
# TrustedX - Plataforma de firma electrónica

## Whitepaper

# CONTENIDO

# Introducción

La importancia estratégica de la firma electrónica es cada vez mayor como parte del proceso de mejora de la eficiencia y el esfuerzo de eliminación del formato en papel. Por otra parte, la directiva Europea 1999/03/EC de firma electrónica establece el marco jurídico común para el uso de las firmas electrónica, por lo que es equiparable legalmente a la manuscrita.

Las soluciones de seguridad de Safelayer se basan en tecnología PKI y certificados digitales. Se trata de una tecnología ampliamente adoptada por la industria en numerosas aplicaciones y usada, por ejemplo, para la implementación de mecanismos de **firma electrónica reconocida y/o avanzada**. La tecnología PKI también es la base de los mecanismos de **autenticación** basados en certificados, caracterizados por el alto nivel de confianza que ofrecen.

Las soluciones de firma electrónica de Safelayer destacan por su flexibilidad en la integración de mecanismos de firma electrónica y autenticación en los procesos corporativos y por su diseño para arquitecturas orientadas a servicios. Aportan diferentes niveles de modularidad y escalabilidad, admitiendo diferentes configuraciones en función del ámbito de uso:

- **Entornos corporativos**. Configuración orientada al despliegue rápido de la firma electrónica en el entorno empresarial. Los empleados pueden firmar de forma inmediata desde sus aplicaciones de escritorio y las aplicaciones simplemente escribiendo ficheros en carpetas de red.
- **Prestadores de servicios de confianza.** Configuración adecuada para entornos heterogéneos y/o para la prestación de servicios de confianza relacionados con la firma electrónica. Ofrece mucha flexibilidad de integración mediante servicios web SOAP (OASIS DSS y WS-Security), del estilo REST o APIs Java.

# TrustedX de Safelayer

TrustedX es un producto de Safelayer que aporta un conjunto completo de mecanismos de seguridad que se pueden acceder como servicios, o bien, desde unos módulos de integración específicos de determinadas aplicaciones y entornos. A nivel de sistemas, TrustedX proporciona una **plataforma de servicios de seguridad PKI** gestionados de forma centralizada y un sistema de auditoría de los mecanismos de firma electrónica y autenticación que usan las aplicaciones.

Los aspectos más destacados de TrustedX son los siguientes:

- **Interoperabilidad probada y soporte de estándares**

Amplio soporte de los estándares de firma electrónica: CMS, PKCS #7, CAdES, S/MIME, XML-DSig, XAdES, PDF Signature y PAdES.

Safelayer ha participado en todas las pruebas PlugTests que organiza ETSI (Instituto Europeo de Estándares de Telecomunicaciones) desde la primera edición en 2007.

- **Disponible en formato de appliance hardware y virtual**

Es el primer producto de su categoría que se distribuye tanto en formato de appliance físico (para hardware homologado por Safelayer), como de appliance virtual (para entornos de máquina virtual).

El producto TrustedX contiene todo el software necesario para su instalación, mantenimiento y administración.

- **Integración flexible y protección de la inversión**

Incluye módulos y APIs específicas de integración. Soporta los mecanismos de integración adoptados por la industria, tales como SOAP (mediante los estándares DSS y WS-Security de OASIS) y REST.

Incluye funciones de interpretación semántica parametrizables que se utilizan en el procesado y evaluación de la confianza de la información, evitando lógica adicional y complejidad a las aplicaciones.

- **Escalabilidad en funcionalidad y prestaciones**

La plataforma se puede ampliar con el servicio de custodia de firmas digitales y/o servicios que aportan funciones de protección de datos y gestión de claves de cifrado.

Puede incorporar nuevos mecanismos de autenticación mediante agentes, o delegar la validación de credenciales en terceros mediante RADIUS o LDAP/AD. También permite la federación de identidades gracias a SAML.

El formato appliance está optimizado para entornos de alta disponibilidad y la mejora de las prestaciones. El sistema es ampliable pudiendo incrementar su rendimiento.

- **Referencias y certificaciones de terceros**

Único producto de su categoría con certificación Common Criteria EAL4+. Ha sido destacado a nivel europeo como la solución tecnológica más completa en la categoría de herramientas y servicios de validación.

Safelayer es un fabricante de producto especializado, con múltiples referencias en proyectos y diversos partners a nivel nacional e internacional que avalan la solidez de sus soluciones.

Más información de TrustedX:

- http://www.safelayer.com
- http://labs.safelayer.com

CAPÍTULO 1

# Descripción de la plataforma TrustedX

Tal y como se ha explicado anteriormente, TrustedX es una plataforma de servicios de seguridad PKI que incluye servicios de firma electrónica y autenticación. Las características de la plataforma son las siguientes:

- Permite independizar los mecanismos de firma electrónica y validación de certificados de las aplicaciones, aportando la gestión centralizada.
- Soporta un conjunto completo de formatos de firma digital y la gestión de múltiples CAs, facilitando la interoperabilidad y federación de dominios PKI.
- Incluye funciones avanzadas de verificación de firmas digitales y de sellado de tiempo, y la opción de custodiar firmas de archivo conforme los estándares de ETSI.
- Capacidad para implantar modelos de firma basados en servidor. TrustedX permite la gestión centralizada de las claves de usuarios y aplicaciones.
- Soporta repositorios corporativos (LDAP/AD) y mecanismos de autenticación existentes (LDAP y RADIUS), además de federación SAML.
- Ampliable con funciones de protección de datos, como el cifrado de datos y la gestión centralizada de claves de cifrado.
- Flexibilidad en la integración de aplicaciones. Aporta plugins para aplicaciones, incorpora carpetas vigiladas y diversas APIs para la integración en diversos entornos.
- El sistema de gestión de TrustedX está basado enteramente en políticas (de autenticación, autorización, firma electrónica, etc) y roles de administración.
- El sistema de logs y auditoría de la plataforma es extensible y de fácil integración con herramientas SIEM.
- Producto con certificación Common Critera EAL4+, garantizando la máxima seguridad.

Las funciones que ofrece la plataforma TrustedX se agrupan en los siguientes servicios:

- **Gestión de entidades y objetos**. Este servicio se encarga de la gestión de las entidades (e.g. usuarios) y objetos de la plataforma. Puede agregar repositorios externos, tales como LDAP/AD de usuarios, bases de datos, archivos y HSMs para la protección de claves privadas.
- **Autenticación y autorización**. Soporta mecanismos de autenticación basados en certificados digitales y contraseñas. Puede incorporar nuevos mecanismos de autenticación mediante agentes, o delegar la validación de credenciales en terceros mediante RADIUS o LDAP/AD. También permite la federación de identidades gracias a SAML.
- **Validación de certificados**. Incluye funciones para la validación de certificados digitales y el análisis de sus campos. Soporta mecanismos de consulta del estado de los certificados basados en OCSP, CRL y también mecanismos personalizados (e.g. consulta de bases de datos, acceso a la plataforma @firma).

- **Generación de firmas electrónicas.** Servicio de firma en servidor que permite la generación de firmas electrónicas en distintos formatos estandarizados para documentos electrónicos, incluyendo correo electrónico y mensajería web. Se soportan formatos con firmas electrónicas múltiples y firmas electrónicas con sello de tiempo.
- **Verificación de firmas electrónicas.** Servicio que permite verificar firmas en distintos para documentos electrónicos, incluyendo correo electrónico y mensajería web. Se soportan formatos con firmas electrónicas múltiples, firmas electrónicas con sello de tiempo y firmas longevas.
- **Generación y verificación de sellos de tiempo.** Aporta las funciones para solicitar la generación y verificación de sellos de tiempo sobre datos mediante el protocolo de OASIS DSS.
- **Actualización de firmas electrónicas**. Servicio que permite la extensión de la validez de las firmas electrónicas a lo largo del tiempo manteniendo su fiabilidad criptográfica. Aporta funciones para incorporar la cadena de certificación, la información sobre el estado de los certificados digitales en el momento de la firma y un sello de tiempo.
- **Custodia de firmas electrónicas**. Módulo opcional que se encarga de mantener la validez de las firmas electrónicas de manera autónoma, interactuando con el servicio de no repudio y gestionando los metadatos de las firmas electrónicas.
- **Protección de datos**. Se trata de dos servicios que aportan (i) los mecanismos de cifrado para la protección de documentos, correo electrónico y mensajería web y, (ii) la custodia de las claves de cifrado y el control de acceso a las mismas. Estos servicios son opcionales y no se describen en este documento. Si quiere obtener información sobre ellos, consulte el whitepaper "TrustedX - Gestión de claves de cifrado" de Safelayer.
- **Auditoría y accounting**. Centraliza de manera uniforme y segura la información de log relativa al control de acceso y al consumo de los servicios de la plataforma. El sistema de log permite incorporar anotaciones específicas, facilitando su gestión con herramientas de terceros.

Algunos de los servicios enumerados en los puntos anteriores son comunes a todas las configuraciones de la plataforma. Los servicios básicos son el servicio de gestión de entidades y objetos, el servicio de autenticación y autorización y el servicio de auditoría y accounting. El resto de servicios se incorporarán a la configuración de la plataforma en función de su ámbito de uso, habitualmente:

- **Firma electrónica.** Además de los servicios básicos, se incluye el servicio de validación de certificados digitales, el servicio de generación y verificación de firmas electrónicas y el servicio de actualización de firmas. Opcionalmente, se puede incluir también el servicio de custodia de firmas electrónicas.
- **Gestión de claves de cifrado.** Además de los servicios básicos, se incluye el servicio de validación de certificados digitales y los servicios de protección de datos. Esta configuración de la plataforma TrustedX no se describe en este documento. Si quiere obtener información sobre esta configuración, consulte el whitepaper "TrustedX - Gestión de claves de cifrado" de Safelayer.

# Arquitectura

En el contexto de una arquitectura orientada a servicios (SOA), TrustedX se sitúa en el nivel de provisión de servicios especializados, en este caso de servicios de seguridad PKI. De este modo, cuando desde cualquier proceso del negocio se necesita generar una firma, verificarla, actualizarla o archivarla, o bien validar un certificado, dicha operación se solicita a TrustedX a través de alguna de sus *interfaces*.

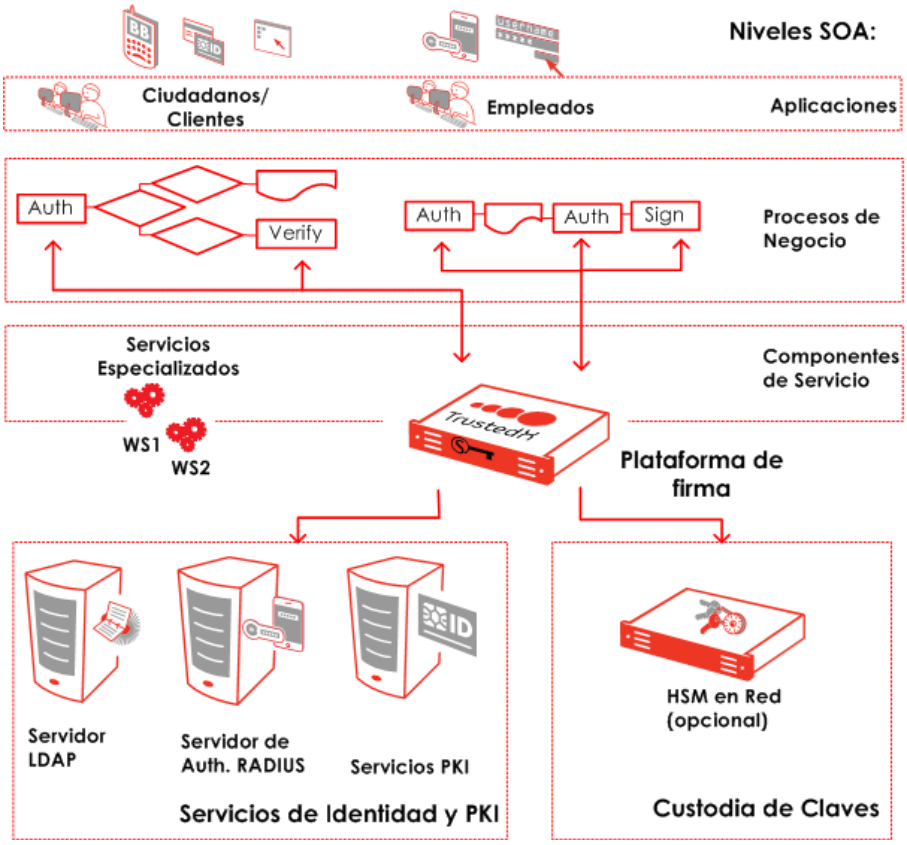


*Figura 1-1. Posición de TrustedX en una arquitectura SOA*

TrustedX se apoya en una infraestructura formada por elementos tales como como servicios de identidad y de PKI, repositorios y HSMs, algunos de los cuales son necesarios para su operación. Los elementos principales de esta infraestructura son los siguientes:

- **Repositorios**

  La plataforma requiere una base de datos SQL con soporte JDBC para la gestión de la configuración del sistema, las entidades, lsas políticas y el almacenamiento de la información de log.

  De forma opcional, se puede configurar la plataforma para que envíe la información de log a un servidor de Syslog, lo cual facilita la integración con sistemas SIEM.

  La plataforma puede integrarse con servidores LDAP/AD y con bases de datos que contengan la información de los usuarios de la organización, sin que por tanto sea necesario realizar ningún proceso masivo de copia o importación de los datos de los usuarios.

  TrustedX puede procesar archivos que hayan sido almacenados en carpetas de red (NFS o SMB/CIFS) por otras aplicaciones, con la finalidad de que realizar operaciones de firma electrónica y/o cifrado sobre ellos.

  Finalmente, para el archivado de documentos y firmas digitales, la plataforma se puede conectar a un sistema de gestión documental (DMS/ECM) como por ejemplo Alfresco.

- **Servicios de identidad y PKI**

  En los procesos de validación de certificados y de verificación de firmas, TrustedX obtiene la información de revocación de los certificados involucrados, accediendo a las VA de confianza por medio de OCSP, o bien recuperando las CRL que sean necesarias por medio de HTTP o LDAP.

Además, mediante conectores de validación, se puede integrar en TrustedX cualquier procedimiento de validación particular. Sólo se considerarán válidos los certificados en cuya ruta de certificación aparezca alguna de las CA de confianza que hayan sido registradas en la plataforma.

Del mismo modo, en los procesos de actualización de firmas, tanto cuando se desencadenan bajo demanda (petición de un cliente), como cuando se realizan de forma automática (custodia de firmas archivadas), TrustedX obtiene los sellos de tiempo necesarios, accediendo por medio de TSP (RFC 3161) a una o varias TSA de confianza.

Finalmente, TrustedX permite la agregación de mecanismos de autenticación mediante protocolos como RADIUS (por ejemplo, en conexión con un sistema de gestión de tokens que implementa claves de un solo uso) y LDAP (por ejemplo, un Active Directory de Microsoft corporativo).

- **HSM (módulo hardware de seguridad)**

  Por lo que respecta a las claves de los usuarios, éstas se pueden proteger de forma opcional con uno o varios dispositivos HSM a los que TrustedX accede a través del correspondiente *driver* PKCS #11.

# Módulos de integración

TrustedX aporta un conjunto de módulos que permiten abordar diferentes estrategias de integración dentro del ámbito corporativo y de la prestación de servicios de firma electrónica. En función del ámbito, se usará alguno de los siguientes módulos o una combiandción de ellos:

- **Tarjeta virtual**: Se integra perfectamente en las aplicaciones de escritorio. El usuario accede de forma trasparente a las claves custodiadas por TrustedX, de forma que sólo debe tratar con una contraseña.
- **Carpetas vigiladas**: TrustedX monitoriza el contenido de unas carpetas de red, ejecutando una serie de acciones sobre todos los archivos que se almacenan en éstas. Orientado tanto a usuarios como aplicaciones. Para firmar, basta con realizar una operación de copiar&pegar sobre una carpeta.
- **Servicios de firma**. Un conjunto de APIs que dan acceso a todos los servicios de TrustedX. Aportan un conjunto completo de opciones de integración pensadas para adaptarse a diferentes entornos:
  - SOAP/WS: Estándar OASIS DSS como protocolo de acceso a servicios web.
  - REST/WS, SOAP/WS: Usando la pasarela de integración de TrustedX que permite configurar el procesado del tráfico y de los datos mediante un lenguaje de pipelines XML.
- **APIs Java**: Permite integrar de forma sencilla los servicios de firma en aplicaciones Java.

La plataforma incluye un **Applet Java** para escenarios de integración de firma electrónica en entornos web.

En el Anexo “Escenarios de uso”, en la página 26, se incluye un conjunto de ejemplos de casos de uso y su arquitectura, en los se muestran los diferentes unos de los módulos integración de TrustedX.

CAPÍTULO 2

# Servicios de la plataforma TrustedX

En este capítulo se describe la funcionalidad que incluyen los servicios de firma y autenticación de la plataforma TrustedX.

## Gestión de entidades y objetos

Este servicio se encarga de la gestión de las entidades (usuarios, aplicaciones y terceros de confianza) y los objetos que utiliza la plataforma para su operación, incluyendo las entidades y objetos que se encuentran en repositorios corporativos que se agregan a los gestionados por la propia plataforma (e.g. un directorio de usuarios).

- Se trata de un servicio básico utilizado por el resto de servicios de TrustedX (i.e. el servicio de autenticación y autorización y el servicio de auditoría y accounting). Su administración se realiza desde la propia consola gráfica de TrustedX.
- Puede ser utilizado por otros servicios corporativos ya que su funcionalidad se expone como servicio SOAP/WS.
- Proporciona acceso uniforme a todos los datos que agrega, independientemente del sistema que gestiona su almacenamiento físico.
- Permite realizar un conjunto de operaciones (Read, Insert, Update, Delete, Search, Count) utilizando expresiones XPath.

Este servicio interactúa con un conjunto de sistemas externos. Tal y como se ha visto anteriormente, estos sistemas son los siguientes:

- **Bases de datos SQL.** TrustedX requiere una base de datos externa donde almacenar las configuraciones y políticas de la plataforma, los datos de las entidades de confianza, los usuarios y las aplicaciones y el log de eventos.
- **Directorios LDAP/AD.** Trustedx puede agregar los usuarios de uno o más directorios corporativos, accediendo a los atributos, certificados digitales y mecanismos de autenticación.
- **Servidores de autenticación.** TrustedX permite agregar servidores de autenticación externos mediante RADIUS.
- **Dispositivos criptográficos (HSM).** TrustedX soporta los HSMs que cumplen el estándar PKCS#11, usándolos para la protección de claves criptográficas. En el supuesto de no disponer de un HSM, el material criptográfico se custodiará de forma protegida en una base de datos SQL o en el sistema de archivos de la plataforma.
- **Gestores documentales (DMS).** TrustedX soporta el uso de gestores documentales para el almacenamiento de documentos y la custodia de firmas electrónicas.

- **Sistema de archivos en red (NFS o SMB/CIFS).** TrustedX puede gestionar archivos almacenados en carpetas de red (carpetas vigiladas) para realizar operaciones de firma electrónica y/o cifrado sobre éstos.
- **Sistemas de archivado de documento (FCS).** TrustedX soporta el uso de sistemas de almacenamiento a largo plazo de documentos electrónicos (Fixed Content Storage) para el archivado de documentos y la custodia de firmas electrónicas.
- **Servicios de confianza (CA, VA, TSA y SSA).** TrustedX accede a servicios y recursos web de terceros de confianza. Por ejemplo, descarga CRLs y accede a autoridades de validación, autoridades de sellado de tiempo y a proveedores de identidad SAML.

# Gestión de entidades

TrustedX distingue entre entidades finales y entidades de confianza.

- Las entidades finales pueden ser usuarios o aplicaciones. Se identifican con un nombre distintivo, disponen de un conjunto de atributos y TrustedX custodia sus claves.
- Las entidades de confianza son entidades que prestan servicios de certificación o sevicios relacionados con la firma electrónica. TrustedX puede reconocer autoridades de certificación (CA), de validación (VA), de sellado de tiempo (TSA) y proveedores de identidad SAML (SAML IdP)

A través de la consola gráfica, TrustedX ofrece la gestión del reconocimiento de las entidades de confianza que se utilizarán en las políticas del sistema. El sistema permite definir el nivel de confianza que se otorgará a cada una de estas entidades.

En cuanto a las entidades finales, TrustedX aporta un sistema propio de gestión de entidades finales orientado a usuarios internos y aplicaciones, a la vez que permite la agregación de entidades del tipo usuario gestionadas en un repositorio LDAP/AD corporativo. En general, TrustedX gestionará las entidades del tipo aplicación, mientas que se apoyará con el directorio corporativo para la gestión de las entidades de tipo usuario.

La gestión de las entidades finales se puede realizar desde la consola gráfica de TrustedX o mediante la API Web, interactuando con el servicio desde una aplicación que lo integre. Concretamente, el sistema proporciona:

- Gestión diferenciada de las entidades en función de su tipo (usuarios y aplicaciones. Las entidades de TrustedX se pueden agrupar para simplificar la concesión de permisos (i.e. la definición de políticas de autorización). Es decir, para que al asignar permisos a un grupo, se asignen los permisos a todas las entidades de dicho grupo.
- Posibilidad de distinguir entre grupos estáticos y grupos dinámicos. Los primeros se definen por extensión (i.e. por enumeración exhaustiva de los miembros que los forman), y los segundos por compresión (i.e. estableciendo la condición de pertenencia al grupo).
- Los grupos dinámicos no requieren que sus miembros hayan sido registrados en TrustedX, por lo que no necesariamente tendrán una identidad local en la plataforma. En estos casos, como resultado de la autenticación, TrustedX asignará un identificador a los usuarios que carezcan de él, con la finalidad de permitir los procesos de control posteriores (e.g. anotación de los consumos).
- Posibilidad de distinguir entre grupos dinámicos organizativos, grupos dinámicos basados en plantillas X.509 y grupos dinámicos basados en consultas (queries) sobre la vista XML del servicio de gestión de entidades y objetos.
- En los grupos organizativos la condición de pertenencia al grupo se establece sobre los atributos del Distinguished Name que la entidad acredite durante su autenticación (Organization, Organizational Unit, Locality, Country y Domain Component)

- En los grupos basados en plantillas X.509, la condición de pertenencia al grupo se establece sobre el certificado cuya titularidad acredite la entidad durante su autenticación.
- En los grupos basados en queries, la condición de pertenencia al grupo se define como una expresión XPath que se evalúa sobre el EP (i.e. la vista XML de toda la información registrada en la plataforma) y que se puede parametrizar en términos del nombre distinguido que acredite la entidad durante su autenticación.
- Capacidad de definir grupos que estén formados (a su vez) por grupos de entidades finales y de gestionarlos como roles, de forma que se simplifique la concesión de permisos (i.e. la definición de políticas de autorización). Así, asignando un rol a un grupo (i.e. declarando que un grupo pertenece a un grupo de grupos), se asignan todos los permisos del rol (del grupo de grupos) a todas las entidades del grupo. De este modo, TrustedX permite implementar un control de acceso basada en roles (Role Based Access Control), tanto para autorizar el consumo de sus servicios como los de otras aplicaciones.

# Autenticación y autorización

Este servicio aporta la infraestructura de autenticación y autorización que usa TrustedX para controlar el acceso al resto de servicios. El servicio de autenticación y autorización también puede usarse desde cualquier aplicación que integre el servicio usando la interfaz SOAP/WS que proporciona.

El servicio está basado en la generación, suministro y validación de aserciones SAML (de autenticación, de autorización y de atributos), ofrece un sistema de token seguro para el consumo de los servicios y soporta la federación con otras autoridades SAML. El funcionamiento básico es el siguiente:

1. Genera una aserción de autenticación SAML a las entidades que utilicen algún mecanismo de autenticación reconocido por la plataforma y presente las credenciales oportunas (e.g. nombre de usuario y contraseña).
2. La entidad podrá incluir la aserción dentro de los mensajes de petición de consumo que dirija o bien a un servicio de TrustedX, o bien a cualquier servicio externo que confíe en TrustedX.
3. Los servicios podrán autenticar a la entidad sucesivas veces sin necesidad de solicitar de nuevo las credenciales a ésta (single sign-on).
4. TrustedX soporta federación, por lo que permite la validación aserciones generadas por terceros. Para ello, basta con que la autoridad SAML en cuestión haya sido registrada en TrustedX.

TrustedX soporta un conjunto de mecanismos autenticación basados en certificados digitales y contraseñas. Además, puede agregar nuevos mecanismos mediante agentes, o bien delegar la validación de las credenciales en terceros mediante RADIUS o LDAP/AD. En concreto, se contemplan tres escenarios:

- **Mecanismo de autenticación interno:** 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 y firmas digitales).
- **Mecanismos de autenticación externo:** El servicio de autenticación y autorización recibe unas credenciales que no han sido validadas y delega su validación en un servicio 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.
- **Agente de autenticación externo:** La validación de las credenciales es realizada por un agente de autenticación externo. TrustedX reconoce el agente, quien proporciona la identidad del cliente. De este modo, se pueden aprovechar las funciones de autenticación de las que ya dispongan las aplicaciones a través de las que se vayan a solicitar los servicios de firma.

Con respecto a la autorización, el servicio permite o deniega el acceso a cualquier servicio de TrustedX que sea solicitado (firma, cifrado, etc). De este modo, el servicio constituye tanto el *Policy Decision Point*, como el

*Policy Enforcement Point* del control de autorización que TrustedX implementa para proteger el acceso a todos sus servicios. Además, el servicio también proporciona información sobre derechos de acceso a recursos, por lo puede ser utilizado como *Policy Decision Point* por cualquier aplicación que desee basar sus decisiones de autorización (i.e. su *Policy Enforcement Point*) en políticas auditables y gobernables de forma centralizada.

Finalmente, el servicio de autenticación y autorización también proporciona un servicio de información sobre atributos de entidades que otras aplicaciones pueden utilizar para implementar un control de acceso basado en atributos (*Attribute Based Access Control*), como sucede en algunos casos de federación de identidad (e.g. al sistema federado no le interesa la identidad local del usuario, sino un atributo que representa el rol del mismo dentro de la organización).

# Generación de firmas

El servicio de generación de firmas se encarga de la generación de firmas de datos y documentos de forma centralizada, en servidor. El protocolo de acceso al servicio es OASIS DSS. Es decir, la interfaz de este servicio cumple, por lo respecta a los mensajes de petición y respuesta, con la especificación *Digital Signature Service* (DSS) de OASIS. OASIS ha definido los mensajes de este protocolo de una manera deliberadamente abierta, de forma que su estructura se tenga que acabar de perfilar en cada escenario particular. En el caso del servicio de generación de firmas de *TrustedX* los mensajes de acceso al servicio se concretan en base al tipo de firma que se quiera generar:

- **Perfil CMS/PKCS#7:** permite generar firmas en formato PKCS#7, CMS y CAdES, tanto a partir de los datos que se hayan de firmar como de su hash. Se soporta la firma simple (firma de unos datos) y la firma múltiple (firma de unos datos ya firmados). Y, dentro de este último tipo, la firma secuencial (firma de una firma) y la firma en paralelo. Se soportan igualmente las firmas separadas (external, detached) y las no separadas (attached, enveloping). También permite generar la firma unos datos a partir del hash de los mismos.
- **Perfil XML-DSig/XAdES:** permite generar firmas en formato XML-DSig y XAdES, tanto a partir de los datos que se hayan de firmar como de su hash. Se soporta la generación de firmas enveloping y enveloped, ambas en el mismo documento que los datos firmados. También se soporta la generación de firmas separadas (detached) que, tras ser obtenidas, el cliente podrá poner en el mismo documento que los datos firmados, o bien en otro distinto.
- **Perfil PDF/PAdES**: permite firmar documentos PDF de acuerdo al formato de firmas definido por Adobe en [PDFRef]. También permite firmar documentos PDF de acuerdo a los perfiles que se definen en las partes 2 y 3 de PAdES (PAdES Basic, PAdES-BES y PAdES-EPES). En futuras releases TrustedX soportará también las partes 4 y 5 de PAdES (PAdES Long-Term y PAdES for XML content).
- **Perfil S/MIME:** permite firmar mensajes de correo electrónico, de manera que los mensajes resultantes tengan el formato S/MIME v2 (RFC 2361) o S/MIME v3 (RFC 2633). Se soportan las firmas enveloping (Content-Type: application/pkcs7-mime) y las firmas detached (Content-Type: multipart/signed)
- **Perfil WS-Security:** permite firmar mensajes SOAP (i.e. el body de éstos) de manera que la firma resultante (una firma XML-DSig) se añada a su cabecera, tal como establece [WSS]. Así pues, utilizando este perfil se pueden proteger la autenticidad e integridad de los mensajes SOAP de cualquier servicio web.
- **Perfil Raw (PKCS #1):** permite generar firmas en formato PKCS #1.

# Gestión de claves

Las claves que las entidades utilizan para generar sus firmas residen en almacenes de claves custodiados por TrustedX. Opcionalmente, las claves pueden protegerse con un HSM y cuya gestión puede realizarse de dos formas:

- **Desde la GUI de la consola de administración gráfica.** En este caso, la gestión sólo podrán realizarla los usuarios pertenecientes al grupo de Oficiales de Seguridad.
- **Accediendo al servicio de gestión de claves.** En este caso, la gestión de los almacenes de claves la podrán realizar los Oficiales de Seguridad y los titulares de dichos almacenes. Sin embargo, una entidad final, a través del servicio de gestión de claves, sólo podrá gestionar su propio almacén de claves.

El servicio de gestión de claves se basa en la especificación [XKMS] de W3C. Concretamente, en la parte de la especificación en la que se define el protocolo para registrar información sobre claves públicas (XML Key Registration Service Specification).

Por otro lado, integrando la tarjeta virtual en los sistemas de registro corporativos, se puede proporcionar claves y certificados a las entidades finales y guardarlos en sus almacenes correspondientes, siguiendo para ello la misma operativa y procedimientos que proporcionase las claves y los certificados en tarjetas físicas.

# Verificación de firmas

El servicio de verificación de firmas sirve para verificar firmas de documentos y de datos, y también para validar certificados, de forma centralizada, en servidor. La interfaz de este servicio cumple, por lo respecta a los mensajes de petición y respuesta, con la especificación *Digital Signature Service* (DSS) de OASIS. OASIS ha definido estos mensajes de una manera deliberadamente abierta, de forma que su estructura se tenga que acabar de perfilar en cada escenario particular. En el caso del servicio de verificación de firmas de *TrustedX* los mensajes de acceso al servicio se concretan en base al tipo de firma que se quiera verificar:

- **Perfil CMS/PKCS#7:** permite verificar firmas en formato PKCS#7, CMS y CAdES (formas BES, EPES, ES-T, ES-C, ES-X Long y ES-A). Se soporta la verificación de firmas simples (con un sólo firmante) y de firmas múltiples (con varios firmantes “en paralelo”). Se soportan igualmente las firmas separadas (external, detached) y las no separadas (attached, enveloping).
- **Perfil XML-DSig/XAdES:** permite verificar firmas en formato XML-DSig y XAdES (formas BES, EPES, ES-T, ES-C, ES-X Long y ES-A). Se soporta la verificación de firmas enveloping, enveloped y detached.
- **Perfil PDF/PAdES:** permite verificar las firmas que contenga un documento PDF tanto si se trata de firmas ISO 32000-1, como si son firmas PAdES de cualquiera de los perfiles que se definen en ETSI TS 102 778-2 y en ETSI TS 102 778-3 (PAdES Basic, PAdES-BES y PAdES-EPES). Nótese que no existe un perfil específico para verificar firmas PAdES sino que el perfil PDF-Signature se utiliza para verificar cualquier firma que contenga un documento PDF.
- **Perfil S/MIME:** permite verificar la firma de un mensaje de correo electrónico que tenga formato S/MIME v2 (RFC 2361) o S/MIME v3 (RFC 2633), tanto si la firma es enveloping (Content-Type: application/pkcs7-mime) como detached (Content-Type: multipart/signed)
- **Perfil certificado:** permite verificar la firma de un certificado y comprobar el estado de validez del mismo.
- **Perfil WS-Security:** permite verificar (de acuerdo a los criterios que establece [WSS]) las firmas XML-DSig que contenga la cabecera de un mensaje SOAP.

## Validación de certificados

La verificación de una firma comporta siempre la validación del certificado del firmante y la de los certificados de su ruta de certificación. Además, *TrustedX* considera la validación de un certificado como un *perfil* o tipo particular de verificación de firma. De este modo, la validación de un certificado puede realizarse a raíz de la verificación de una firma o porque un usuario la solicita explícitamente. En cualquier caso, la validación podrá necesitar la descarga y consulta de CRL y el acceso a una o varias VA, para determinar si el certificado en cuestión ha sido revocado.

El servicio de verificación de firmas permite comprobar el estado de un certificado mediante cualquier combinación de los mecanismos anteriores. Es decir, tanto mediante la consulta de CRL que se obtienen (descargan) por HTTP, LDAP o que residen en el sistema de archivos, como mediante el acceso a una o varias VA, por medio del protocolo OCSP. Por otro lado, mediante la utilización de conectores de validación personalizados, la plataforma permite integrar cualquier mecanismo adicional (no estándar) que permita comprobar el estado de revocación de los certificados.

## Interpretación semántica de las firmas

Un aspecto destacable del servicio de verificación de firmas es que no se limita a indicar si una firma o un certificado son válidos o no, sino que tiene una semántica más rica. Así, en el caso de que considere que una firma o certificado son válidos, proporciona el nivel de confianza (*Level of Assurance*) que le merece dicha validez (bajo, medio, alto, muy alto, etc) y ubica ese nivel en un determinado contexto (corporativo, financiero, administraciones públicas, etc) mediante una etiqueta de confianza. Por otro lado, el servicio puede incluir en las respuestas cualquier dato que la plataforma tenga sobre el firmante y las entidades de confianza que haya utilizado para realizar la verificación, de modo que incluirá más o menos datos dependiendo de cuál sea la política de verificación utilizada. En definitiva, *TrustedX* permite configurar qué datos del firmante y de las entidades de confianza incluirá en las respuestas del servicio de verificación.

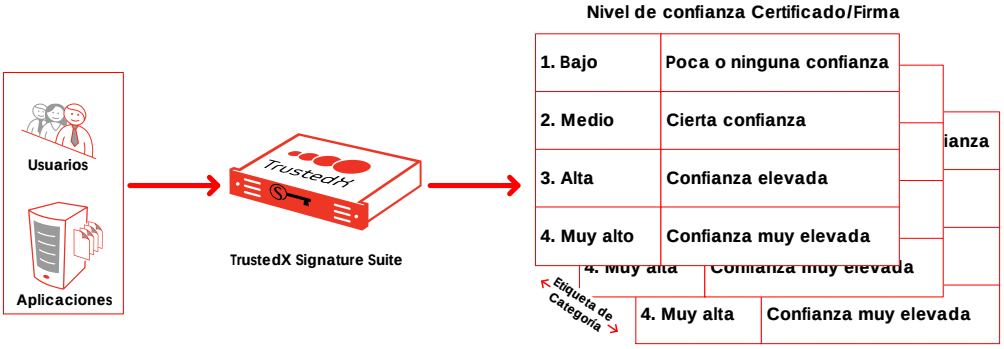


*Figura 2-1. Cuantificación y calificación de la confianza en una firma o certificado*

# No repudio

Hay una necesidad de conservar las garantías que proporciona la firma y de evitar que deje de ser válida cuando caduque el certificado del firmante, o después de la hipotética revocación de dicho certificado. Se tiene que poder repetir la verificación de la firma en el futuro, para lo cual es necesario recopilar las evidencias que permitan repetir dicha verificación (sello de tiempo de la firma, certificado del firmante, cadena de certificación, CRLs, respuestas OCSP) y, además, preservar su fortaleza criptográfica (y la de la firma inicial) mediante la obtención de sucesivos sellos de tiempo sobre la totalidad de los datos.

El servicio de actualización de firmas (DR) sirve para añadir a las firmas evidencias de no repudio (sellos de tiempo, certificados, CRL, respuestas OCSP). Esta actualización se realiza inmediatamente después de haber verificado las firmas. De esto modo, el servicio sólo actualizará firmas que sean válidas. Esto se consigue incorporando a la firma, las evidencias que en cada momento sean necesarias para contrarrestar el efecto de las amenazas que pudieran invalidarla (e.g. el certificado del firmante caduca).

En consecuencia, el servicio de actualización de firmas hará lo siguiente, dependiendo de cómo y cuándo sea invocado:

- **Añadir un sello de tiempo (ES-T).** De este modo se demuestre la existencia de la firma en el instante de la generación del sello (ES-T), lo cual sirve de base para poder conservar la firma a lo largo del tiempo

- **Añadir todos los certificados, CRL y respuestas OCSP que haya utilizado para verificar la firma y un sello de tiempo que demuestre la existencia de todos estos datos de validación en el instante de la generación del sello (ES-X Long, ES-A).** De este modo, garantizará la posibilidad de repetir la verificación de la firma más adelante (e.g. en el curso de un proceso de arbitraje). La firma mantendrá su validez mientras el nuevo sello de tiempo sea válido. Es decir, la firma seguirá siendo válida (y se podrá repetir su verificación) no sólo después de que el certificado del firmante caduque o sea revocado, sino también después de que lo haga cualquiera de los certificados de su ruta de certificación.
- **Añadir un sello de tiempo de archivo que extienda la validez de la firma (ES-A).** De este modo, la firma mantendrá su validez mientras el nuevo sello de tiempo sea válido. Es decir, la firma seguirá siendo válida después de que pierda la validez el sello de tiempo anterior o de que se "rompa" cualquiera de los algoritmos criptográficos que se hayan utilizado en la construcción de la firma (e.g. se “criptoanaliza” con éxito la función de hash que utilizó el firmante para firmar los datos)

Las firmas que actualiza el servicio de actualización de firmas son firmas CAdES y XAdES de ETSI (formas BES, EPES, ES-T, ES-C, ES-X Long y ES-A). En futuras *releases, TrustedX* soportará la actualización de firmas PAdES (ETSI TS 102 778) para que, utilizando el perfil PAdES-LTV, las firmas de un PDF puedan conservar su validez durante períodos muy largos de tiempo.

# Sellos de tiempo

Mediante perfiles de los servicios de generación y verificación de firman que implementan el protocolo DSS de OASIS, TrustedX ofrece la posibilidad de solicitar la generación de sellos de tiempo sobre datos, así como de su posterior verificación. Para la emisión de sellos de tiempo, el sistema requiere la disponibilidad de un servicio de confianza TSA (RFC 3161). La verificación de los sellos de tiempo también lleva a cabo la comprobación de la confianza en la TSA emisora.

# Custodia de firmas

El servicio de custodia de firmas implementa un servicio de archivado de documentos y firmas. Por archivado debe entenderse el almacenamiento en repositorios de los documentos y firmas, junto con sus correspondientes metadatos, durante periodos de tiempo de larga duración. El servicio también incluye la posibilidad de recuperar los documentos, firmas y metadatos que se guarden en el archivo, la de verificar las firmas archivadas y la de actualizarlas (bajo demanda) con evidencias de no repudio.

## Preservación del valor de las evidencias y de la fortaleza criptográfica de la firmas

En el caso particular de las firmas, el servicio de custodia de firmas no se limita a permitir su archivado, recuperación, verificación y actualización bajo demanda, sino que también realiza una custodia activa que, mediante actualizaciones automáticas, permite mantener su validez durante períodos de tiempo arbitrariamente largos (firmas longevas). Concretamente, el servicio de custodia de firmas es capaz de mantener la validez de las firmas que custodia, más allá de la fecha de expiración del certificado del firmante. Es incluso capaz de hacerlo aunque el certificado del firmante sea revocado después de que la firma sea archivada (i.e. el sistema protege las firmas archivadas de los intentos de repudio que pudieran realizar firmantes malintencionados).

## Soporte de múltiples formatos de documento y de firma

Se puede guardar cualquier tipo de documentos en el archivo (PDF, Word, XML, HTML, imágenes, videos, etc). Por lo que respecta a las firmas, el servicio de custodia de firmas soporta todos los formatos que las especificaciones CAdES y XAdES definen sobre la base de los estándares CMS y XML-DSig (i.e. formatos

BES, EPES, ES-T, ES-C, ES-X Long y ES-A). Además, en futuras versiones, se soportará la actualización de firmas PDF, de acuerdo a la especificación de PAdES.

## Soporte de múltiples sistemas para el archivado

En cuanto a los tipos de repositorios que se pueden utilizar, el servicio de custodia de firmas soporta el archivado de documentos y firmas en sistemas de gestión documental que sean accesibles por medio de HTTP/WebDAV (e.g. Alfresco) y en sistemas de tipo Fixed Content Storage que sean accesibles por medio de XAM (eXtensible Access Method) como EMC Centera, que proporcionan mecanismos de integridad adicional como las políticas de retención. Además, se pueden configurar las políticas del servicio de manera que, con cada una de ellas, el archivado se realice en un repositorio diferente y/o con propiedades distintas.

# Auditoría y accounting

Todos los servicios de *TrustedX* envían los *logs* al mismo conjunto (extensible) de repositorios, normalmente bases de datos y/o servidores Syslog. La conexión con estos repositorios y la granularidad de los eventos que se registran en ellos se pueden administrar con el intérprete de comandos.

La plataforma proporciona de serie algunos *appenders* o módulos para el envío de *logs*. Por ejemplo, proporciona uno para guardar los logs en cualquier base de datos a la que se puede acceder mediante JDBC y otro para enviarlos a un servidor Syslog. Además, mediante la instalación de *appenders* personalizados, se puede enviar la información de log a repositorios que utilicen protocolos de comunicación particulares o que requieran recibir los *logs* en un formato determinado.

Los *logs* se pueden etiquetar con el identificador de una política de contabilidad con la finalidad de facilitar su explotación posterior. De hecho, las políticas de contabilidad permiten llevar la cuenta tanto del número de autenticaciones (sesiones iniciadas) como de autorizaciones (servicios consumidos) que realicen los usuarios. Estas cifras resultan importantes para el control estadístico y de facturación.

Los *logs* que se guardan en base de datos se pueden consultar utilizando la consola de administración gráfica o a través del servicio de integración información que incorpora la plataforma.

CAPÍTULO 4

# Integración de aplicaciones

Una de las principales ventajas de la plataforma *TrustedX* es su facilidad de integración, que se debe a su gran flexibilidad y a su elevado grado de estandarización.

De este modo, se puede acceder a las funciones de *TrustedX:*

- Como servicios web
- Desde carpetas vigiladas.
- Desde aplicaciones de escritorio, mediante la tarjeta virtual
- Desde un gestor documental o de contenidos mediante un plugin específico

Además, *TrustedX* dispone de una pasarela de integración que, mediante *pipelines,* permite personalizar la interfaz web de acceso a las funciones de firma de la plataforma.

## Integración mediante programación del acceso a interfaces SOAP, REST y HTTP

Tanto las aplicaciones nuevas como las ya existentes pueden integrar el acceso a funciones de firma, realizando desarrollos sencillos en los que sólo se tiene que programar el acceso a uno o varios servicios web, y en los que el desarrollador no tiene necesidad de tener conocimiento sobre formatos de firma, certificados, CRLs, CAs, VAs, TSAs, gestión de claves, etc. Este acceso puede consistir en intercambio de mensajes SOAP con la interfaz de servicios web *nativa* de *TrustedX*, la cual está descrita mediante WSDL. Por lo tanto, la programación se puede realizar utilizando herramientas (Axis, .NET, JAX-WS, etc) que generan librerías (Java, .NET) de acceso a servicios web de forma automática, a partir de su definición WSDL. En el caso de las aplicaciones Java, como alternativa, se puede utilizar la librería de acceso a los servicios de *TrustedX* que se distribuye con la propia plataforma.

Alternativamente, mediante la definición de *pipelines* en la pasarela de integración, se puede implementar una interfaz personalizada (SOAP, REST o simplemente HTTP) de acceso a los servicios de *TrustedX*. Así, para completar la integración, habrá que programar en la aplicación cliente, los accesos a los recursos web que se hayan definido en la pasarela de integración, para lo cual podrán utilizarse las APIs cliente que sean adecuadas (JAX-WS, JAX-RS, etc). Este es un enfoque que incluye programación en *TrustedX* y que, por tanto, concentra todavía más la complejidad en el lado del servidor y hace que sea más sencilla la integración de los servicios de firma en las aplicaciones nuevas o existentes. Por ejemplo, utilizando este enfoque, validar un certificado se convierte en algo tan sencillo como enviar el certificado a una URL concreta de un mensaje HTTP que contiene el certificado, codificado en base64, dentro del `Body` de dicho mensaje.

## API Java de Integración

La API Java de integración de *TrustedX* está desarrollada sobre Axis y provee de acceso a los servicios de firma mediante las distintas clases implementadas. Estas clases corresponden a las peticiones y respuestas que se pueden dirigir a los diferentes servicios.

Esta API permite implementar aplicaciones cliente sin necesidad de adentrarse en la complejidad de Axis, aunque a su vez permite el acceso a estructuras Axis que pueden ser necesarias en un uso avanzado. De este modo, proporciona aplicaciones Java muy sencillas con muy pocas líneas de código y resuelve la complejidad que supone escribir peticiones SOAP.

Otro de los beneficios destacados de la API Java de integración de *TrustedX* es facilitar el tratamiento de documentos y firmas de gran tamaño.

## Applet Java para Entornos Web

Como complemento a la firma en servidor que proporciona *TrustedX*, Safelayer dispone del *applet* OpenSignX que permite realizar firmas de manera local (i.e. no centralizada), en el cliente. De este modo, se contemplan también los escenarios en los que la firma se genera con una clave que está almacenada en una tarjeta criptográfica (*smartcard*) o *dispositivo* similar que el titular (el usuario) transporta consigo, o bien en un almacén *software* de claves que gestiona el Sistema Operativo de su estación de trabajo (*workstation*) o *laptop.*

Utilizando OpenSignX se pueden firmar tanto formularios web como ficheros del sistema de archivos local.

# Integración mediante escritura y lectura de ficheros en carpetas vigiladas

En muchas aplicaciones, el único mecanismo de integración posible consiste en la escritura y lectura de ficheros en carpetas. Así, por ejemplo, si se quiere añadir la firma electrónica a los datos que genera una aplicación, puede que la única posibilidad sea que la aplicación escriba los datos en un fichero y lo copie después en una determinada carpeta de la red, para que, posteriormente, una aplicación de firma lo lea, genere la firma de los datos, escriba la firma y los datos en otro fichero y copie este fichero en otra carpeta de la red. *TrustedX* soporta este mecanismo de integración mediante su funcionalidad de carpetas vigiladas (*watched folders*). En base a esta funcionalidad, *TrustedX* consulta periódicamente el contenido de las carpetas vigiladas y procesa los archivos que encuentra en ellas mediante la ejecución de *pipelines* de la pasarela de integración (*SmartGateway*). El resultado de ejecutar cada *pipeline* será un fichero en una carpeta de la red, en la que la aplicación cliente lo pueda recoger.

# Integración mediante tarjeta virtual

En muchos casos, las aplicaciones están diseñadas para acceder a las funciones de firma y autenticación a través de interfaces criptográficos predefinidas. Así, por ejemplo, es habitual que un navegador (Firefox, Internet Explorer) acceda a estas funciones utilizando la interfaz PKCS #11 o Microsoft CAPI.

Estas interfaces son una manera de aislar las aplicaciones de las particularidades que tengan los dispositivos criptográficos que se utilicen en cada caso. Es decir, un modo de que no sea necesario modificar las aplicaciones si se cambia de proveedor (*token)* criptográfico. En la medida en que el proveedor o *token* criptográfico implemente la misma interfaz (PKCS #11 o Microsoft CAPI) dará lo mismo que se trate de un proveedor implementado exclusivamente en software o en hardware (e.g. una tarjeta inteligente) o que sea de un fabricante o de otro.

Generalmente, la manera que tienen estas aplicaciones de utilizar los mecanismos criptográficos implica una gestión distribuida de las claves de los usuarios ya que éstas se suelen guardar en el propio sistema sobre el que se ejecuta la aplicación (*token software*), o en una tarjeta criptográfica que el usuario transporta consigo (*token hardware*). En cualquiera de los casos, no resulta posible regular el uso de estos mecanismos mediante políticas de alcance corporativo, ni llevar un *log* centralizado del uso de las claves que pueda ser auditado en cualquier momento.

La tarjeta virtual de TrustedX es una librería que implementa las funciones de las interfaces PKCS #11 y Microsoft CAPI, accediendo a los servicios de *TrustedX*. Es decir, se trata de una librería que proporciona acceso a un *token criptográfico* remoto. Al disponer de un interfaz PKCS #11 o Microsoft CAPI, se puede integrar de forma inmediata con todas las aplicaciones que sean compatibles con dicha interfaz. Por otro lado, cuando la aplicación invoca (en nombre de un usuario) alguna de las funciones de la tarjeta virtual (e.g. firma), ésta ejecuta un código mediante el que solicita a *TrustedX* que realice la operación. Esto posibilita centralizar el almacenamiento y el uso de las claves de los usuarios en HSM de alta seguridad, someter a políticas de alcance corporativo el uso de mecanismos criptográficos desde aplicaciones de escritorio y llevar un registro único que recoja la información relativa a cada uno de estos usos.

La tarjeta virtual proporciona la misma funcionalidad que una tarjeta física (*smartcard*) pero sin ser realmente una tarjeta. Esto supone una importante reducción de costes ya que la organización se ahorra el tener que dar una tarjeta física a todos los usuarios y proporcionarles el correspondiente lector. No obstante, se comporta como una tarjeta física y, por tanto, proporciona a los usuarios una manera segura de utilizar sus claves, ya que éstas se guardan centralizadas en *TrustedX* y, en consecuencia, quedan aisladas del sistema operativo desde el que se utilizan. Por otro lado, el control de acceso a las claves, que en las tarjetas físicas se realiza mediante la verificación de un PIN estático, se realiza, en el caso de la tarjeta virtual, por el servicio de autenticación y autorización de *TrustedX*, lo cual permite la utilización de PINs de un sólo uso (OTPs) o de PINs que combinan una parte estática (*something you know*) con una parte dinámica generada mediante un determinado dispositivo (*something you have*).

La tarjeta virtual, en tanto que dispositivo accesible mediante PKCS #11 o Microsoft CAPI se puede integrar en las autoridades de registro presencial corporativas (KeyOne LRA). De este modo, tras la introducción de las credenciales del usuario (e.g. nombre y contraseña con los que el usuario está registrado en *TrustedX*) el sistema de registro podrá solicitar a *TrustedX* la generación de las claves del usuario en cuestión. Una vez que se emita el correspondiente certificado, el usuario podrá utilizar sus claves desde cualquier sistema en el que se haya instalado la tarjeta virtual, como si las claves estuviesen dentro de una tarjeta física.

# Administración de la plataforma TrustedX

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. Véase *Intérprete de comandos*, pág. 22.

## 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. Las funciones de administración que implementa esta aplicación incluyen:

- **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 entidades de confianza**: permite gestionar las autoridades de certificación, las autoridades de validación y las autoridades de sellado de *tiempo (Figura 4-1)* en las que confía la plataforma.

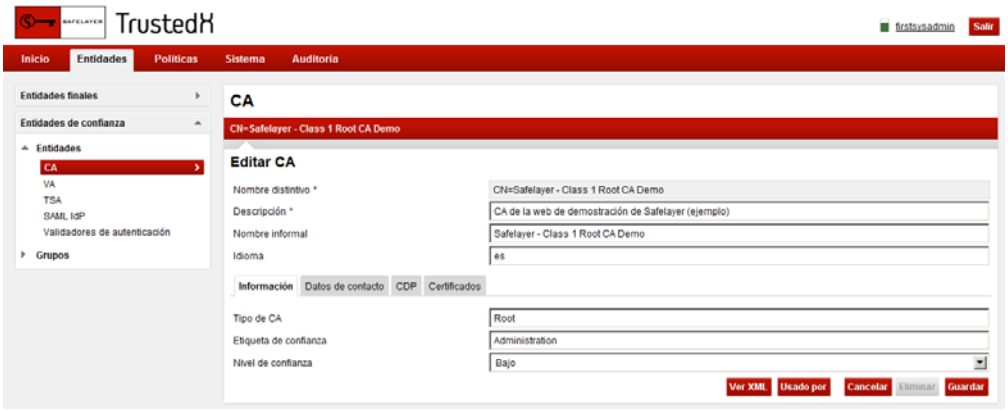


*Figura 3-1. Gestión de entidades de confianza.*

- **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 (ver figura)

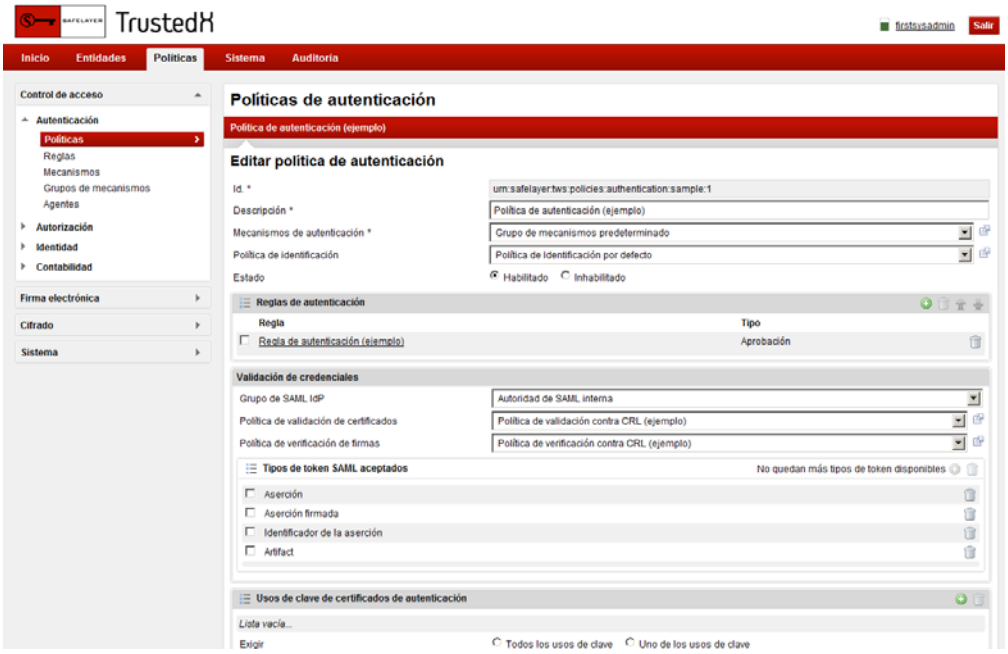


*Figura 3-2. Gestión de políticas de autenticación y autorización.*

- **Gestión de políticas de generación de firmas digitales:** permite definir y modificar las políticas que se aplicarán para generar firmas electrónicas.
- **Gestión de políticas de verificación de firmas digitales y de validación de certificados:** permite definir y modificar las políticas que se aplicarán para verificar firmas digitales y para validar certificados de clave pública (*Figura 4-3*).

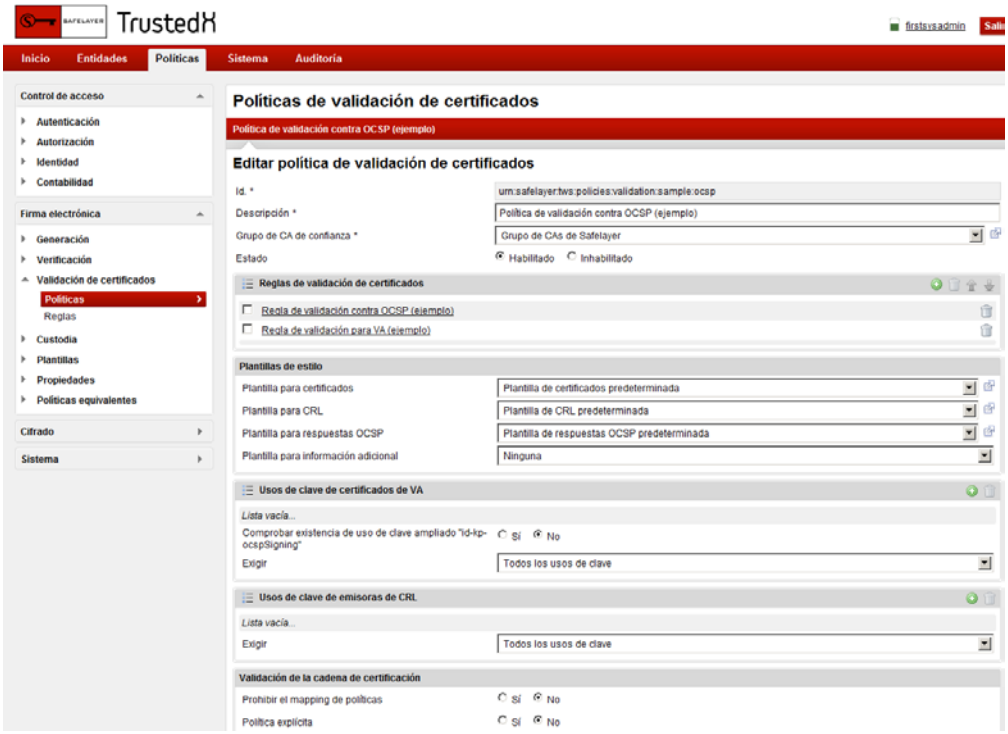


*Figura 3-3. Gestión de políticas de validación de certificados*

- **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 HSMs:** 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*, permitiendo, por ejemplo (Figura 4-4):

- 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, servidores NTP, 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.

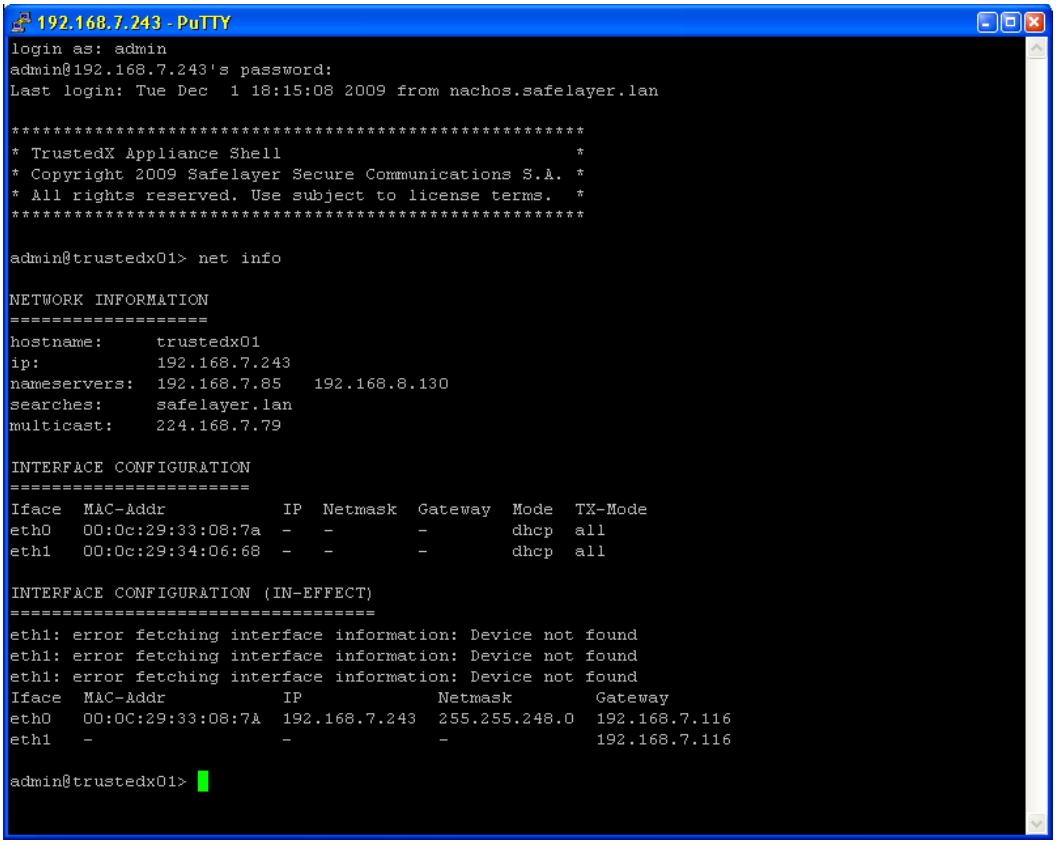


*Figura 3-4. Consola de administración en línea de comandos*

# 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 4-5.*

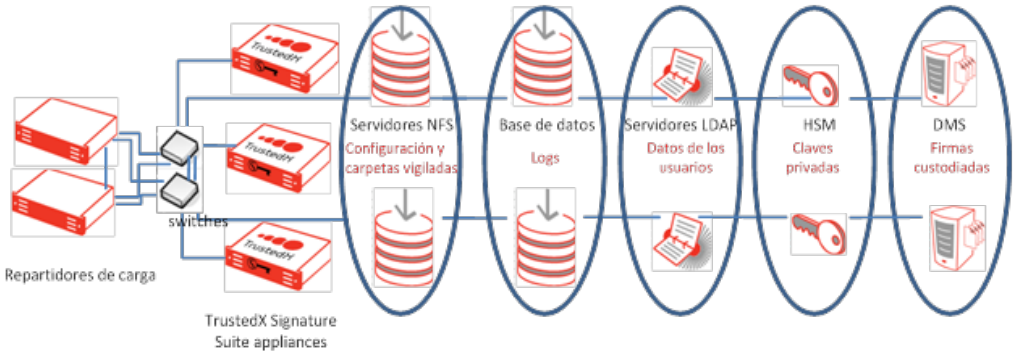


*Figura 3-5. Despliegue de TrustedX en alta disponibilidad*

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. Sólo hay una copia de la configuración de *TrustedX* y reside en un sistema de ficheros en red (e.g. SMB/CIFS, NFS). Cada *appliance* del *cluster* tiene montadas en su sistema de ficheros local, las carpetas de red que contienen esta configuración. De este modo, la configuración se puede administrar accediendo a la Consola de Administración Gráfica de cualquiera de los *appliances*, sin que sea

necesario realizar después ningún tipo de sincronización. Por otro lado, todos los sistemas y recursos (base de datos de logs, servidores LDAP, dispositivos HSM, sistemas DMS, etc) a los que acceden los servicios de 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 4-6*. 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 esta se realiza a partir del envío a un sistema externo (e.g. Splunk), mediante Syslog (*Figura 4-6*), de toda la actividad que tenga lugar en la plataforma, con la finalidad de generar informes de negocio y de *compliance*.

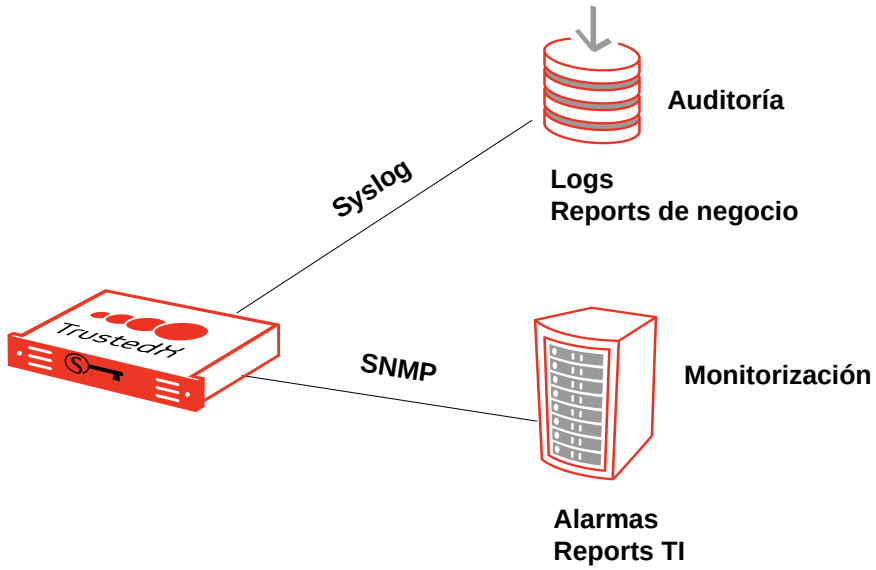


*Figura 3-6. Monitorización y auditoría de TrustedX*

A continuación se muestra un ejemplo de *report* gráfico elaborado con Splunk que muestra estadísticas de las transacciones de generación de firma realizadas por *TrustedX*.


*Figura 3-7. Reports del servicio de generación de firmas*

*Apéndice A*

# Escenarios de uso

En este apéndice se presentan tres escenarios de uso de la plataforma *TrustedX, en los que se usan diferentes módulos de integración de la plataforma*:

- Firma de usuarios en servidor
- Firma corporativa en servidor
- Firma de formularios web con tarjeta

## Firma de usuarios en servidor

Las claves se custodian en un repositorio centralizado, opcionalmente con apoyo de un HSM, de forma que los empleados las puedan usar de forma remota cuando tienen que realizar operaciones de firma. Este escenario se presenta cuando la organización quiere realizar una gestión centralizada de las claves de firma de todo el personal, de forma que sea posible auditar su uso y evitar la copia de las claves en los puestos del usuario.

El sistema admite las siguientes modalidades de integración:

- **Usuario con tarjeta virtual:** El usuario puede usar las claves del repositorio de forma transparente desde las aplicaciones de escritorio (i.e, Explorer, Chrome, Acrobat, Office, etc..). Para esta modalidad se requiere del módulo de tarjeta virtual y del módulo de servicios de firma de TrustedX.
- **Firma desde una aplicación:** Una aplicación que usan los usuarios requiere la firma de documentos o de formularios web. En este caso, cuando la aplicación requiera la firma, enviará el documento a TrustedX quien gestionará la firma del usuario. Para esta modalidad se requiere el módulo se servicios de firma de TrustedX.

Por lo que respecta a la validación de las credenciales del firmante, que es indispensable para controlar el acceso a sus claves, ésta se realiza a través de *TrustedX,* pudiendo hacerse uso de sus posibilidades de integración con los repositorios (LDAP, Active Directory) y servicios de autenticación (RADIUS) corporativos. Cuando el acceso se realice a través de la tarjeta virtual la credencial será un PIN que podrá ser estático o dinámico. Cuando el acceso se realice desde aplicaciones centralizadas, se podrá utilizar cualquier otro mecanismo de autenticación.

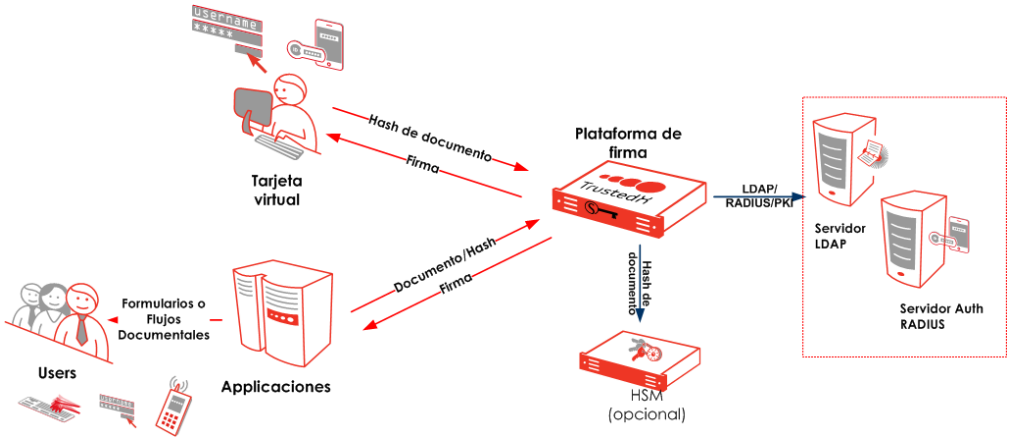


*Figura 3-1. Firma de usuarios en servidor*

Para soportar este escenario *TrustedX* dispone del servicio de generación de firmas, mediante cuya administración a través de una consola gráfica y su generación de *logs*, se puede controlar y supervisar (auditar) de manera efectiva la capacidad de firma del todo el personal de la organización. Por ejemplo, se puede rechazar toda petición de firma en la que no se especifique el compromiso que quiere adquirir el firmante con respecto a los datos firmados. O limitar los algoritmos de firma que se pueden utilizar. También se puede establecer que toda firma incluya en un atributo firmado de la misma, el identificador de la política que se utilice para su generación.

Todas las aplicaciones en las que los usuarios tengan que generar una firma personal deberán incluir un mecanismo para acceder a TrustedX. Las aplicaciones quedan al margen de tener que gestionar, además de las claves de firma de todos los usuarios, la configuración de seguridad de dicha función de firma (e.g. las políticas aplicables), así como el registro de los *logs* que se derivan de uso. O sea, que por lo que respecta a la función de firma, pasamos de un despliegue de la misma basado “en silos” a un despliegue centralizado, basado en SOA, con todas las ventajas de control, coherencia y ahorro de costes que esto comporta.

En el caso de aplicaciones centralizadas (firma de formularios, flujos documentales con firmas) a las que los usuarios acceden desde múltiples terminales que pueden ser de diferentes tipos, se requerirá integrar mediante programación el acceso a *TrustedX*, puesto que normalmente no será viable la instalación de la tarjeta virtual en todos los terminales.

# Firma corporativa en servidor

La firma se realiza utilizando una clave corporativa. Es decir, una clave de la que la propia organización es titular y que se gestiona de forma centralizada, por ejemplo, utilizando un módulo de *hardware* criptográfico.

Este caso de uso se presenta cuando se quiere realizar una gestión centralizada de las claves que las aplicaciones de la organización utilizan para firmar, en nombre de ella, de forma automatizada. Con este tipo de gestión de claves se elude la necesidad de mantener múltiples copias de las claves corporativas (una por aplicación) y, por tanto, el tener que repetir los procedimientos de gestión con cada una de ellas (lo cual puede llegar a ser inmanejable), además de posibilitar el control (*policy enforcement*) y la vigilancia del uso (auditoría) de dichas claves.

Todas las aplicaciones que tengan que generar una firma en nombre de la organización deberán incluir un mecanismo para acceder a TrustedX, quedando al margen de tener que gestionar, además de las claves de firma que utilizan, la configuración de seguridad de la función de firma (e.g. las políticas aplicables) y el registro de los *logs* que se derivan de uso.

TrustedX admite dos modalidades de integración:

- **Carpetas vigiladas:** En muchos entornos es conveniente la técnica de integración basada en carpetas vigiladas por su bajo coste y rapidez de puesta en marcha. El módulo de TrustedX de carpetas vigiladas monitoriza el contenido de una carpetas de red (NFS o SMB/CIFS), ejecutando una serie de acciones sobre los archivos que se almacenan en ésta. Una vez procesados, TrustedX los dipositará en una carpeta de salida, igualmente accesible por red, incluyendo un report de los resultados. TrustedX permite establecer múltiples carpetas vigiladas y definir los pipelines de procesamiento que habrá ejecutar para cada una de ellas.
- **Servicios de firma:** Mediante el módulo de servicios de firma, se aporta un conjunto completo de APIs y servicios Web que permiten la integración de los mecanismos en aplicaciones usando diferentes estrategias. Este escenario es adecuado para entornos heterogéneos en los que se requiera proporcionar acceso a todas las funciones avanzadas de TrustedX, tales como SOAP/WS, REST/WS o APIs de Java.

En definitiva, por lo que respecta a la función de firma corporativa, también pasamos de un despliegue basado “en silos” a un despliegue centralizado, basado en servicios, con todas las ventajas de control, coherencia y ahorro de costes que esto comporta. El acceso programático, por parte de las aplicaciones, a la función de generación de firma corporativa permite la automatización de dicha generación y, en consecuencia, la de buena parte de los procesos de gestión de datos que se dan en la organización.

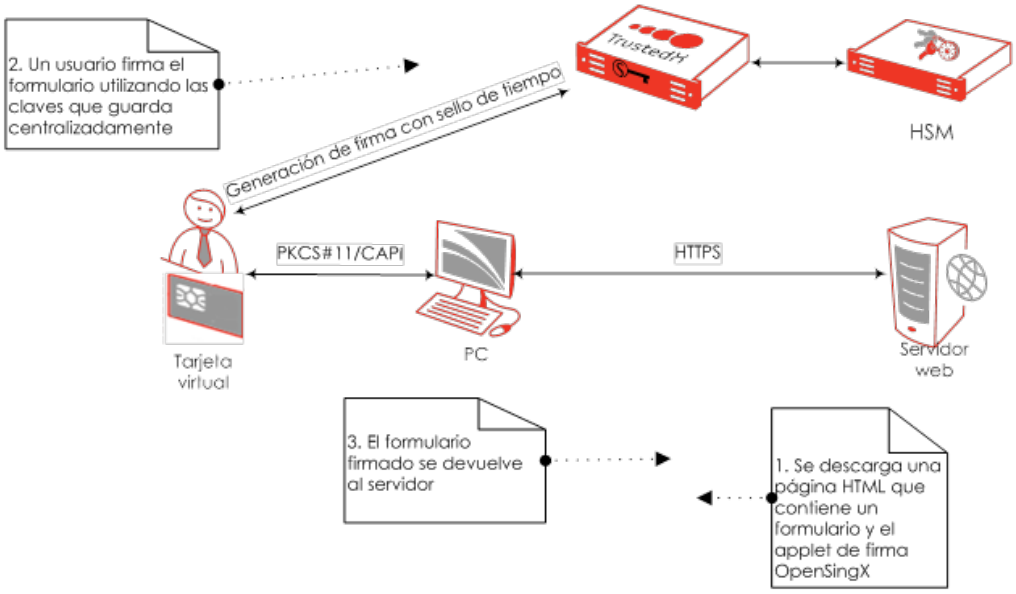


*Figura 3-1. Firma de servidos usando carpetas vigiladas*

# Firma de formularios web con tarjeta

La capacidad de firma en el lado del servidor no permite abordar las situaciones en las que la firma se tiene que generar con una clave que el usuario tiene en su poder (e.g. en una tarjeta criptográfica, en el almacén de claves del navegador). Estas situaciones son típicas de los escenarios en los que la organización se relaciona con entidades externas mediantes formularios web (e.g. escenarios *business to business*, *busines to customers*, *government to citizens*).

Para cubrir esta necesidad, la plataforma *TrustedX* se complementa con un *applet* de firma que se denomina OpenSignX. Mediante este *applet* se proporciona a los usuarios la capacidad de firmar formularios y archivos

de manera local, sin más requisito que disponer de un navegador web provisto del *plugin* de Java (*Figura 4-1*). Además, una vez que el servidor web recibe el formulario o documento firmado, puede acceder al servicio de actualización de firmas de *TrustedX* para añadir un sello de tiempo a la firma. De este modo, se garantizará la validez de la firma (i.e. su no repudiabilidad) durante el período de tiempo en el que el sello de tiempo permanezca válido.

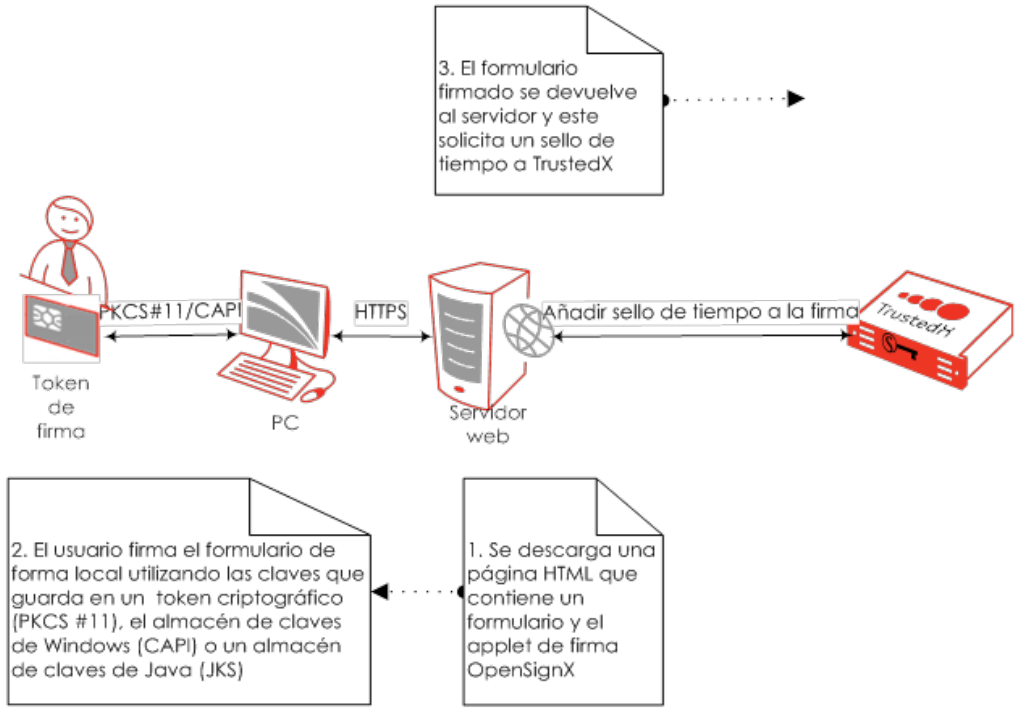


*Figura 3-1. Firma local de formulario web*

Sin embargo, también cuando las claves de los usuarios están gestionadas centralizadamente (i.e. se trata de usuarios corporativos) resulta ventajoso utilizar el *applet* OpenSignX para firmar formularios web. En este caso (*Figura 4-2*), el interés está en utilizar el *applet* en combinación con la *tarjeta virtual*, porque, de este modo, se aprovecha que el *applet* ya incorpora la capacidad de pedir a la tarjeta la generación de la firma, por lo que no será necesaria programar esta solicitud en el servidor web ya que la tarjeta virtual la enviará directamente a *TrustedX*.

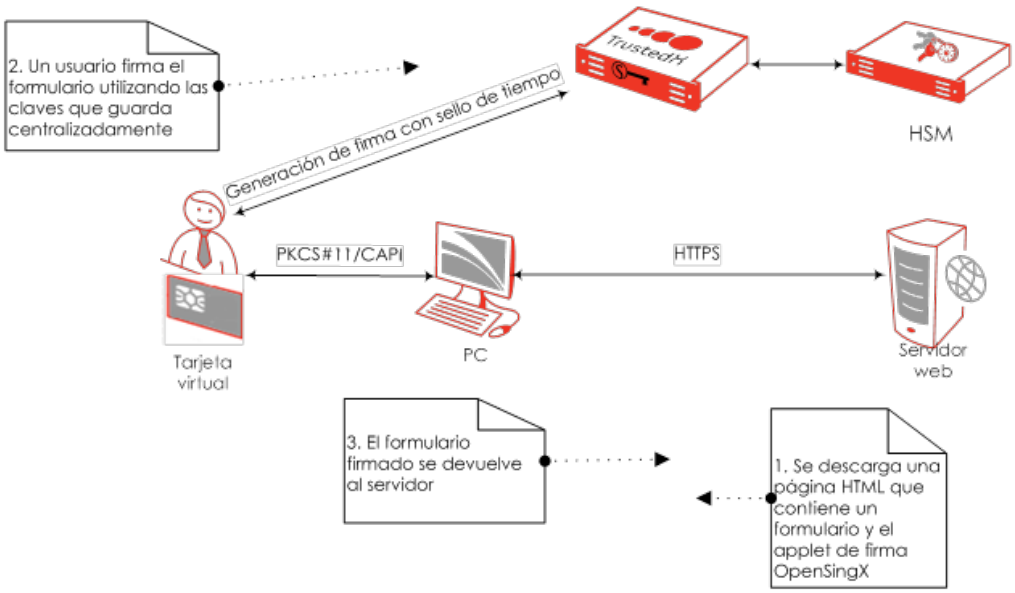


*Figura 3-2. Firma centralizada de formulario web con OpenSignX y tarjeta virtual*

# Estándares y algoritmos de firma soportados

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

## Estándares

*TrustedX* soporta los siguientes estándares:

| *Referencia* | *Estándar* |
|---|---|
| [CMS] | Cryptographic Message Syntax, IETF RFC 5652 |
| [DSS] | T. Perrin et al. *Digital Signature Service Core Protocols, Elements, and Bindings*. OASIS, Draft 27. |
| [CAdES] | *Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats.* ETSI TS 101 733 V1.5.1, December 2003 |
| [OCSP] | Online Certificate Status Protocol, IETF RFC 2560 |
| [LDAP] | Lightweight Directory Access Protocol |
| [PAdES] | PDF Advanced Electronic Signature Profiles. ETSI TS 102 778-1, ETSI TS 102 778-2 y ETSI TS 102 778-3. |
| [PDFRef] | PDF Reference (sixth edition). Adobe Portable Document Format Version 1.7 o superior |
| [PKCS#1] | PKCS #1 v2.1: RSA Cryptography Standard, version 2.1. IETF RFC 3447. |
| [PKCS#7] | PKCS #7: Cryptographic Message Syntax, version 1.5. IETF RFC 2315 |
| [PKCS#11] | PKCS #11 v2.20: Cryptographic Token Interface Standard |
| [RADIUS] | Remote Authentication Dial In User Service (RADIUS). IETF RFC 2865 |
| [SAML] | Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1, September 2003 |
| [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 |

| *Referencia* | *Estándar* |
|---|---|
| [SSL/TLS] | Secure Socket Layer / Transport Layer Security |
| [TSP] | Time-Stamp Protocol, IETF RFC 3161 |
| [X509] | ITU-T Recommendation X509v3 |
| [XAdES] | *XML Advanced Electronic Signatures*. ETSI TS 101 903, March 2006 |
| [XML-DSig] | D. Eastlake et al. *XML Signature Syntax and Processing.* W3C Recommendation, June 2008 |
| [XKMS] | XML Key Management Specification (XKMS 2.0) |
| [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 firma

*TrustedX* soporta los siguientes algoritmos de firma digital:

- RSA-MD2
- RSA-MD5
- RSA-SHA1
- RSA-SHA256
- RSA-SHA384
- RSA-SHA256

Para las firmas RSA, los tamaños de claves que se soportan son:

- Hasta 4096 bits, en software.
- Hasta 4096, en HSM homologados por Safelayer (según modelos).

TrustedX Platforma de firma electrónica



Safelayer Secure Communications, S.A.

Teléfono: +34 93 508 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