TrustedX

Plataforma de firma electrónica

Descripción

Plataforma de servicios web para la gestión de los procesos de firma electrónica:

- Soporte de estándares y formatos de firma electrónica avanzada.
- Facilita la integración en las aplicaciones mediante servicios web y carpetas vigiladas.
- Gestión de la confianza de múltiples CAs, públicas o corporativas.
- Servicio opcional de archivado de firmas, garantizando el no repudio temporal.
- Independiza los mecanismos de firma electrónica de las aplicaciones, con gestión centralizada.
- Registro de log centralizado propio extensible y de fácil integración con herramientas SIEM.

Beneficios

Integración de firma electrónica avanzada

TrustedX soporta los distintos estándares de firma electrónica avanzada y facilita a las aplicaciones la integración de los procesos de generación y verificación. Actúa como un repositorio centralizado de claves y certificados, de forma que se puede usar de manera remota por las aplicaciones sin necesidad de mantener sus propios repositorios locales. Esta aproximación aporta mayor control del uso de las claves de forma auditada y simplifica el despliegue, mantenimiento y uso de la PKI, al gestionarse de forma centralizada. La autenticación y el control de acceso ofrecen diferentes mecanismos y niveles de confianza, y el sistema se puede integrar fácilmente con otros repositorios para la gestión de las identidades.

Interpretación semántica de las firmas

TrustedX es la plataforma de validación más completa de su categoría, permitiendo la gestión de múltiples CAs, soporta cualquier formato de firma y evita cualquier indicio de complejidad a las aplicaciones en la gestión de la confianza. Los servicios semánticos que incorpora permiten obtener toda la información sobre el firmante/firma, así como su nivel de confianza indicado mediante valores discretos (4 niveles) y etiquetas (i.e. Government, Corporative, Finance, etc...).

Ahorro de costes y flexibilidad de integración

Permite despliegues rápidos gracias a su estandarización y múltiples opciones de integración. Se puede usar como servicios web o desde carpetas vigiladas. El producto incorpora una pasarela de integración permitiendo integrar en la plataforma el procesado de datos y tareas comunes, de forma simple mediante pipelines.

Gestión centralizada, auditoría y no repudio

Aporta gestión centralizada de todas las políticas de firma, el mantenimiento de las firmas electrónicas y el registro de logs y auditoría. Esta aproximación permite la regulación del uso de la criptografía a nivel corporativo, la gestión efectiva del reconocimiento de las CAs/VAs y acometer de forma transparente el mantenimiento de firmas debido a la caducidad de los certificados y a la renovación criptográfica.

TrustedX

Plataforma de firma electrónica

Funcionamiento

TrustedX incorpora funciones que aportan un conjunto de mecanismos de seguridad y confianza como servicios. Dichos servicios se pueden usar de diferentes formas, soportando diferentes estrategias de integración:

- **APIs Java o .NET.** Permite integrar de forma sencilla los servicios de firma en aplicaciones nativas Java y .NET (*).
- **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.

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

El conjunto de funciones de la plataforma se agrupan en los siguientes servicios:

- **Autenticación y autorización.** Se encarga de la gestión de las políticas de autenticación y el control de acceso a los recursos/servicios de la plataforma. Soporta mecanismos internos de autenticación basados en contraseña y certificados digitales, así como servicios de autenticación de terceros basados en RADIUS (TMS), SAML o en LDAP/AD.
- **Gestión de entidades y objetos.** Este servicio se encarga de la gestión de las entidades 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 las claves privadas.
- **Validación de certificados.** Proporciona funciones PKI para validar cadenas de certificados y consulta de estado de los certificados.Soporta OCSP/CRL y mecanismos personalizados (por ejemplo, bases de datos y la plataforma @firma).
- **Generación y verificación de firmas.** Genera y verifica firmas en la mayoría de los formatos estándares para documentos electrónicos, incluyendo correo electrónico y mensajería web. En concreto, los formatos soportados incluyen firmas múltiples, firmas con sello de tiempo y firmas longevas.
- **Auditoría y accounting.** Centraliza de manera uniforme y segura la información de log relativa a la firma electrónica. El sistema de log permite incorporar anotaciones específicas, facilitando su gestión con herramientas de terceros.
- **No repudio.** Permite extender la validez de la firma a lo largo del tiempo manteniendo su fiabilidad criptográfica e incorporando la cadena de certificación, la información sobre el estado de los certificados en el momento de la firma y un sello de tiempo.

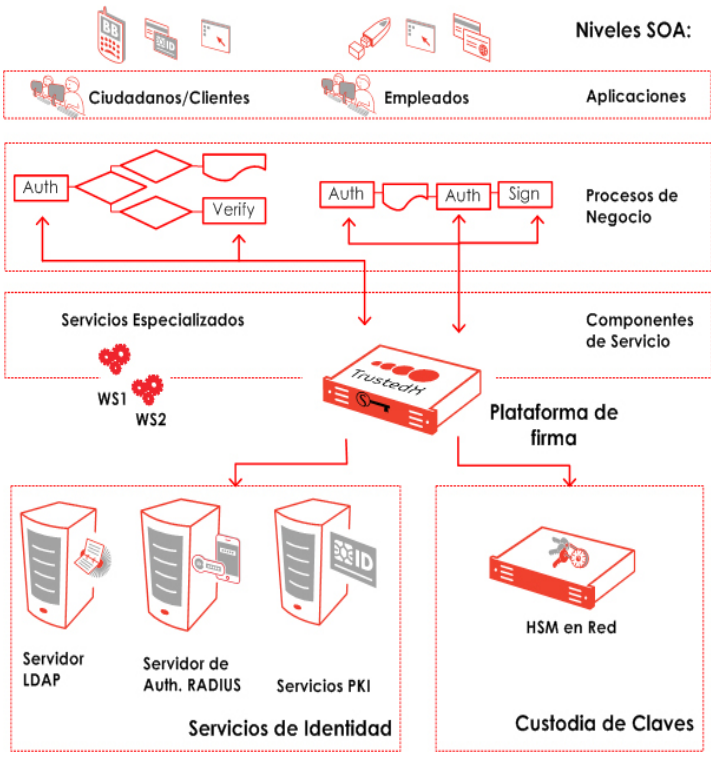
Opcionalmente, pueden añadirse los siguientes módulos:

- **Carpetas vigiladas.** Gestor de carpetas por red que permite aplicar procesos de firma desasistidos sobre archivos. Adecuado para firmas en lote.
- **Custodia de firmas electrónicas.** Se encarga de mantener el no repudio de las firmas electrónicas, interactuando de forma transparente con el servicio de no repudio y gestionando los metadatos relativos a la firma electrónica y los documentos electrónicos.

(*) Consultar disponibilidad

Arquitectura

La siguiente figura muestra las posibles configuraciones arquitectónicas que admite TrustedX.



Características técnicas

- **Formato:** Software appliance. Consultar para más información sobre entornos hardware o virtuales homologados.
- **Monitorización de eventos:** Simple Network Management Protocol (SNMP).
- **Servicios de seguridad:** OASIS WS-Security, DSS (Digital Signature Service) y SAML, REST, SOAP y SSL/TLS.
- **Estándares de sobre digital:** PKCS #7, IETF CMS, ETSI TS 101733 - CAdES, W3C XML-DSig, W3C XML-Enc, ETSI TS 101903 - XAdES, Firma para documentos PDF según IETF y S/MIME y ETSI TS 102 778) - PAdES.
- **Soporte de sellado de tiempo digital:** TSP de IETF – RFC 3161.
- **Verificación de estado de certificados digitales:** Mediante CRLs, protocolo OCSP de IETF y otros mecanismos personalizables.
- **Acceso a base de datos y directorios:** Oracle, Microsoft SQL Server o MySQL. Protocolo de acceso a directorio LDAP.
- **Acceso a servicio de autenticación:** Autenticación basada en LDAP/AD y TMS compatibles con protocolo RADIUS.
- **Soporte de gestor documental:** Protocolo HTTP/WebDAV y XAM.
- **Soporte de HSM:** Dispositivos PKCS #11 homologados por Safelayer.
- **Sistemas de archivos de red soportados:** SMB/CIFS y NFS.

Safelayer Secure Communications S.A.
Basauri, 17 Edif. Valrealty Edif. B Pl. Baja Izquierda Ofi. B
28023 Madrid (Spain)
Tel. +34 917 080 480 Fax +34 913 076 652

www.safelayer.com
World Trade Center (Edif. Sud- 4ª Planta). Moll de Barcelona s/n
08039 Barcelona (Spain)
Tel. +34 935 088 090 Fax +34 935 088 091

SAFELAYER