



Identity  
Federation



Adaptive  
Authentication



Electronic  
Signature



Transaction  
Confirmation



# TrustedX

## eIDAS

(electronic IDentification, Authentication and Signature)

### Descripción

### Plataforma de identificación, autenticación y firma electrónica centrada en el usuario para entornos Web

- Autenticación multi-factor y firma electrónica cualificada desde cualquier dispositivo
- Use su móvil para identificarse de forma segura y sencilla
- Federación de identidades con gestión del nivel de confianza
- Firma remota con claves PKI custodiadas en un servidor seguro
- API Web para la integración en todo el ecosistema de aplicaciones
- Preparado para prestar servicio a grandes volúmenes de usuarios
- Conforme al Reglamento eIDAS y la Directiva PSD2

### Beneficios

#### Solución completa

Solución diseñada para proporcionar identificación segura de usuarios en un contexto de movilidad y nube. Además de incluir autenticación, SSO y federación de identidades, destaca por aportar funciones de firma remota cualificada a través de APIs Web.

#### Elevación de la confianza

Motor de autenticación adaptativa que clasifica el nivel de confianza del mecanismo de autenticación (según NIST AAL / eIDAS Assurance Levels) y permite elevar el nivel de confianza mediante un factor de autenticación adicional tal como un SMS/Email OTP o Mobile ID de Safelayer.

#### Firma en la nube

Gestión de los atributos de identidad de infraestructura de clave pública (PKI) y funciones de Firma Remota según la norma técnica CEN TS 419 241. Producto adecuado a las partes 1 y 2 del próximo estándar CEN EN 419 241 para sistemas fiables de firma en servidor.

#### Integración estándar

Gracias al soporte de API de servicios Web REST que implementan los estándares OAuth2/OpenID Connect, SAML y formatos de firma ETSI \*AdES, podrá usar herramientas HTTP básicas disponibles en cualquier entorno/lenguaje para integrar.

#### Seguridad y auditoría

El sistema contabiliza y agrega la información de identificación, autenticación y firma electrónica según los requisitos de seguridad aplicables en las normas técnicas asociadas al Reglamento eIDAS.

### Funcionamiento

La plataforma TrustedX eIDAS actúa de proveedor de identidad (IdP) y proveedor de firma (eSigP) de usuarios frente a las aplicaciones proporcionando las siguientes funcionalidades.

#### Proveedor de identidad (IdP):

Proporciona validación de identidades de usuarios, gestión del nivel de confianza de la autenticación según NIST AAL/eIDAS Assurance Level, Federación de identidades y SSO entre aplicaciones.

Incluye mecanismos de autenticación basados en PKI, SMS/Email OTP y Safelayer Mobile ID (\*). Soporta plugins de autenticación para incorporar otros servicios de autenticación.

#### Proveedor de firma electrónica (eSigP):

Gestiona el material PKI de los usuarios como atributos de identidad en un repositorio seguro y auditado basado en un HSM. El usuario puede disponer de uno o varios certificados digitales para firmar electrónicamente documentos una vez identificado por el IdP.

Las funciones de firma están disponibles como servicio Web o con el componente de Tarjeta Virtual de Safelayer (\*).

#### Estándares de integración:

Soporte los estándares SAML y OAuth/OpenID Connect para Web SSO. Las funciones de firma están accesibles como API Web, soportando los formatos ETSI PAdES, XAdES, CAdES y RSA PKCS#1.

Visite nuestro  
portal de demos:  
[demo.safelayer.com/id](http://demo.safelayer.com/id)

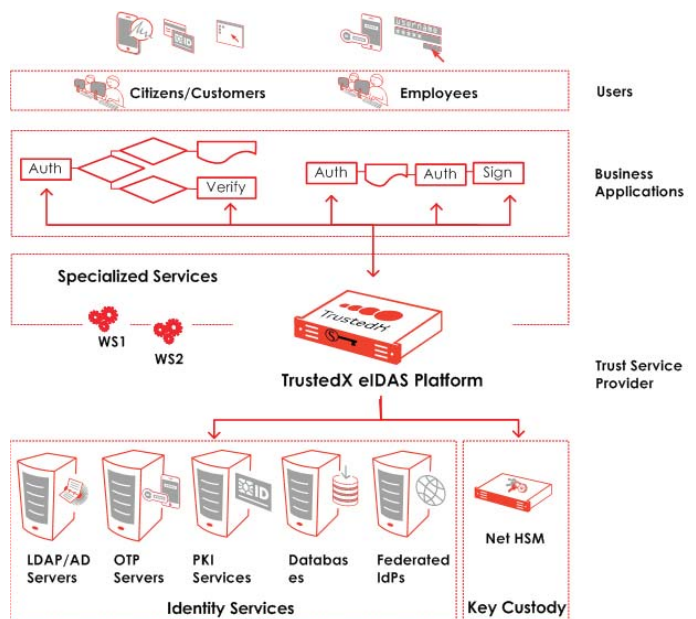


### Arquitectura

TrustedX proporciona las funciones de autenticación multi-factor y firma remota de usuarios a las aplicaciones a través de servicios web de ámbito corporativo u operado por un prestador de servicios de confianza.

En la figura se muestran las interacciones de TrustedX eIDAS con los siguientes componentes de infraestructura:

- Servicios de Identidad: Pueden incluir el Servidor LDAP (para atributos y autenticación), servidor de Autenticación (por ejemplo, OTP), Servicios de PKI, Bases de Datos y/o IdPs federados.
- HSM en red: Dispositivo de seguridad criptográfico que garantiza la protección de las claves privadas PKI de los usuarios.
- Otros componentes (no mostrados en la figura): Servidores de correo, Servidor de SMS, sistemas de monitorización



### Características técnicas

- **Formato:** Software appliance. Consultar para más información sobre entornos hardware o virtuales homologados.
- **Estándares de autenticación:** Soporta OASIS SAML 2.0 y OAuth 2.0/OpenID Connect.
- **Mecanismos de autenticación nativos:** Certificado digital, SMS/Email OTP, LDAP/AD, Safelayer Mobile ID.
- **Mecanismos de autenticación de terceros:** Mediante plugin de autenticación. Consultar.
- **Clasificación de la autenticación:** eIDAS Level of Assurance / NIST Authenticator Assurance Level (AAL) / ITU-T X.1254 / ISO/IEC 29115.
- **Estándares de firma electrónica:** ETSI TS 101733 - CAdES, ETSI TS 101903 - XAdES, ETSI TS 102 778 – PadES y RSA PKCS#1.
- **Gestión de certificados digitales:** Plataforma PKI KeyOne de Safelayer o PKIs de terceros mediante conector PKI de TrustedX.
- **Soporte de HSMs:** Fabricantes Thales nCipher y SafeNet. Consultar para productos homologados.
- **Monitorización de eventos:** Simple Network Management Protocol (SNMP). Syslog y formato raw para procesar con SIEM externo.
- **Sistemas de base de datos y directorio:** Oracle, Microsoft SQL Server, My SQL o Maria DB. Protocolo de acceso a directorio LDAP.
- **Pasarela de SMS/Email:** Requerida pasarela SMS y/o servidor SMTP para mecanismos OTP.

(\*) Consultar ficha del producto para más información de este componente.