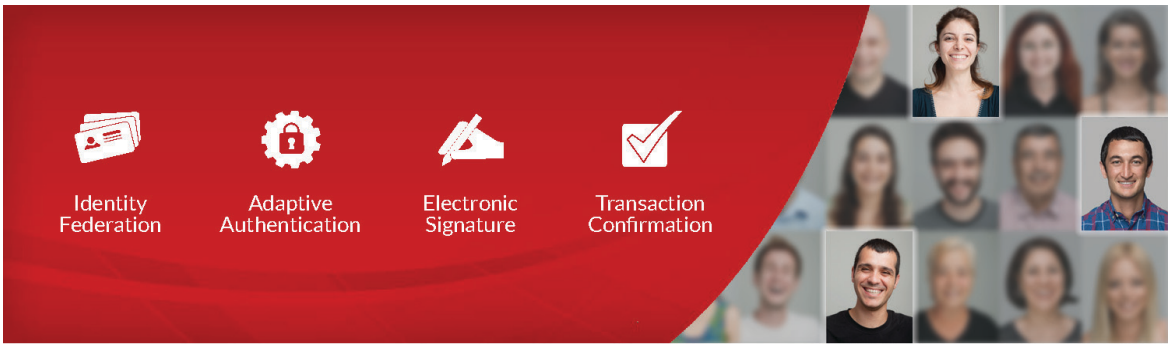

TrustedX: eIDAS Platform

Identification, authentication and electronic signature platform for Web environments. Guarantees identity via adaptive authentication and the recognition of either corporate, recognized or social identities:

- Includes authentication, single sign-on and identity federation functionality. Provides authentication methods based on context, behavior biometrics, one-time keys, digital certificates and mobile devices.

- Platform complemented through the incorporation of PKI identity attributes for developing electronic signature functions. Along with the authentication functionality, provides server and mobile device signature services, providing an integral solution for deploying the new eIDAS trust services.

Characteristics

Adaptive Authentication, Federation and SSO Methods

- Integration of the organization in Social, Mobile and Cloud (SoMoClo) media to assure a variable level of trust tailored to the applications.

- Adaptive authentication. Balances security, risk/cost and user convenience through the intelligent elevation of trust based on contextual information and the dynamic accumulation of multiple factors.

- Manages trust in the federation of identities and provides single sign-on (SSO) control between applications across different media and devices, adapting it to the variable trust requirements.

Electronic Signature Methods

- Two modes for the straightforward and uniform integration of advanced eSigning into applications on a server (e.g., in the Cloud) and in user devices (e.g., a mobile).

Safelayer Secure Communications S.A. is a leading provider of security software for public key infrastructure (PKI), multi-factor authentication, electronic signature, data encryption and for the protection of electronic transactions. - 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

Auditing and Regulations

- Provides a single point for data incorporation, audits, reporting and intelligence analysis on the use of credentials for authentication and eSigning.

- Serves as a technology framework for deploying applications and services based on the new European regulation on electronic identification and authentication services (eIDAS) and the new EU Directive on ePayment and financial services.

Benefits

Identity Provider/Broker

Acts as an identity provider and/or broker. Supports federation with external providers and enhances security in the authentication of existing users and groups. Also provides SSO between applications. Supports corporate directories (including AD/Kerberos), national eIDs and social identifiers (i.e., Google, Facebook, etc).

Electronic Signature Provider

The system treats PKI material as identity attributes and/or credentials and centrally manages them on the server or distributed on devices (e.g., mobiles) that can be used to perform advanced electronic signatures as set out in the new eIDAS regulation.

Integration Standards

Extends the control of corporate authentication to Cloud applications such as Google Apps, Salesforce and Office 365 through the implementation of generalized Web and Cloud protocols. Support for SAML 2.0 Web SSO and OAuth 2.0/OpenIDConnect 1.0, which facilitates the integration and deployment of applications promoting the API Economy.

Versatile Authentication

Integration of authentication and eSignature in multiple user devices based on browser and/or native applications (e.g., mobile devices). Thanks to the Web OAuth and OpenIDConnect protocols and Safelayer's Mobile ID app, integration in applications is very straightforward and highly secure.

Trust Elevation

An additional layer of security transparently assesses the authentication risk level by taking into account the user's profile, habits and biometrics. Users continue using their identities. They are only prompted for an additional authentication step when a certain risk threshold is exceeded.

Rules and Regulations

The new eIDAS regulation is of particular relevance. It puts forward functions and recommendations for assuring identity, authentication and the electronic signature with the aim of improving trust, security and interoperability between both public and private organizations, e.g., the new ePayment directive on financial services and the banking sector is based on the eIDAS regulation.

Operation

The eIDAS platform acts as an identity, authentication and electronic signature provider for multiple applications through the use of the following functionality and concepts:

- **Adaptive Authentication Policies:** Identity and authentication workflows are modeled that can accumulate identity attributes and request one or more authentication factors (deployed OTPs, SMSs, emails, etc.) explicitly or when a threshold of acceptable risk is exceded.

- **Authentication Method Classification:** Support for the level of assurance (LoA) identity classification as recommended by the new EU regulation (eIDAS), Spain's ENS regulations, the US's OMB/NIST 800-63 recommendation and the ITU-T X.1254 / ISO/IEC 29115 standard.

- **Trust Elevation y Step-up:** Methods for analyzing the user's context (the user's device, location and connection habits) are incorporated along with an improvement in security (intuitive server authentication, device registration, typing rhythm) that allow elevating the trust within an LoA or skipping to another level depending on the risk configured and detected.

- **Adaptive Single Sign-On (SSO):** User authentication in multiple applications is streamlined while observing security requirements. Two types of SSO are supported: i) by LoA and ii) by factor. In the first, SSO only occurs if the destination application requires an LoA less or equal to that obtained in a prior authentication. In the second, SSO only occurs if the factors required were successfully passed previously. If SSO cannot be applied, step-up reauthentication (factor accumulation) can be forced.

- **Federation:** The can connect with any external identity provider and in particular with social networks (e.g., Facebook, Google plus, etc.) to incorporate new sources of users and identity information. It also acts as an identity provider for external service providers and in particular with Cloud/SaaS applications (e.g., salesforce, Google Apps, Office 365, etc.). All the applications integrated in the federation can also make use of the trust elevation, step-up and adaptive SSO functionality.

- **Electronic Signature:** As an identity provider, the system can authoritatively manage PKI attributes (keys and certificates) associated to the identities and can also in this way act as an eSignature provider. The PKI key attributes are protected by a secure container that can be on the server itself, in an HSM or on a user device, e.g., a mobile, in all cases under the exclusive control of the user. Only user–owners of the key attributes can access these attributes via an eSignature service.

- **Mobile eIDAS:** The platform can be complemented with the “Mobile ID" mobile application (app) that protects PKI keys and certificates transparently and in a user-friendly way. This app, in cooperation with the eIDAS platform, lets the user perform PKI strong authentication and advanced electronic signing in any Web application either on the mobile or another device. In practice, it follows the recommendations of the eIDAS regulation.

- **User-centricity and Privacy:** The system is based on a user-centric identity management paradigm, which means that it is the user in the last instance who authorizes the identity provider to provide identity information to the applications and services requesting it. The protocols used are OAuth 2.0, OpenIDConnect 1.0 and SAML 2.0 WebSSO, which use the user as the point of interconnection between the providers. The OAuth and OpenIDConnect protocols respect the privacy of user data.

- **Integration, Interoperability and the API Economy:** The system is completely based on Web technologies: REST, HTTP, HTML, JavaScript, JSON and Web OAuth and OpenIDConnect protocols, which means that the organization can provide its community with an authentication and authorization API to identity information on its users along with a delegated eSignature service with which applications can request eSigning authorization on behalf of users. Furthermore, an infinite number of systems and third-party tools support these Web technologies.

- **BigData and Intelligence:** As the system is user-centric, it accumulates and adds identity information, context, credentials, authentication attempts, SSO, service and application authorization, etc., that the user performs via the platform. This generates a lot of information about the user that seen together with the entire population provides potential for a very valuable intelligence analysis for the company, both in terms of security and incident prevention and for insights on the user community.

The following is a use-case example:

- A user is usually logged in to Facebook in their portable computer. At a given moment, they access an e-commerce application (RP). This application delegates to an identity provider (IdP) federated with Facebook so that when the primary authentication starts, as the user is already logged in, the IdP obtains information on the user from Facebook without the user having to re-authenticate.

- The IdP's authentication flow was configured to transparently analyze the user's context information so that if it is the first time that the user accesses using the device and/or from a new country geolocation, the user must enter an OTP sent via SMS. Once the OTP has been entered, the system registers the device and the location as trusted so that further accesses detect this situation and do not request more factors from the user.

- At this point, the platform assigns a medium level of assurance (LoA) to the user's identity. With this trust, the user has read access to their e-commerce profile, including the purchase agenda, mobile telephone number, delivery addresses, direct debit accounts, personalized offers, etc. However, with this medium level they cannot make changes to or write to their profile.

- The user purchases a digital product for which they need to authorize a direct debit in their bank account. At this point, and in cooperation with the account owner's financial entity, the system detects that the user has a mobile signature key (Mobile ID app) and sends a transaction acceptance notification for the user to sign electronically.

- The user now wants to enter a new delivery address into their profile. When the user accesses the form, the system detects that the LoA is “medium” and that to edit the profile, a "high" level is required. As a result, the system sends an authentication notification to the user's mobile (Mobile ID app) so the user can perform a PKI strong authentication that will result in a high LoA.

This use-case example aims to demonstrate the versatility and potential of the platform for resolving identity security demands that arise depending on how critical the service to be consumed is or the risk attached to it. The methods described in the example can be replaced by others more suited to the service being provided.

Architecture