TrustedX

Authentication Platform

Description

Adaptive authentication and federation platform for Web and Cloud environments:

- Supports corporate, social and government authentication mechanisms.
- Step-up authentication. Authentication trust level assessed and increased when required by the application.
- Context information analysis. Enhances authentication security without affecting the user experience.
- Identity federation trust management. Single access control between applications.
- Authentication reporting system for quick response to security problems.

Benefits

Identity provider

Acts as an identity provider, allows federation with external providers and enhances the security in the authentication of existing users and groups. Supports corporate directories (including Kerberos), national eIDs and social identifiers (i.e., LinkedIn, Facebook, etc).

Layered security

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

Cloud Applications

Integrates the authentication control for Cloud applications such as Google Apps, Salesforce and Office 365 through the implementation of standard Web and Cloud protocols. SAML 2.0 and OAuth 2.0 / Open ID Connect are supported for the federation of applications

Centralized control and auditing

Authentication factors can be tailored to each user group (employees, collaborators, clients, etc.) and application. Single sign-on managed according to the required trust level. Quick response to security incidents. Centralization of all the audit information — data provided on each authentication decision.

TrustedX

Authentication Platform

Functions

The authentication platform acts as an identity provider for the applications and enables customizing the authentication in each case using:

- **Adaptive authentication workflows:** which form an authentication process that can request an additional step (deployed OTPs, SMS, etc.) when a threshold of acceptable risk is exceeded.
- **Context analysis policies:** which analyse the user's device, location and connection habits to assess the risk of the authentication. Each policy is highly configurable and supports establishing which factors are considered and their weightings.
- **Authentication method classification:** which determines the security level reached in each authentication.
- **Single Sign-On (SSO):** which streamlines the authentication of the users in multiple applications while respecting the security requirements.
- **Intuitive server authentication:** which safeguards users against phishing and pharming attacks and entails the users having to recognize a customized image in the authentication interface.
- **User consent:** It ensures that the user knows which identity information will be transferred to applications and which kind of operations can be done on the user behalf.

The following are the characteristics of the context analysis:

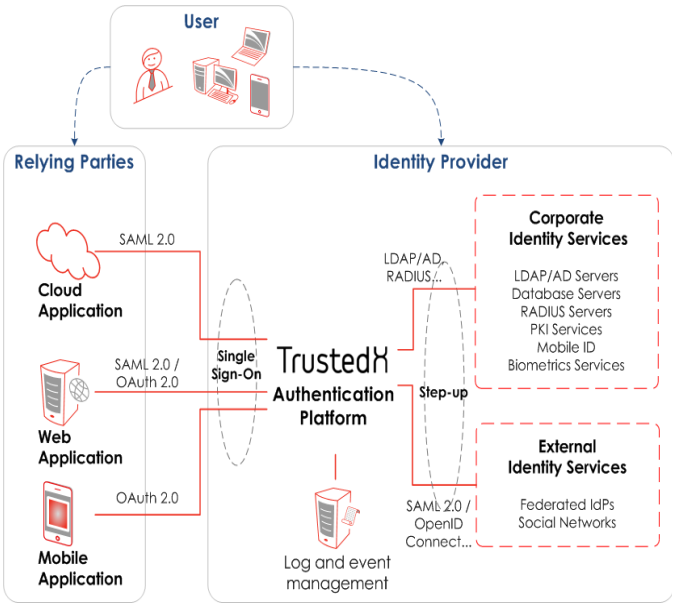
- TrustedX keeps a profile for each user. This profile is updated progressively and transparently after each access. In the interest of privacy, profiles can be abstracted from the explicit user identities.
- Users can explicitly register trusted devices. TrustedX can recognize the devices registered by a user and any other devices used by that user.
- TrustedX recognizes the user's keystroke dynamics. Keystroke dynamics is a biometric factor that does not affect the user experience.
- Network information can be used to obtain the geographic location of the user, recognize locations the user has previously visited and even check whether the user accessed with the same device from this location. It can even check if the user could have physically traveled between two consecutive access locations.
- The risk assessment of an authentication can be determinant if the user is required to pass a set of factors. Alternatively, the risk can be assessed using a weighted combination of several factors. Optional factors can be used to detect minor anomalies.
- The platform provides detailed reports and graphs on the authentication factors analyzed in each access, both for auditing purposes and for fine tuning the policies applied in each use case.
- The capture of all the context factors uses browser and server technologies (JavaScript) that do not require applets or plug-ins or the installation of software in the user devices.

Applications can invoke authentication functionality using the SAML 2.0 (e.g., Google Apps, Salesforce and Office 365) and OAuth 2.0 (adapted for mobile applications) protocols, both HTTP based. In each authentication response, TrustedX includes the identity attributes required for applications to establish their own sessions. The platform also supports the applications invoking the TrustedX signature and encryption services.

Architecture

TrustedX mediates between user applications and identity services both managed by the corporation (such as Safelayer Mobile ID) or by third parties (partnerships, social networks, etc.). The platform provides several strategies for integrating the authentication:

- Using TrustedX's end user authentication interface.
- Mimicking the authentication in the application interface, which provides a user experience that is totally harmonious with the applications.
- Externalized in other identity providers, and complemented with TrustedX's adaptive authentication and SSO functionality.
- In addition, TrustedX can be a source of information for business intelligence tools.



Technical Specifications

- **Format:** Software appliance. Contact for more information about supported hardware or virtual machines.
- **Event monitoring:** Simple Network Management Protocol (SNMP).
- **Database and directory access:** Oracle, Microsoft SQL Server and MySQL. LDAP directory access protocol.
- **Integration with SMS gateways and e-mail servers** for additional authentication.
- **Access to authentication services:** Authentication based on LDAP/AD, RADIUS, etc.
- **Integration in applications** using SAML 2.0 and OAuth 2.0. HTML/JavaScript technologies.
- **Trust level classification:** Based on OMB/NIST SP 800-63-1 (LoA classification) and the ISO/IEC FDIS 29115 standard

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