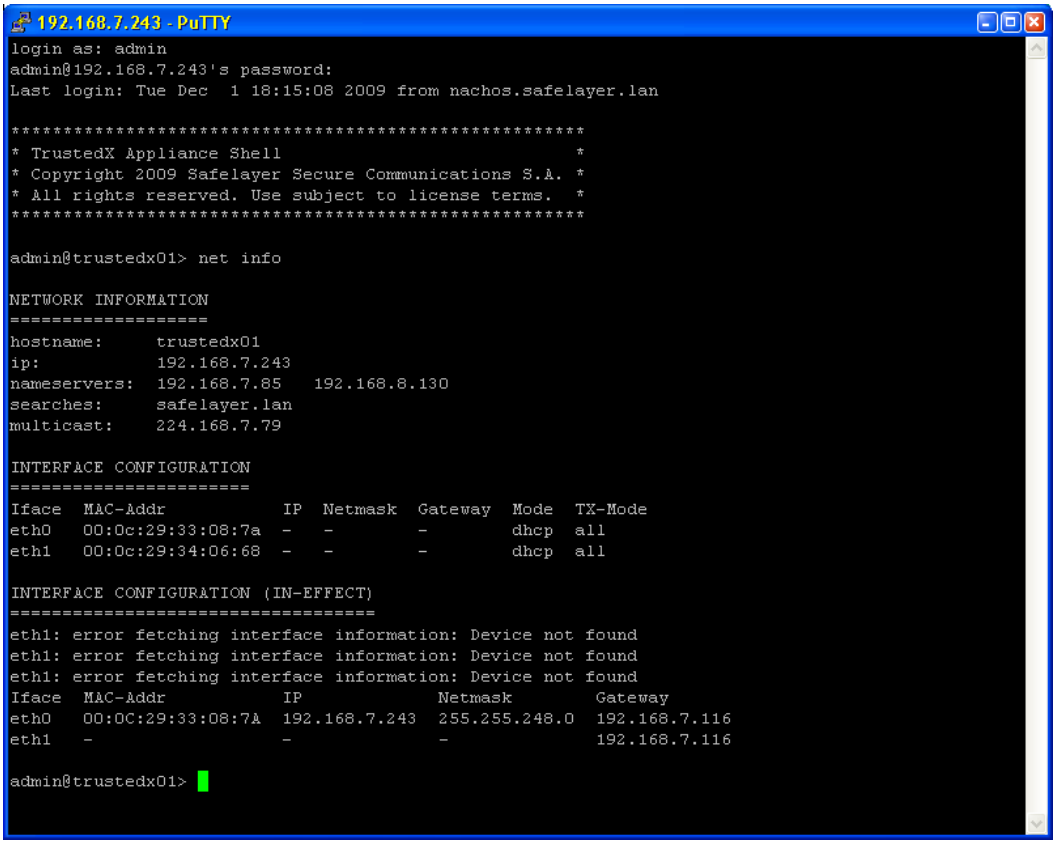

Figura 3-3. Consola de administración en línea de comandos

Alta disponibilidad

Los servicios de TrustedX pueden desplegarse en alta disponibilidad de manera que estén accesibles de forma ininterrumpida. La arquitectura de este despliegue se muestra en la Figura 4-4.

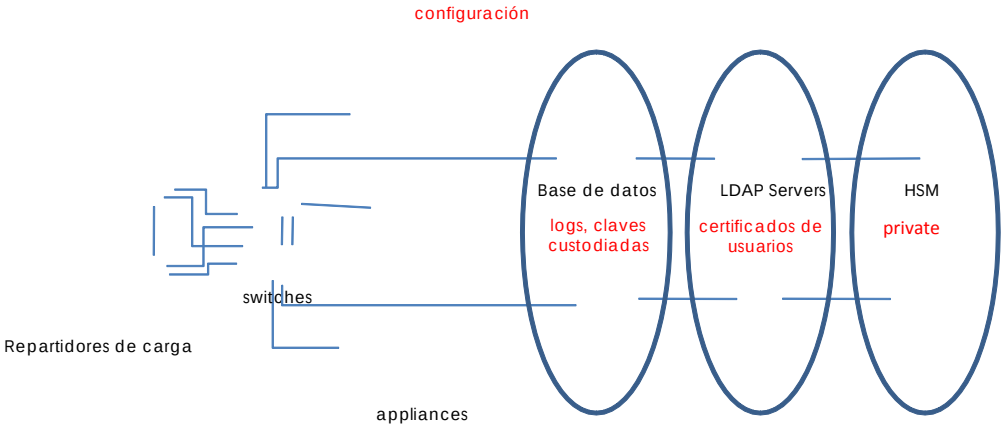

Figura 3-4. Despliegue de TrustedX en alta disponibilidad

Esta arquitectura dispone de un cluster formado por dos o más appliances de TrustedX a los que un repartidor de carga, también en alta disponibilidad (e.g. configuración activo/pasivo), reparte las peticiones

que recibe de los clientes. Por otro lado, todos los sistemas y recursos (base de datos de logs, servidores LDAP, dispositivos HSM, etc) a los que accede TrustedX deberán estar en alta disponibilidad.

Monitorización y auditoría

La monitorización de TrustedX se realiza mediante un agente SNMP y tiene como finalidad garantizar el correcto funcionamiento de la plataforma Figura 4-5. El producto de monitorización externo del que se disponga la organización recibirá avisos (traps) de este agente, en el preciso instante en que se produzca una situación excepcional.

Además, el producto de monitorización externo también realizará peticiones al agente SNMP (probing) para detectar fallos durante periodos de aparente inactividad. Con la información obtenida el producto de monitorización permitirá la elaboración de informes para el departamento de sistemas TI de la organización.

Por lo que respecta a la auditoría, ésta se realiza a partir del envío a un sistema externo (e.g. Splunk), mediante Syslog (Figura 4-5), de toda la actividad que tenga lugar en la plataforma, con la finalidad de generar informes de negocio y de compliance.

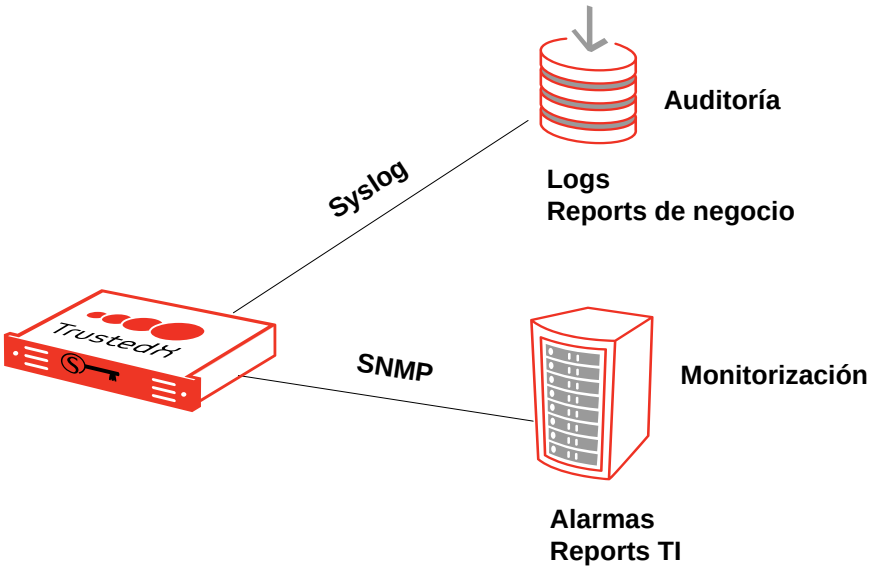

Figura 3-5. Monitorización y auditoría de TrustedX

APÉNDICE A

Estándares y algoritmos de cifrado soportados

Este apéndice contiene la relación de estándares y de algoritmos de cifrado que soporta TrustedX .

Estándares

TrustedX soporta los siguientes estándares:

Referencia	*Estándar*
[CMS]	Cryptographic Message Syntax, IETF RFC 5652
[LDAP]	Lightweight Directory Access Protocol
[PKCS#7]	PKCS #7: Cryptographic Message Syntax, version 1.5. IETF RFC 2315
[SMIME2]	S/MIME Version 2 Message Specification, IETF RFC 2311
[SMIME3]	S/MIME Version 3 Message Specification, IETF RFC 2633
[SOAP]	Simple Object Access Protocol Version 1.1, W3C. May 2001
[SSL/TLS]	Secure Socket Layer / Transport Layer Security
[X509]	ITU-T Recommendation X509v3
[XML-Enc]	XML Encryption Syntax and Processing. W3C Recommendation 10 December 2002
[WSDL]	Web Service Description Language (WSDL) 1.1, W3C. March 2001
[WSS]	OASIS Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) February 2006

Algoritmos de cifrado

TrustedX soporta los siguientes algoritmos de cifrado:

- RC2
- DES

- Triple DES
- AES-128
- AES-192
- AES-256
- RSA

TrustedX Gestión de claves de cifrado

Safelayer Secure Communications, S.A.

80 90

Fax: +34 93 508 80 91

Web: www.safelayer.com

Edificio Valrealty C/ Basauri, 17 Edifico B Pl. Baja Izq. Of. B 28023 Madrid (SPAIN) Tel.: +34 91 7080480 Fax: +34 91 3076652
World Trade Center (Edif. S-4), Moll de Barcelona S/N 08039 Barcelona (SPAIN) Tel.: +34 93 5088090 Fax: +34 93 5088091