TrustedX - Autenticación basada en PKI

Whitepaper

CONTENIDO

Introducción

La necesidad de identificación es permanente en todos los sistemas de seguridad. La autenticación es el proceso que asegura que la otra parte es quien dice ser, por lo que su fiabilidad es fundamental para la mejora de la seguridad en la identificación electrónica.

TrustedX de Safelayer es una plataforma que agrupa un conjunto de servicios de seguridad basados en (i) criptografía de clave pública (PKI), incluyendo mecanismos de autenticación, firma electrónica y cifrado de datos, o bien, (ii) mecanismos de autenticación basados en información contextual y biometría del comportamiento.

La plataforma se puede desplegar en un contexto SaaS (Software as a Service) orientada a la prestación de servicios de seguridad a nivel gubernamental, corporativo o sectorial. Los servicios de seguridad que ofrece son accesibles como servicios web, mediante protocolos SOAP (Service Oriented Access Protocol) o REST (Representational State Transfer).

Las configuraciones básicas de TrustedX son las siguientes:

- **Plataforma de Autenticación PKI**. Servicio de autenticación PKI basado en certificados digitales y proveedor de Identidad SAML y OAuth. Opera como un proveedor de identidad (IdP) SAML/OAuth y permite la agregación de mecanismos de autenticación no PKI.
- **Plataforma de Autenticación Adaptativa**. Autenticación basada en información contextual y el comportamiento del usuario para la mejora de la seguridad de los mecanismos de autenticación basados en contraseñas de usuario.
- **Plataforma de Firma Electrónica**. Aporta los mecanismos de firma electrónica avanzada, tales como CAdES, XAdES y PAdES. Soporta esquemas de firma en cliente o en servidor, usando un almacén de claves centralizado.
- **Plataforma de Gestión de Claves de Cifrado**. Aporta funciones de cifrado y descifrado de datos accesibles como servicio web. Permite la gestión y custodia centralizada de las claves de cifrado, con control de acceso basado en roles.

En este documento se detallan las características de la **Plataforma de Autenticación PKI de TrustedX**. Para más información acerca de otras configuraciones de TrustedX (Autenticación Adaptativa, Firma Electrónica o Gestión de Claves de Cifrado) solicitar los correspondientes whitepapers.

CAPÍTULO 1

TrustedX Autenticación PKI

TrustedX Autenticación PKI es una plataforma de autenticación robusta y para entornos Web y Cloud que presenta las siguientes características:

- Servidor centralizado de credenciales PKI que incluye federación SAML/OAuth y control de acceso único (SSO y SLO).
- Gestión del nivel de confianza de los certificados digitales y las Autoridades de Certificación (CA) – por ejemplo: confianza muy alta, alta, media o baja-.
- Puede ampliarse a otros mecanismos de seguridad PKI tales como la firma electrónica y cifrado. Permite la agregación de otros mecanismos de autenticación no-PKI.
- Mejora el nivel de auditoría de la autenticación. Sistema centralizado de log que genera información de seguridad en tiempo real y/o destinada a la generación de reports.

Las características destacadas de TrustedX Autenticación PKI son las siguientes:

- **Integración y gestión de certificados de CA**. La autenticación basada en certificados digitales requiere la implantación de algoritmos PKI y la gestión del reconocimiento e interacción con múltiples Autoridades de Certificación (CA). TrustedX simplifica la integración evitando cualquier complejidad en las aplicaciones, y permitiendo su gestión de forma centralizada.
- **Gestión del nivel de confianza.** TrustedX permite clasificar otros mecanismos de autenticación en función de su nivel de confianza (p. ej., nivel medio para contraseñas y muy alto para certificados), permitiendo adecuar su aplicación al valor de los activos electrónicos y los canales de negocio. Los mecanismos de autenticación puede agregarse mediante protocolos como RADIUS o LDAP, incorporando agentes específicos o federación.
- **Integración directa y sencilla**. Garantiza la puesta en marcha rápida y eficiente en aplicaciones como Google Apps, Salesforce o el portal Web corporativo gracias a la implementación de protocolos generalizados en entornos Web y Cloud. Soporta SAML 2.0 y OAuth 2.0, facilitando la federación de aplicaciones mediante el uso de APIs web.
- **Conexión con repositorios de identidad**. Se conecta a repositorios de identidad existentes en la organización tales como LDAP o AD de Microsoft, por lo que no introduce procedimientos adicionales de gestión de la identidad y atributos. Actúa como proveedor de identidad e incrementa la seguridad en la autenticación de los usuarios y grupos existentes en uno o más repositorios.
- **Interpretación semántica uniforme**: TrustedX permite la interpretación semántica de los atributos de identidad de forma uniforme. Además, destaca por aportar una indicación del nivel de confianza de la

identidad mediante valores discretos y etiquetas configurables (p. ej., Corporate o Government), y permite complementar esta información con otro tipo de atributos procedentes de repositorios corporativos (p. ej., con roles almacenados en LDAP).

- **Gestión basada en políticas**. Su sistema de gestión está basado en políticas que permiten la adecuación de los factores de autenticación a cada colectivo de usuarios (empleados, partners, clientes, etc.) y para cada aplicación, en función del nivel de confianza necesario en cada caso.
- **Control centralizado y auditoría**. El servidor facilita el control de acceso único (Single Sign-On y Single Logout), centraliza la respuesta rápida a incidentes de seguridad y agrega la información de auditoría, aportando detalles de cada decisión de autenticación que pueden usarse en las auditorías de seguridad corporativas.

Escenarios de uso

La solución de autenticación de Safelayer hace foco en la protección de aplicaciones Web, portales y aplicaciones SaaS en el Cloud, destinadas a distintos grupos de usuarios como empleados, partners, proveedores y clientes de una organización, o ciudadanos usuarios de la administración pública:

- **Aplicaciones para el cliente/ciudadano**. Aplicaciones Web que requieren niveles altos de seguridad y facilidad de uso, con mínima instalación en el puesto de usuario y mínima logística. Por ejemplo, portales de clientes o ciudadanos tales como administraciones públicas, retail o banca.
- **Aplicaciones corporativas**. Incluye la autenticación para acceder a aplicaciones Cloud, tales como Salesforce o Google Apps, desde cualquier ubicación. También incluye la autenticación a aplicaciones Web y portales para empleados, partners y/o proveedores.

En todos los escenarios de uso, la autenticación se gestiona de forma centralizada en base a las políticas de seguridad corporativas y la auditoría se mantiene en la propia corporación indistintamente de si la aplicación está alojada on-premises o en Cloud.

TrustedX minimiza la integración de la autenticación en las aplicaciones Web y está, además, preparado para la integración de nuevas aplicaciones Cloud cubriendo futuras necesidades. TrustedX destaca por:

- No introducir procedimientos propios de gestión de la identidad y operar como una capa adicional que aporta mayor seguridad.
- Permitir aplicar diferentes políticas de autenticación en función del tipo de usuario (ciudadanos, partners, empleados, clientes, etc.) y el tipo de aplicación.
- Todo el proceso de autenticación se delega por completo en TrustedX. Una vez autenticado, el usuario puede acceder a otras aplicaciones Web y Cloud.
- La auditoría y control de acceso se gestiona de forma centralizada en la propia corporación, de forma agregada al resto de aplicaciones corporativas.

Figura 1-1. Casos de uso de TrustedX Autenticación PKI para workforce y protección de aplicaciones web orientadas a clientes.

Funcionamiento

La plataforma de autenticación TrustedX actúa como un proveedor de identidad (IdP) frente a las aplicaciones. Agrega los atributos de identidad de los repositorios corporativos y permite definir el nivel de seguridad de la autenticación en cada caso mediante los conceptos siguientes:

- **Validación de certificados**. Aporta las funciones de PKI referentes a la validación de cadenas y consulta del estado de los certificados. Soporta mecanismos OCSP/CRL o personalizados (como bases de datos o plataforma @firma).
- **Federación, Single Sign-On (SSO) y Single Logout (SLO)**: Agiliza la autenticación de los usuarios en múltiples aplicaciones, respetando las exigencias de seguridad. TrustedX mantiene la sesión de autenticación, por lo que el usuario no debe autenticarse de nuevo cuando cambie de aplicación.
- **Agregación de mecanismos**. Soporta mecanismos nativos de autenticación basados en contraseñas y certificados digitales. Puede incorporar nuevos mecanismos mediante agentes, o delegar la validación en terceros mediante RADIUS o LDAP/AD. También permite la federación de identidades gracias a SAML.
- **Clasificación de mecanismos de autenticación**: TrustedX mantiene un catálogo de mecanismos de autenticación (soportados por TrustedX o de terceros), a los que asocia un nivel de confianza. Por ejemplo, los diferentes mecanismos se pueden clasificar según los 4 niveles LoA del NIST o los equivalentes ITU-T X.1254/ISO/IEC 29115.
- **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 o archivos.
- **Auditoría y accounting**. Centraliza de manera uniforme y segura la información de log relativa al control de acceso y a la validación de los certificados. El sistema de log permite incorporar anotaciones específicas, facilitando su gestión con herramientas de terceros.

Arquitectura e integración

La solución de autenticación de Safelayer puede desplegarse junto a una solución de autenticación y autorización ya existente en las aplicaciones para aportar niveles de seguridad adicionales o puede desplegarse con el soporte de servicios de identidad y herramientas estándares de terceros (p. ej., bases de datos, directorio LDAP/AD, servidores RADIUS y/o servicios de confianza PKI).

TrustedX está disponible en formato para appliances, que puede ser para un conjunto de hardware o entornos virtuales homologados por Safelayer. El sistema requiere un sistema de base de datos externo para la gestión de los datos de configuración y el mantenimiento de la información de los perfiles, logs y auditoría (no mostrado en la siguiente figura).

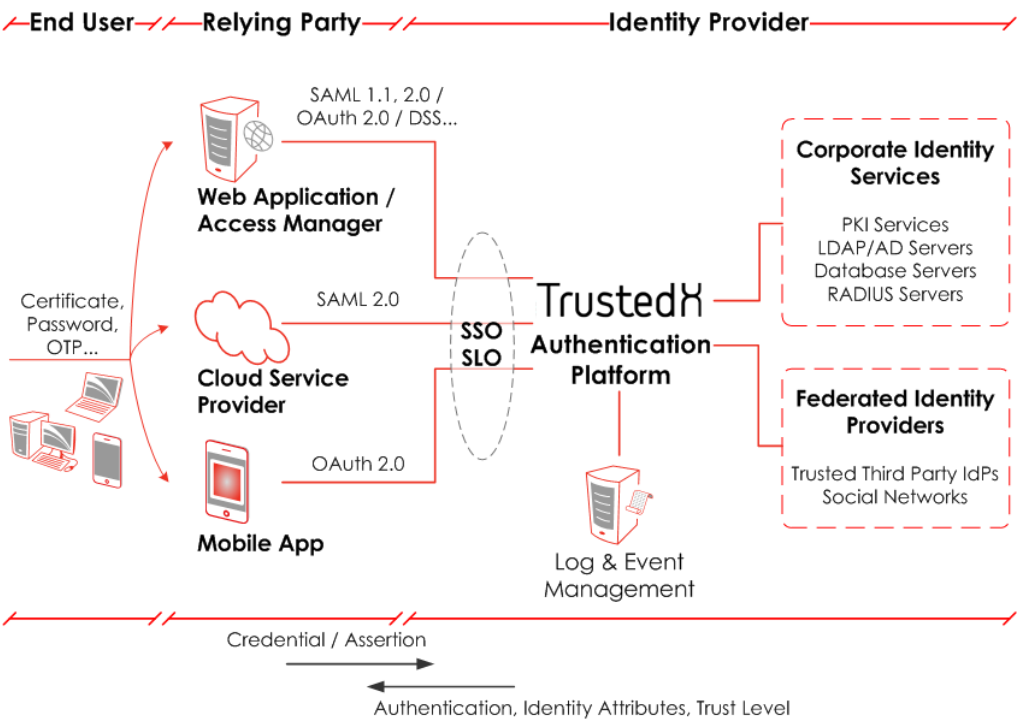

Figura 1-2. Arquitectura del sistema.

En cuanto a la integración con las aplicaciones (*relying parties*, RP), el servicio de autenticación de TrustedX constituye la base para que el sistema desarrolle funciones de valor añadido tal como la autenticación, obtención de atributos de identidad, gestión de autorización y control de acceso, y auditoría centralizada.

Para esto, TrustedX media entre las aplicaciones de usuario y los servicios de identidad. Las aplicaciones invocan a TrustedX con los protocolos basados en HTTP OAuth 2.0 o SAML 2.0. Las distintas estrategias de integración de la autenticación que permite acometer TrustedX son las siguientes:

- **Autenticación estándar**, utilizando la propia interfaz de autenticación de usuarios finales de TrustedX. La aplicación web (RP) a integrar redirecciona los usuarios a la página de login estándar de TrustedX, quien se encarga directamente de interactuar con el usuario para autenticarlo.
- **Autenticación con interfaz gráfica delegada**, para ofrecer una experiencia de usuario más armónica con las aplicaciones. La página de login se incluye en la aplicación web (RP) a integrar, en la cual TrustedX delega para capturar y aportar la información de la credencial primaria, y contexto y comportamiento del usuario.
- **Autenticación externalizada** en otros proveedores de identidad y autenticación ya desplegados. En este caso, la página de login se incluye en la aplicación web (RP) a integrar, en la cual TrustedX delega para capturar y aportar la información sólo de contexto y comportamiento del usuario. El proceso de autenticación primario es independiente de TrustedX.

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 siguiente figura:

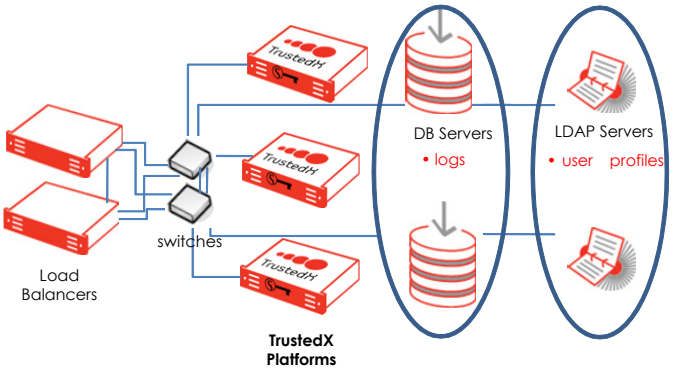

Figura 1-3. Despliegue de TrustedX en alta disponibilidad

Esta arquitectura dispone de un *cluster* formado por dos o más *appliances* de TrustedX a los que un repartidor de carga, también en alta disponibilidad (e.g. configuración activo/pasivo), reparte las peticiones que recibe de los clientes. Por otro lado, todos los sistemas y recursos (base de datos de logs, servidores LDAP, dispositivos HSM, etc.) a los que accede TrustedX deberán estar también en alta disponibilidad.

SAML y OAuth

TrustedX puede actuar de Proveedor de Identidad (IdP) SAML u OAuth en cuanto ofrece adicionalmente a la autenticación las siguientes funciones:

- **Gestión de atributos de identidad**. La solución permite utilizar diferentes repositorios de identidad que se encuentren en producción, basados en estándares como LDAP/AD o basados en bases de datos, mapeando los atributos de identidad y el formato de servicio que se proporciona basado en OAuth y SAML. La solución supone la existencia de un sistema de aprovisionamiento de usuarios externo que incorporará y actualizará los usuarios y sus atributos de identidad.

- **Gestión de sesiones**. Incorpora funciones de SSO y SLO para todas las aplicaciones que usen tanto OAuth como SAML. Esto quiere decir que cualquier usuario y aplicación que inicie una sesión en el IdP, ya sea a través de SAML o de OAuth, se mantendrá de forma uniforme para cualquier aplicación en el dominio del IdP, independientemente del protocolo. Esta propiedad es muy conveniente para crear un clima de integración uniforme entre aplicaciones corporativas on-premise y en el Cloud.

- **Gestión de federaciones de IdPs** que representan diferentes dominios o círculos de confianza. Futuras versiones de TrustedX soportarán OAuth para implementar una federación amplia. En cuanto a SAML, se soporta el perfil Web Browser SSO para poder comunicar con el IdP las aplicaciones existentes (mayoritariamente Cloud) que de momento soportan sólo SAML.

TrustedX soporta el perfil Web Browser SSO de SAML 2.0 implementado el conjunto de atributos de identidad mínimo necesario para actuar como elemento de integración con las aplicaciones Cloud (Salesforce, Google Apps…). En general, este tipo de aplicaciones requieren un subconjunto de atributos de identidad como “user_id” o “email”. En cuanto a OAuth, se soporta el flujo Authorization Code Grant de la versión 2.0 y TrustedX se contempla esencialmente como un proveedor OAuth 2.0.

Figura 1-4. Cada IdP puede soportar uno o más protocolos, permitir SSO y SLO, y definir su propio flujo de autenticación.

Servicios web RESTful

TrustedX potencia un modelo Web que descansa sobre la tripleta HTTP/JSON/HTML, un estilo REST (Representational State Transfer) de arquitectura de sistemas distribuidos, modelo de diseño y provisión de contenidos y servicios Web. De esta forma, TrustedX podrá integrarse y desplegarse en cualquier entorno Web utilizando un API que oculta toda la complejidad real del sistema.

El modelo RESTful permite a integradores y programadores incorporar los servicios de autenticación de TrustedX de forma muy sencilla en sus aplicaciones y entornos web utilizando los frameworks y herramientas habituales.

Los servicios web RESTful son también especialmente adecuados en entornos AJAX de navegador en los que con HTML y JavaScript se alcanzan experiencias de usuario excelentes sin que el usuario tenga que instalar ningún componente previamente. Por otra parte, el modelo de integración y programación RESTful en Internet es ya tan popular que la mayoría de entornos, herramientas y servicios de aplicación ofrecen esta alternativa como único modelo de uso.

La práctica del modelo web RESTful está soportado en todas las plataformas de computación actuales, tanto para servidores como para usuario final. De estos, es interesante destacar el soporte para usuario final:

- Por medio de una aplicación de navegador web en Desktop/PC, teléfonos móviles, tabletas, consolas de juego, web TVs, etc.
- En los sistemas operativos de usuario final (MS Windows, Apple iOS, Google Android, etc.) que incorporan de forma nativa soporte para el procesado de las tecnologías web (HTTP/JSON/HTML) a través de motores web (WebKit).
- Mediante el uso de herramientas (SDKs) de código nativo (Java, Objective C, C#, etc.) que existen para todas las plataformas se puede integrar y programar fácilmente la incorporación de cualquier contenido y servicio web siguiendo el modelo RESTful.

Monitorización y auditoría

Un aspecto muy importante de la seguridad en general, y de la autenticación en particular, es el registro (generación y almacenamiento), búsqueda, recuperación, análisis de eventos y presentación de conclusiones (*reporting*) para i) auditorías de seguridad, ii) informes de cumplimento de normativas (*compliance*), iii) monitorización y alarmas de seguridad, iv) observación y sintonización del sistema, u v) obtención de informes de actividad (por ejemplo, para facturación).

En este sentido, TrustedX dispone de un completo sistema de generación de informes que cuenta con su propia consola gráfica de análisis (por ejemplo, para la observación y sintonización del sistema en período de entrenamiento) y que, a la vez, se integra de forma sencilla con herramientas de terceros del tipo SIEM y de monitorización SNMP, gracias al soporte de formatos de log estándares (por ejemplo, para conexión con sistemas corporativos de monitorización y alarmas).

En general, la solución se ha diseñado para incluir funciones y facilidades de log y reporting suficientes para una operativa y explotación básica del sistema. No obstante, si se quiere realizar una explotación avanzada de éste, como por ejemplo, agregación y correlación de eventos, informes de *compliance*, procesos de gobierno y auditoría avanzada, retención longeva de datos, etc., deberán utilizarse herramientas externas, generalmente, un SIEM con dichas funciones.

Gestión de eventos y auditoría

Los eventos de TrustedX se pueden explotar mediante herramientas externas (generalmente del tipo SIEM) y correlar información asociada a los eventos de autenticación con eventos de otros componentes IT de la organización para preparar informes más completos de auditoría y una detección más eficaz de posibles anomalías.

A nivel organizativo (o de prestador de servicios), TrustedX también aporta información que puede usarse para contabilizar el uso de los activos IT ofrecidos, y además, aprovechar las reglas de control de acceso para limitar el consumo de dichos activos en función del contexto de usuario.

Para esto, TrustedX ofrece diferentes servicios y formatos de información de log. Los registros se pueden procesar con herramientas externas de la siguiente forma:

i) Mediante una herramienta externa del tipo Security and Information Event Management (SIEM) que aplica funciones de inteligencia. Para esto, TrustedX permite la generación de eventos de log en formato CIM y usar almacenes Syslog.

ii) A través de un servicio Web que proporciona la propia plataforma. El servicio proporciona los registros de logs en formato XML de forma que se pueden realizar funciones de inteligencia, incluidas búsquedas y localización de información más detallada, o informes de actividad de cualquier tipo.

Monitorización y alarmas

La solución de Autenticación de TrustedX genera diversas fuentes de información. Su monitorización puede usarse para generar alarmas que pueden conllevar actuaciones inmediatas de administradores y operadores, dependiendo de la severidad de la alarma.

La siguiente es la lista de fuentes de información y métodos de monitorización disponibles en la solución:

- Información de errores y estadística de uso de recursos del sistema a través de una fuente SNMP que incluye la solución. Se pueden utilizar monitores SNMP (p. ej., Nagios, OpenNMS, IBM Tivoli o HP

Network Management Center) para hacer un mapa de red de los servidores dedicados a la solución de Autenticación, monitorizar los parámetros y generar alarmas ante situaciones anómalas.

- Información de posibles fallos, errores de funcionalidad o de ejecución de los procesos que implementan la solución a través de i) la consulta activa del registro de eventos propietario, o ii) programación de extensiones de la herramienta "log4j". En la solución se hace público el formato propietario de los eventos que puede consultarse en una base de datos o fichero, o también a través del API de servicios web proporcionado.
- Mediante análisis de los eventos generados por TrustedX en formato CIM dirigidos a un servidor Syslog, opcionalmente con soporte de herramientas SIEM y a tiempo real, para obtener información de posibles fallos, errores de funcionalidad o de ejecución de los procesos que implementan la solución.

TrustedX Autenticación basada en PKI

Safelayer Secure Communications, S.A.

Telephone: +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