TrustedX: eIDAS Platform

Plataforma de identificación, autenticación y firma electrónica para entornos Web. Proporciona aseguramiento de la identidad basada en autenticación adaptativa y el reconocimiento de identidades, ya sean corporativas, reconocidas o sociales:

- Aglutina las funcionalidades de autenticación, inicio de sesión único (SSO) y federación de identidades. Proporciona un conjunto de mecanismos de autenticación basados en contexto, biometría del comportamiento, claves de un solo uso, certificados digitales y dispositivos móviles.

- Complementa la plataforma incorporando atributos de identidad PKI para desarrollar funciones de firma electrónica. Aporta, conjuntamente con la funcionalidad de autenticación, servicios de firma en servidor y dispositivos móviles, ofreciendo una solución integral para el despliegue de los nuevos servicios de confianza eIDAS.

Características

Mecanismos de autenticación, federación y SSO adaptativos

- Integración de la organización en los medios Social, Mobile y Cloud (SoMoClo) asegurando un nivel de confianza variable ajustado a las aplicaciones.

- Autenticación adaptativa. Equilibra los vectores seguridad, riesgo/coste y conveniencia de usuario mediante la elevación de la confianza inteligente basada en información contextual y la acumulación dinámica de múltiples factores.

- Gestiona la confianza en la federación de identidades y proporciona control de inicio de sesión único (SSO) entre aplicaciones independientemente del medio y dispositivo, y adaptándose a los requerimientos de confianza variable.

Mecanismos de firma electrónica

- Permite dos modalidades de integración de firma electrónica avanzada en las aplicaciones de forma sencilla y uniforme tanto remota en servidor (p.e. cloud) como en dispositivo en posesión del usuario (p.e. mobile).

Auditoría y regulaciones

Safelayer Secure Communications S.A. es un fabricante de software de seguridad para soluciones de infraestructura de clave pública (PKI), sistemas de autenticación multifactor, firma electrónica, cifrado y transacciones seguras. - C/ Basauri, 17 Edif. Valrealty Edif. B Pl. Baja Izq. 28023 Madrid - World Trade Center (Edif. S-4), Moll de Barcelona S/N 08039 Barcelona - +34 917080480 – Safelayer.com

SAFELAYER

- Ofrece un punto único de agregación de datos, auditoria, reporting y análisis de inteligencia sobre el uso de credenciales para la autenticación y firma.

- Sirve de marco tecnológico para el despliegue de aplicaciones y servicios basados en la nueva regulación europea de identificación electrónica y servicios de confianza (eIDAS), así como la nueva Directiva europea sobre ePayment y Servicios Financieros.

Beneficios

Proveedor/broker de identidad

Actúa como proveedor y/o broker de identidad. Permite la federación con proveedores externos e incrementa la seguridad en la autenticación de los usuarios y grupos existentes, así como el SSO entre aplicaciones. Soporta directorios corporativos (incluido AD/Kerberos), eIDs nacionales e identificadores sociales (i.e. Google, Facebook, etc).

Proveedor de firma electrónica

Como unos atributos de identidad y/o una credencial más, el sistema gestiona material PKI de forma centralizada en el servidor o distribuida en dispositivos (p.e. móviles) con los que se puede llevar a cabo una firma electrónica avanzada tal y como se entiende en la nueva regulación eIDAS.

Estándares de integración

Extiende el control de la autenticación corporativa a las aplicaciones Cloud tales como Google Apps, Salesforce y Office 365 gracias a la implementación de protocolos generalizados en entornos Web y Cloud. Soporta SAML 2.0WebSSO y OAuth 2.0/OpenIDConnect 1.0, facilitando la integración y despliegue de aplicaciones favoreciendo así la API Economy.

Autenticación versátil

Aporta la integración de la autenticación y firma-e en múltiples dispositivos de usuario basados en navegador y/o aplicaciones nativas (p.e. dispositivos móviles). Gracias a los protocolos Web OAuth y OpenIDConnect, y a la App Mobile ID de Safelayer, la integración en aplicaciones es muy sencilla y de alta seguridad.

Elevación de la confianza

Aporta una capa adicional de seguridad que evalúa de forma transparente el nivel de riesgo de la autenticación en base al perfil, los hábitos y la biometría del usuario. El usuario sigue usando su identidad, solicitándole un paso adicional de autenticación únicamente cuando se supera un determinado umbral de riesgo configurable.

Normativa y regulaciones

Se destaca el nuevo reglamento eIDAS en el que se proponen funciones y recomendaciones para el aseguramiento de la identidad, la autenticación y la firma electrónica con el objetivo de mejorar la confianza, seguridad e interoperabilidad entre organizaciones tanto públicas como privadas. Como ejemplo, la nueva directiva de ePayment para servicios financieros y de banca se basa en el reglamento eIDAS.

Funcionamiento

La plataforma eIDAS actúa de proveedor de identidad, autenticación y firma electrónica frente a múltiples aplicaciones mediante el uso de las funcionalidades y conceptos siguientes:

- **Políticas de Autenticación Adaptativa:** Modelan flujos de identidad y autenticación que pueden acumular atributos de identidad y solicitar uno o varios factores de autenticación (OTPs desplegados, SMS, e-mail, etc.) de forma explícita o cuando se supera un umbral de riesgo aceptable.

- **Clasificación de Mecanismos de Autenticación:** Ofrece soporte para la clasificación de niveles de aseguramiento de identidad (LoA) tal y como recomiendan el nuevo reglamento europeo (eIDAS), las normas ENS en España, la recomendación OMB/NIST 800-63 en USA, o el estándar ITU-T X.1254 / ISO/IEC 29115.

- **Trust Elevation y Step-up:** Se incorporan medidas de análisis del contexto de usuario (el dispositivo del usuario, la ubicación y los hábitos de conexión)y mejora de la seguridad (autenticación servidor intuitiva, registro del dispositivo, ritmo de tecleo) que permiten elevar la confianza dentro de un nivel LoA, o saltar de nivel según el riesgo configurado y observado.

- **Single Sign-On (SSO) Adaptativo:** Agiliza la autenticación de los usuarios en múltiples aplicaciones, respetando las exigencias de seguridad. Se soportan 2 tipos de SSO: i) por nivel LoA, y ii) por factor. En el primero, el SSO sólo se produce si la aplicación destino exige un nivel LoA menor o igual que el obtenido en una autenticación previa. En el segundo, el SSO ocurre sólo si los factores que se exigen se han pasado con éxito previamente. En el caso de no cumplirse el SSO, se puede forzar re-autenticación con step-up (acumulación de factores).

- **Federación:** El sistema enlaza con cualquier proveedor de identidad externo en general, y con redes sociales en particular, p.e. Facebook, Google+, etc. para incorporar nuevas fuentes de usuarios e información de identidad. También actúa de proveedor de identidad para proveedores de servicio externos en general, y con aplicaciones Cloud/SaaS en particular, p.e. Salesforce, Google Apps, Office 365, etc. Todas las aplicaciones integradas en la Federación podrán practicar también las funcionalidades de Trust Elevation, Step-up y SSO adaptativo.

- **Firma electrónica:** Como proveedor de identidad, el sistema puede gestionar de forma autoritativa atributos PKI (claves y certificados) asociados a las identidades, así de esta forma puede actuar como proveedor de firma-e. Los atributos claves PKI están protegidos por un contenedor seguro que puede estar en el propio servidor,

custodiado por un HSM, o en un dispositivo en posesión del usuario, p.e. un móvil, en ambos casos, bajo el control exclusivo del usuario. Sólo los usuarios propietarios de los atributos clave pueden acceder a ellos a través de un servicio de firma-e.

- **Mobile eIDAS:** La plataforma se puede complementar con una aplicación móvil (app) denominada "Mobile ID" en la que se custodian de forma transparente y amigable claves y certificados PKI. Esta app, en cooperación con la plataforma eIDAS, permite que el usuario pueda practicar autenticación fuerte PKI y firma electrónica avanzada desde cualquier aplicación Web, ya sea desde el propio móvil o desde otro dispositivo. Esta práctica sigue las recomendaciones de la regulación eIDAS.

- **User-centricity y Privacidad:** El sistema está basado en un paradigma de gestión de identidad user-centric de forma que es el usuario en última instancia quién puede autorizar al proveedor de identidad a entregar información de identidad a las aplicaciones y servicios que los demanden. Los protocolos utilizados son OAuth 2.0, OpenIDConnect 1.0 y SAML 2.0 WebSSO los cuales utilizan al usuario como punto de interconexión entre proveedores. Los protocolos OAuth y OpenIDConnect son respetables con la privacidad de la información de usuario.

- **Integración, Interoperabilidad y API Economy:** El sistema está completamente basado en tecnologías Web: REST, HTTP, Html, JavaScript, JSON y protocolos Web OAuth y OpenIDConnect de forma que la organización puede proveer a su comunidad una API de autenticación y autorización a información de identidad de sus usuarios, así como un servicio de firma-e delegado, en el que aplicaciones pueden pedir autorización de firma-e en nombre de los usuarios. Por otra parte, existen infinidad de sistemas y herramientas terceras de soporte a estas tecnologías Web.

- **BigData e Inteligencia:** Debido a la propiedad user-centric, el sistema acumula y agrega información de identidad, contexto, credenciales, intentos de autenticación, SSO, autorización a servicios y aplicaciones, etc. que el usuario practica a través de la plataforma. Esto generará mucha información relacionada con el usuario que vista de forma agregada a toda la población ofrecerá un potencial de análisis de inteligencia muy valioso para la compañía, tanto a nivel de seguridad y prevención de incidentes, como de conocimiento delacomunidad de usuarios.

Un ejemplo de caso de uso podría ser el siguiente:

- Un usuario está habitualmente conectado en Facebook desde su PC portátil. En un momento dado accede a una aplicación de e-commerce (RP). Esta aplicación delega en un proveedor de identidad (IdP) que está federado con Facebook, de forma que cuando inicia una autenticación de 1ª línea, como el usuario ya está conectado, el IdP obtiene información del usuario a través de Facebook sin re-autenticar a éste.

- En el flujo de autenticación del IdP se ha configurado que se analice, de forma transparente, la información de contexto del usuario, de forma que si es la 1ª vez que se accede desde el dispositivo y/o geo-localización a nivel de país, se fuerce al usuario a introducir un OTP que se envía mediante un SMS. Una vez introducido este OTP, el sistema registra el dispositivo y la localización como de confianza de

manera que próximos accesos se detecte esta situación y no se pidan más factores al usuario.

- En este punto, la plataforma asigna al usuario un nivel de aseguramiento de identidad (LoA) medio. Con esta confianza, el usuario tendrá acceso de lectura a su perfil de e-commerce incluyendo el diario de compras, número de teléfono móvil, direcciones de entrega, cuentas de domiciliación, ofertas personalizadas, etc. No obstante, con un nivel medio no se puede cambiar/escribir en el perfil.

- El usuario procede a la compra de un producto digital para cuya descarga debe autorizar un cargo directo en su cuenta bancaria. En este punto, y en cooperación con la entidad financiera titular de la cuenta, el sistema detecta que el usuario dispone de una clave de firma en móvil (app Mobile ID) y enviará una notificación de aceptación de transacción para que el usuario la firme electrónicamente.

- El usuario ahora desea introducir en su perfil una nueva dirección de entrega. Al acceder al formulario, el sistema detecta que el nivel LoA es medio, y para editar el perfil se necesita un nivel Alto. En consecuencia, el sistema enviará una notificación de autenticación a su móvil (app Mobile ID) para proceder a una autenticación fuerte PKI que resultará en un LoA alto.

Este ejemplo de caso de uso intenta demostrar la versatilidad y potencia de la plataforma para resolver las demandas de seguridad en la identidad cuando es necesario y en función de la criticidad o riesgo del servicio que se quiere consumir. Los mecanismos descritos en el ejemplo pueden ser otros que se consideren más ajustados al servicio a proveer.

Arquitectura