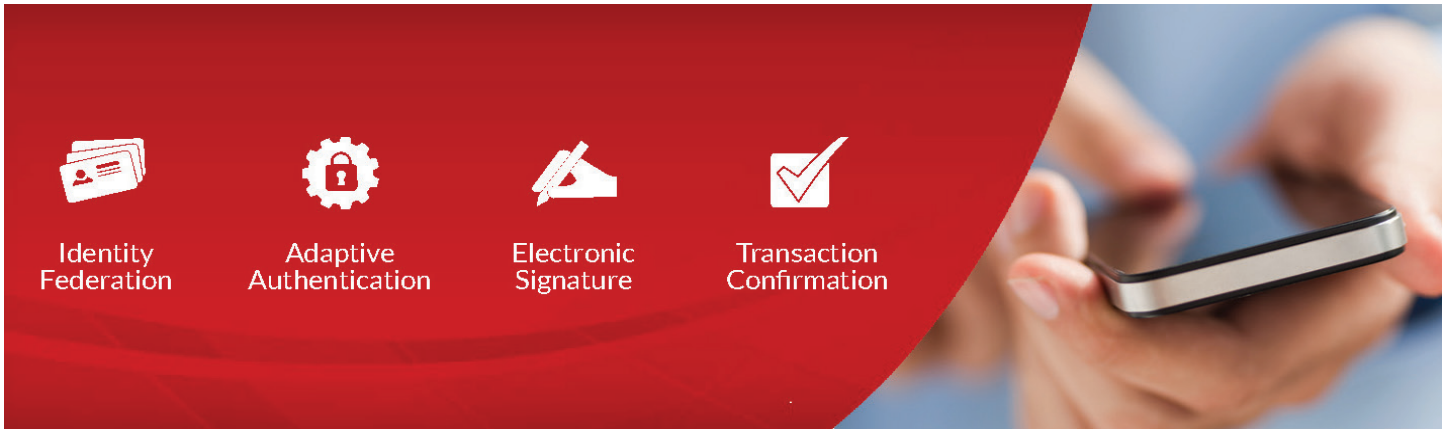


TrustedX

eIDAS

Description

Trust services platform for Web/Cloud environments:

- Identification, 2FA authentication and electronic signature services from any device.
- Mobile ID, easy and secure use of mobile to identify users.
- Legally binding signature with non-repudiation capabilities.
- Identity federation, SSO with dynamic trust level management (AAL).
- Remote signing with PKI keys protected in a HSM.
- Complete set of Web APIs for application integration.
- Highly scalable in number of users and transactions per seconds.
- Compliant with eIDAS Regulation and PSD2 Directive.

Benefits

All-in-One platform

TrustedX operates as a back-end where identification, authentication, authorisation, SOO, identity federation and signature services (advanced or qualified) are centrally and securely managed while providing accurate user identification. All services are available via WebAPIs.

Trust elevation

TrustedX eIDAS provides an adaptive authentication engine that classifies the level of trust of every authentication method (as defined by NIST's ALL/ eIDAS's assurance levels). The adequate trust level is raised by sending additional challenge out-of-band such as SMS/email OTP or Safelayer's Mobile ID notification.

Cloud signing

Management of public key infrastructure (PKI) identity attributes and remote signing functions in accordance with the CEN 419 241 technical standards. Ongoing Qualified Signature Creation Device (QSCD) certification to be operated by Trust Service Providers (TSPs).

Standard integration

Thanks to the support of the REST Web services API implemented via the OAuth 2.0/OpenID Connect, SAML and ETSI's *AdES signature format standards, basic HTTP tools available in any environment/language for integration can be used.

Security and auditing

The system records and aggregates identification, authentication and electronic signature information as per the security requirements applicable in the technical standards associated to the eIDAS Regulation.

TrustedX

eIDAS

Operation

The TrustedX eIDAS platform acts as an identity provider (IdP) and a signature provider (eSigP) for the users in their interactions with the applications by providing the following functionality.

Identity provider (IdP):

Validates user identities, manages the trust level of the authentication as per NIST's ALL/eIDAS's assurance levels, and provides identity federation and SSO between applications.

It includes authentication methods based on PKI, SMS/Email OTP and Safelayer Mobile ID (*). Supports authentication plug-ins for incorporating other authentication services.

Electronic signature provider (eSigP):

Manages the PKI material of the users as identity attributes in a secure and audited HSM-based repository. The user can have one or more digital certificates for electronically signing documents once identified by the IdP.

Signing functions are available as a Web service or via the Safelayer Virtual Card component (*).

Integration standards:

It supports the SAML and OAuth/OpenID Connect standards for Web SSO. Signature functions are accessible via a Web API. TrustedX eIDAS as well supports the ETSI PAdES, XAdES, CAdES and RSA PKCS #1 formats.

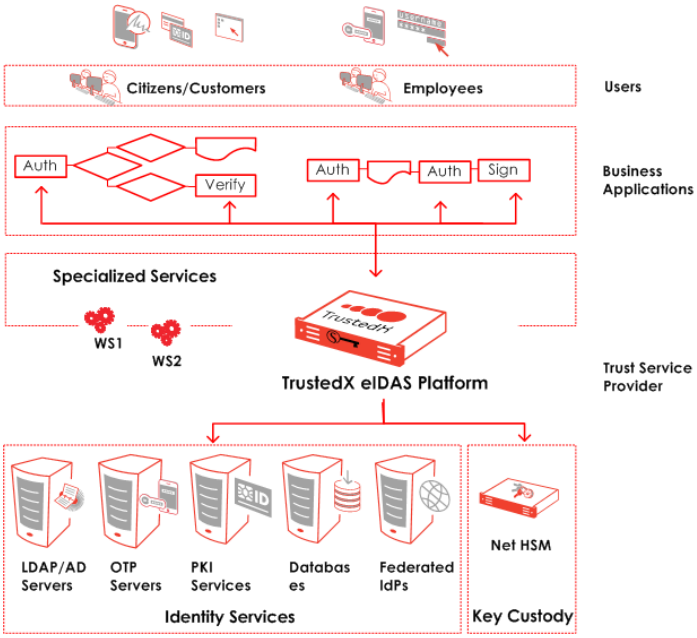
Visit our demo site:
demo.safelayer.com

Architecture

TrustedX provides multifactor authentication and user remote signing to the applications via corporate Web services or services operated by a trust service provider.

The following figure illustrates the interactions between TrustedX eIDAS with the following infrastructure components:

- Identity services: Can include the LDAP server (for attributes and authentication), an authentication server (e.g., OTP), PKI services, databases and federated IdPs.
- Network HSM: Cryptographic security device that guarantees the protection of user PKI private keys.
- Other components (not displayed in the figure): Mail servers, SMS servers, monitoring systems.



Technical specifications

- **Format:** Software appliance. Inquire for more information on approved hardware or virtual environments.
- **Authentication standards:** Supports OASIS SAML 2.0 and OAuth 2.0/OpenID Connect.
- **Native authentication methods:** Digital certificate, SMS/email OTP, LDAP/A/D, Safelayer Mobile ID.
- **Third-party authentication methods:** Via authentication plug-in. Consult for more Information.
- **Authentication classification:** eIDAS's assurance levels, NIST's authenticated assurance levels (AAL), ITU-T X.1254, ISO/IEC 29115.
- **Electronic signature standards:** ETSI TS 101733 - CAdES, ETSI TS 101903 - XAdES, ETSI TS 102 778 - PadES and RSA PKCS#1.
- **Digital certificate management:** Safelayer's KeyOne PKI platform or third-party PKIs via TrustedX PKI connector.
- **HSM support:** Thales nCipher and SafeNet manufacturers. Consult for more Information.
- **Event monitoring:** Simple Network Management Protocol (SNMP). Syslog and raw format for processing with an external SIEM.
- **Database and directory systems:** Oracle, Microsoft SQL Server, My SQL or Maria DB. LDAP directory access protocol.
- **SMS/Email gateway:** Required SMS Gateway and/or SMTP server for OTP methods.

(*) See the product sheet for more information on this component.

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