TrustedX - PKI Authentication

Whitepaper

CONTENTS

Introduction **3**

1 – TrustedX PKI Authentication **4**

Use Scenarios 5
Operation 5
Architecture and Integration 6
SAML and OAuth *7*
RESTful Web Services *8*
Monitoring and Auditing 9
Event and Auditing Management *9*
Monitoring and Alerts *9*

Introduction

The need for identification is a constant in all security systems. Authentication is the process that guarantees the identity of the other party. Its reliability is fundamental for improving security in electronic identification.

Safelayer's TrustedX is a platform that provides a set of security services based on (i) public-key cryptography (PKI) based authentication mechanisms, electronic signature and data encryption, or, (ii) authentication mechanisms based on context information and behavioral biometrics.

The platform can be deployed in a SaaS (Software as a Service) context for providing security services for governments, companies and different industries. The security services provided are accessible as Web services via the SOAP (Service Oriented Access Protocol) and REST (Representational State Transfer) protocols.

The following are TrustedX's basic configurations:

- **PKI Authentication Platform.** PKI authentication service based on digital certificates and SAML and OAuth identity providers. Acts as a SAML/OAuth Identity Provider (IdP) and supports adding non-PKI authentication methods.
- **Adaptive Authentication Platform.** Authentication based on context information and user behavior to improve the security of password-based authentication methods.
- **Electronic Signature Platform.** Advanced electronic signature methods, including CAdES, XAdES and PAdES. Supports client and server signature schemes using a centralized keystore.
- **Encryption Key Management Platform.** Data encryption and decryption functionality accessible as a Web service. Supports centralized management and the custody of encryption keys with role-based access control.

This document outlines the characteristics of **TrustedX's PKI Authentication Platform**. For more information on the other TrustedX configurations (Adaptive Authentication, Electronic Signature or Encryption Key Management), please request the corresponding white papers.

CHAPTER 1

TrustedX PKI Authentication

TrustedX PKI Authentication is a strong authentication platform for Web and Cloud environments that has the following characteristics:

- Centralized PKI credential server that supports SAML/OAuth federation and single sign-on (SSO and SLO).
- Trust level management for digital certificates and certification authorities (CA), for example: very high, high, medium or low trust.
- Supports adding other non-PKI authentication methods, which allows extending the range of use cases and being able to adapt to the requirements of service providers and different user groups.
- Enhanced authentication auditing. A centralized log system that generates security information in real-time that can be used for generating reports.

The following are the main characteristics of TrustedX PKI Authentication:

- **Integration and management of CA certificates.** Digital-certificate based authentication requires implementing PKI algorithms and managing the recognition of and interaction with multiple certification authorities (CA). TrustedX simplifies integration by removing all complexity from the applications and providing centralized management.
- **Trust level management.** TrustedX supports classifying other authentication methods according to their trust level (e.g., medium for passwords and very high for certificates), which means they can be applied depending on the value of the electronic assets and the business channels. Authentication methods can be added via protocols including RADIUS and LDAP using specific agents or federation protocols.
- **Direct and straightforward integration.** Guaranteed quick and efficient start-up in applications including Google Apps, Salesforce and corporate Web portals in general owing to the implementation of standard Web and Cloud environment protocols. Support for SAML 2.0 and OAuth 2.0, which facilitates the federation of applications using Web APIs.
- **Connection with identity repositories.** Connection with the organization's existing identity repositories, including LDAP and Microsoft AD. This means no additional identity or attribute management procedures are introduced. The platform acts as an identity provider. It increases the security in the authentication of the users and groups located in one or more repositories.
- **Uniform semantic interpretation.** TrustedX semantically and uniformly interprets identity attributes. It also assigns a trust level to the identity using discrete values and configurable labels (e.g., corporate, government) and supports complementing this information with other types of attributes from corporate repositories (e.g., with roles stored in LDAP).
- **Policy-based management.** Management is based on policies that allow tailoring the authentication factors to each user group (employees, partners, clients, etc.) and application according to the trust level required in each case.

- **Centralized control and auditing.** The server provides single sign-on access control (single sign-on and single logout), centralizes the quick response to security incidents and gathers audit information, providing data on each authentication decision that can be used in the corporate security audits.

Use Scenarios

Safelayer's authentication solution is aimed at protecting Web applications, portals and SaaS applications in the Cloud for different user groups, including the employees, partners, suppliers and clients of an organization and citizen users of public services.

- **Client/citizen applications.** Web applications that require high levels of security and must be easy to use while keeping installation in user stations and logistics to a minimum (e.g., citizen and client portals for public services, retail and banking).
- **Corporate applications.** Includes the authentication for accessing external applications, such as Salesforce and Google Apps, from anywhere and the authentication for Web applications and portals for employees, partners and suppliers.

In all use scenarios, authentication is centrally managed based on corporate security policies. Auditing is kept within the organization, regardless of whether the application is hosted on-premises or in the Cloud.

TrustedX minimizes the integration of the authentication in the Web applications and is also prepared for integrating new Cloud applications to meet future needs. TrustedX's strengths include:

- Not implementing proprietary identity management procedures. TrustedX operates as an additional layer providing enhanced security.
- Capability for applying different authentication policies according to type of user (citizens, partners, employees, clients, etc.) or application.
- Delegation of the entire authentication process to TrustedX. Once authenticated, the user can access other Web and Cloud applications.
- Centralized management in the organization of auditing and access control alongside the management of other corporate applications.

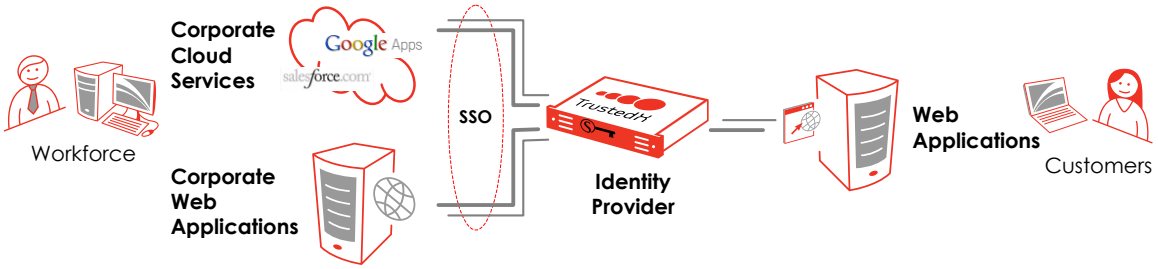

Figure 1-1. TrustedX PKI Authentication use cases for workforce and protecting customer-oriented Web applications.

Operation

The TrustedX authentication platform acts as an identity provider (IdP) for the applications. It adds the identity attributes of the corporate repositories and supports defining the authentication's security level in each case based on the following concepts.

- **Certificate validation.** PKI functions for validating certification chains and querying certificate status. Support for OCSP/CRL and customized mechanisms (e.g., third-party platforms and databases).

- **Federation, single sign-on (SSO) and single logout (SLO).** Streamlining of user authentication in multiple applications that observes all security requirements. TrustedX maintains the user's authentication session so the user does not have to re-authenticate on changing applications. The logout is also propagated to all applications.
- **Addition of new methods.** Support for native authentication mechanisms based on passwords and digital certificates. New methods can be incorporated using agents, or the validation can be delegated to third-parties via RADIUS or LDAP/AD. Identity federation via SAML is also supported.
- **Authentication method classification.** TrustedX keeps a catalog of authentication methods (supported by TrustedX or provided by third parties) classified by their trust level, e.g., the methods can be classified according to the four LoA levels of the NIST or the equivalent ITU-T X.1254/ISO/IEC 29115 levels.
- **Object and entity management.** Management of platform entities and objects. External repositories such as user LDAP/AD, databases or files can be added.
- **Auditing and accounting.** Secure and uniform centralization of log data on access control and certificate validation. The log system supports incorporating specific entries, which facilitates management with third-party tools.

Architecture and Integration

Safelayer's authentication solution can be deployed alongside an existing authentication and authorization solution in the applications to provide additional levels of security. It can also be deployed with the support of third-party tools and identity services (e.g., databases, LDAP/AD directory, RADIUS servers and/or PKI trust services).

TrustedX's software is available in appliance format and can be executed on hardware and in Safelayer-approved virtual environments. The system requires an external database system for managing the configuration data and storing data on profiles, log records and auditing (not shown in the following figure).

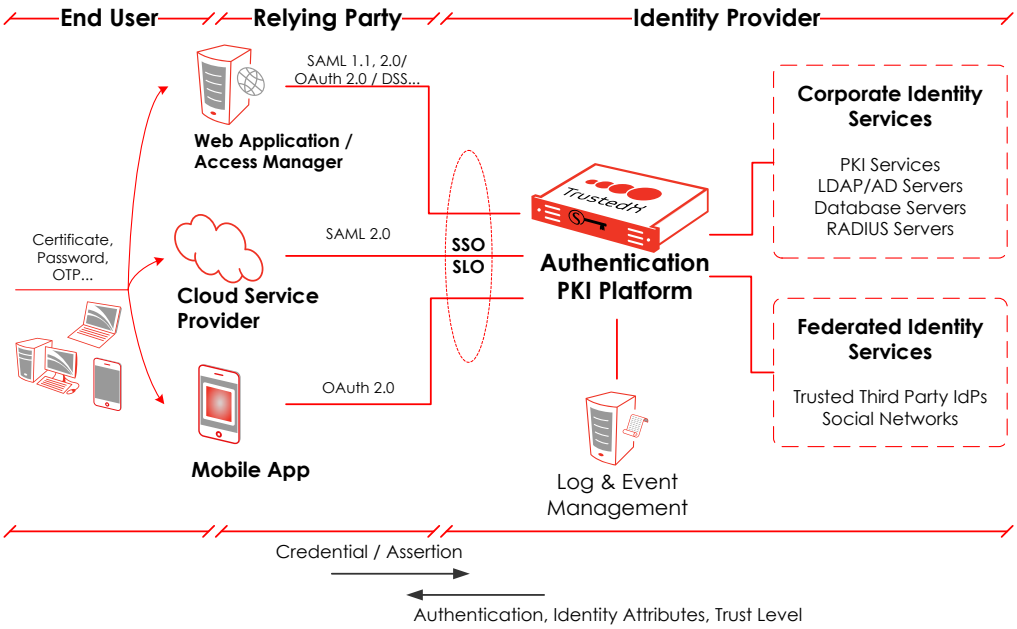

Figure 1-2. System architecture.

For integration with applications (relying parties, RP) TrustedX's authentication service is the base on which the system develops its value-added functions such as authentication, obtaining of identity attributes, authorization management and access control, and centralized auditing.

TrustedX acts as an agent between the user applications and the identity services. The applications use protocols based on HTTP, OAuth 2.0 or SAML 2.0 to invoke TrustedX. The following are the different authentication integration strategies supported by TrustedX:

- **Standard authentication**, which uses TrustedX's end-user authentication interface. The integrated Web application (RP) redirects users to TrustedX's standard login page, which directly interacts with the user for authentication.
- **Authentication with delegated graphical interface**, which provides a user experience that is more harmonious with the applications. The login page is included in the integrated relying party (RP), which TrustedX delegates the capture of primary credentials to.
- **Authentication externalized** to other, already deployed, identity and authentication providers. In this case, the login page is managed by the federated identity provider and the primary authentication process, which can be complemented with context information, is independent of TrustedX

TrustedX's services can be deployed in high availability so that they are always accessible. The architecture for this high-availability deployment is illustrated in the following figure:

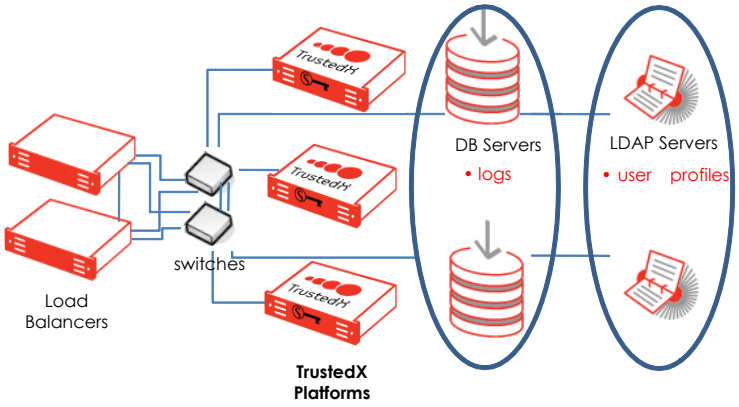

Figure 1-3. TrustedX high-availability deployment.

This architecture has a cluster formed by two or more TrustedX appliances to which a load balancer, also in high availability (e.g., active/passive configuration), distributes the requests received from clients. All the systems and resources (log databases, LDAP servers, HSM devices, etc.) accessed by the TrustedX services must also be in high availability.

SAML and OAuth

TrustedX can act as an SAML or OAuth identity provider (IdP) as it offers the following functionality in addition to authentication:

- **Management of identity attributes.** The solution supports using different identity repositories that are found in production, based on standards such as LDAP/AD or databases, by mapping the identity attributes and the format of the service provided based on OAuth and SAML. The solution assumes the existence of an external user provisioning system that incorporates and updates the users and their identity attributes.

- **Session management.** Incorporates SSO and SLO functionality for all applications that use OAuth and SAML. Any user or application that starts a session in the IdP, either via SAML or OAuth, is uniformly maintained for all applications, regardless of the protocol. This characteristic is ideal for creating a uniform integration environment between on-premise and Cloud-based corporate applications.
- **Federation management of IdPs** that represent different trust circles or domains. Future versions of TrustedX will support OAuth (as the client) for implementing broad federation. For SAML, the Web Browser SSO profile is supported for communication between the IdP and existing applications (mainly Cloud applications) that currently only support SAML.

TrustedX supports the SAML 2.0 Web Browser SSO profile and implements the set of minimum identity attributes required for acting as an agent for integrating with the Cloud applications (Salesforce, Google Apps, etc.). In general, this type of applications requires a subset of identity attributes such as "user_id" or "email". For OAuth, the Authorization Code Grant workflow of version 2.0 is supported. TrustedX is conceived essentially as an OAuth 2.0 provider.

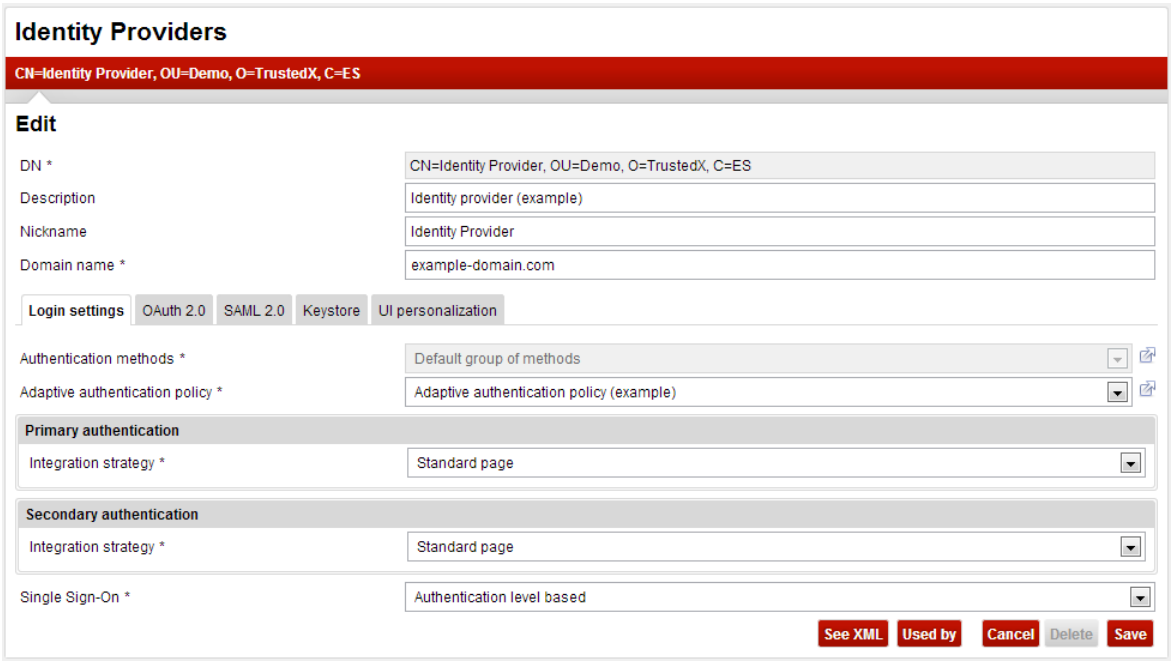

Figure 1-4. Each IdP can support one or more protocols and SSO and SLO and define its own authentication workflow.

RESTful Web Services

TrustedX makes use of a Web model based on the HTTP/JSON/HTML triple, a REST style (Representational State Transfer) distributed system architecture, design model and provision of contents and Web services. This means that TrustedX can be integrated and deployed in any Web environment using an API that hides all the actual complexity of the system.

The RESTful model lets integrators and programmers incorporate TrustedX's authentication services in their applications and Web environments using standard tools and frameworks in a very straightforward fashion.

RESTful Web services are also ideal in AJAX browser environments in which excellent user experiences can be attained with HTML and JavaScript without the user having to install any component beforehand. Furthermore, the RESTful programming and integration model is already so widespread on the Web that most environments, tools and application services offer it as the only use model.

RESTful Web model practice is supported by all current IT platforms, both for servers and end users. In terms of the end-user, support is possible:

- Via a Web browser application on desktops, mobile phones, tablets, video-game consoles, WebTV, etc.
- In end-user operating systems (MS Windows, Apple iOS, Google Android, etc.) that natively include support for processing Web technologies (HTTP/JSON/HTML) via Web engines (WebKit).
- Via the use of native-code (Java, Objective C, C#, etc.) tools (SDKs) available for all platforms, the RESTful model can be followed for the straightforward integration and programming for the inclusion of any content and Web service.

Monitoring and Auditing

One very important aspect of security in general and of authentication in particular is the logging (generation and storage), search, recovery and analysis of events and presentation of conclusions (reporting) for i) security auditing, ii) reports on regulatory compliance, iii) monitoring and security alerts, iv) system observation and tuning, and v) obtaining activity reports (e.g., for invoicing).

To meet these needs, TrustedX has a complete system for generating reports that has its own graphical analysis console (e.g., for system observation and tuning in the training period). This system integrates in a straightforward manner with third-party SIEM and SNMP monitoring tools as it supports standard logging formats (e.g., for connecting with corporate monitoring and alert systems).

In general, the system was designed to include logging and reporting functionality and capability sufficient for basic system operation and exploitation. However, for advanced functionality of this type, e.g., for adding and correlating events, compliance reports, advanced governance and auditing processes, long-term data storage, etc., external tools are required, usually a SIEM with such functionality.

Event and Auditing Management

TrustedX events can be exploited using external tools (normally, SIEM tools) and used to correlate information associated to the authentication events to events of other IT components of the organization to compile more complete auditing reports and for a more effective detection of anomalies.

For organizations (and service providers), TrustedX also provides information that can be used for tracking the use of the IT assets provided as services. To do this, TrustedX provides different log information services and formats. Logging can be processed with external tools as follows:

i) Using an external Security and Information Event Management (SIEM) external tool that applies intelligence functionality. To enable this, TrustedX supports generating log events in CIM format and using syslog stores.

ii) Via a Web service provided by the platform. The service provides the logging in XML format so that intelligence functions can be performed, including searching and locating more detailed information or any type of activity reports.

Monitoring and Alerts

TrustedX's Authentication solution generates multiple sources of information. Its monitoring can be used to generate alerts that can entail immediate administrator and operator actions depending on the severity of the alert.

The following is the list of information sources and monitoring methods available in the solution:

- Error and statistic information on system resource use via an SNMP source included in the solution. SNMP monitors (i.e. Nagios, OpenNMS, IBM Tivoli or HP Network Management Center) can be used to

map the network of servers dedicated to the Authentication solution, monitor the parameters and generate alerts for anomalous situations.

- Information on possible failures, functionality or execution errors of the processes that implement the solution via i) actively browsing the proprietary event logging or ii) "log4j" tool programming extensions. In the solution, the proprietary format of the events is made public through browsing a database or file or also via using the Web service API provided.
- Through the analysis of the events generated by TrustedX in CIM format sent to a syslog server, optionally through the support of SIEM tools and in real time, to obtain information on possible failures, execution or functionality errors of the processes that implement the solution.

TrustedX PKI Autentication

Safelayer Secure Communications, S.A.

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