



TrustedX - Adaptive Authentication Whitepaper



CONTENTS

1 – Introduction	3
Adaptive Authentication	4
Identity Federation	4
Safelayer's Solution	5
Use Scenarios.....	6
<i>Workforce</i>	6
<i>Consumers</i>	7
2 – TrustedX Adaptive Authentication	8
Operation	9
<i>Security Factors</i>	9
<i>Authentication Workflows</i>	15
Architecture and Integration	17
<i>SAML 2.0 and OAuth 2.0/OpenIDConnect</i>	18
<i>RESTful Web Services</i>	19
<i>Mobile Devices</i>	20
Monitoring and Auditing	20
<i>Authentication Risk Analysis</i>	21
<i>Event and Auditing Management</i>	22
<i>Monitoring and Alerts</i>	23



Introduction

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

The ideal authentication method provides a level of security appropriate to the risks while also being easy to use in different types of terminals (PCs or mobiles). An inadequate authentication method increases costs and hinders making security advances. Some of the typical reasons organizations want to improve their authentication methods include wanting to:

- Mechanize the integration of authentication in Web applications and portals for employees and collaborators and also in Cloud applications such as Salesforce, Google Apps and Microsoft 365.
- Incorporate the recognition of identities managed by trusted third parties, such as collaborator entities and social networks, without sacrificing the security level required by the application.
- Improve the security of password-based methods without affecting the user experience. The new security factors must be very straightforward to use, especially for applications aimed at clients and citizens. They must also be adapted for mobiles.

Safelayer's authentication solution is a platform that assesses the risk level of the authentication and acts as an additional security layer, even for identities managed by third parties. The system transparently analyzes context information, including biometric parameters. It achieves an optimal balance between security, costs and ease of use.



Adaptive Authentication

For years the industry has opted for using different authentication methods according to the level of security required and the costs that can be assumed in each scenario. In general, the user password has been used for low levels of security and OTP tokens and digital certificates have been reserved for medium and high levels of security.

However, owing to new needs of security, mobility and ease of use, adaptive authentication is one of the most viable options for authentication because it improves the security of passwords and offers protection against phishing attacks while tailoring the mechanism to optimize security and the user experience.

Adaptive authentication is based on a combination of multiple authentication factors and aims to achieve greater accuracy and trust. It complements the current authentication method in use, such as the password, with context information it observes, correlates and compares to the information in the user's profile to assess the risk level of the login and the transaction.

Where a given fraud risk threshold is exceeded, an additional authentication factor is launched to guarantee the authentication's trust level. For instance, when the user tries to access from a device they have not used before, at an unusual time or from a location at a seemingly impossible distance to travel from the previous connection in the time between the last access and the current login attempt, there is a risk that the password is being used fraudulently, and the user is prompted for a second line of authentication.

Adaptive authentication provides the following advantages:

- **Ideal for mobiles.** The reduced size and limited ergonomics of mobiles complicate using certain hardware-based methods. Adaptive authentication is adequate for these environments and also makes use of the mobile as a second factor. It thus reduces costs and logistical problems.
- **Easy to deploy.** The authentication server provides an additional, transparent layer of security that analyses the user's context information. No installation is required in the user's terminal, which eliminates the cost of installing and maintaining software in client workstations.
- **Easy to use.** For the successful launch of new business channels, the user experience must be as fluid as possible. Adaptive authentication lets users continue to use the methods they are familiar with, and their experience is only affected when strictly necessary.
- **Lower property costs.** Costs are reduced through the use of one-time keys received by SMS or email or generated by mobile device apps when the use of OTPs, economical methods and less user support are required.

Identity Federation

Organizations have traditionally managed the entire life-cycle of the identities of the users accessing their applications from the moment they are registered until they are removed from the system, which entails the ongoing maintenance of the identity attributes. One of the most costly aspects of this life-cycle is the managing of the authentication credentials, i.e., providing support to users who forget their passwords, training for installation and use of new authentication methods, distribution and replacement of physical tokens, etc.

This approach is also evident in corporate scenarios in which each organization directly controls the identity attributes of the individuals forming part of it. Organizations, however, are becoming increasingly less isolated and business development units require exploiting new services and new forms of collaboration with user groups whose identities are not necessarily under the organization's control.

As well as increasing the options for extending services to external user groups, identity federation is also coherent with a more user-centered view that allows users to access services using the identity they want on each occasion, for instance, depending on the device they are using. The most typical case is federation with



the identity services of social networks, which enhance the user experience and foster user loyalty while being completely integrated in mobile platforms.

In short, identity federation is the capability to use user identities and attributes via different domains managed by different identity providers. Obviously, though, promoting the user experience can under no circumstances result in reduced security, and the authentication server remains the element that must continue to provide the assurance level required by the applications by adapting the authentication workflows in each case. For instance, if a collaborator authenticates with a LinkedIn social network identity linked to an existing profile in the corporate repository but conditions entailing some risk of identity fraud are detected, the authentication server must automatically prompt for an additional strong factor (e.g., a one-time password received by SMS in a verified telephone) for the identity requirements of the relying party to continue to be met.

Safelayer's Solution

Safelayer's authentication solution implements the adaptive authentication and federation concepts described above. Authentication factors tailored to the user experience and costs at any given time are used, and security is continually improved.

Context information is analyzed, including, optionally, behavioral biometrics. This information, which complements the first line of authentication, is continually checked and updated in the profiles of each user. Optionally, when the risk threshold established in the security policies is exceeded, TrustedX can launch an additional method, i.e., a second line of authentication.

The risk of the authentication is analyzed based on the following concepts:

- **Context information:** The user's devices and their characteristics are identified. Correlations between these devices and certain user habits, such as geographic location (based on IP data) and time range, are established.
- **Transparent biometrics:** Electronic signatures derived from interactions with the keyboard, by recognizing the user's typing speed, are detected. For mobiles, touch-screen interactions and gestures are recognized¹. This functionality verifies that the user's device is not being used fraudulently.
- **Other information:** In certain scenarios, other types of identity-related information relevant for the application (e.g., a user role) are verified. TrustedX supports assessing other information through queries on databases or directory attributes.

Context information is obtained from data observed without requiring the installation of applications in the user's workstation or using Java applets. In general, the browser environment is captured using JavaScript methods, system data and secure one-time cookies.

In terms of system versatility and the authentication methods supported, Safelayer's approach entails maintaining a catalog of own or third-party methods classified into levels of assurance² (LoA). When an application requires a given LoA, only methods that can provide this level or higher are used for authenticating.

The second-line methods provided by the solution consist mainly of second-channel OTP methods based on mobile devices, i.e., one-time codes sent by SMS or e-mail or methods based on native applications. Other third-party second-line authentication methods already in use in an organization can also be used.

¹ Future versions

² National Institute of Standards and Technology (NIST) Special Publication 800-63-1 "Electronic Authentication Guideline" (December 2011) classifies authentication trust into four levels (Levels of Assurance, LoA). This same four-level classification is defined in the new ITU-T X.1254/ISO/IEC 29115 standard.



Safelayer's solution provides federation and single sign-on (SSO) for integration. It acts as an identity provider and offers, in addition to authentication, identity attribute and session management and SSO functionality, which means the user does not always have to re-authenticate to access other applications.

Lastly, Safelayer's solution improves authentication auditing. It provides information for real-time analysis, which, furthermore, can be exported to SIEM/BI systems for monitoring, alert management and obtaining reports that facilitate detecting phishing attacks and security problems. For instance, when an attacker tries to use a stolen password, the second line of authentication is launched, and this is registered in the log records and in the auditing system.

Use Scenarios

Safelayer's adaptive 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 for government departments.

- **Corporate applications.** Includes authentication for accessing external applications, such as Salesforce, Google Apps and Microsoft 365, from anywhere. Authentication of Web applications and portals for employees and collaborators is also included.
- **Consumer applications.** Web applications that require high levels of security and ease of use, no installation in the user workstation and minimal logistics (e.g., client or citizen portals for retail, banking or government departments).

Furthermore, owing to its federation capabilities, the TrustedX Adaptive Authentication solution is also ideal for providing added-value security services to third parties. The managed security service providers (MSSP) are one option for the entire handling of the identity management procedures in certain government domains (e.g., citizens, civil servants, etc.). The services they can provide include the guaranteeing of the authentication of end users.

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

Workforce

Adaptive authentication aims to enhance security and reduce costs through optimizing the use of the authentication methods. TrustedX minimizes the work required to integrate adaptive authentication in Web applications and is also designed to integrate new Cloud applications to meet future needs.

In corporate environments, TrustedX's strengths include:

- No implementation of new management or identity procedures. TrustedX operates as an additional layer providing enhanced security.
- Different authentication policies can be applied according to user (employees, collaborators, clients, etc.) and application types.
- Delegation of the entire authentication process to TrustedX. Once authenticated, the user can access other Web and Cloud applications.
- Implementation of Web federation protocols. Direct integration of TrustedX into applications such as Google Apps, Salesforce and Microsoft 365.
- Centralized management in the organization of auditing and access control alongside the management of other corporate applications.



Consumers

In Web applications and portals for consumers such as clients and citizens, correctly adapting security and the user experience is especially important.

Improving the quality of passwords protects against brute force attacks but does not provide protection against phishing and pharming attacks. Furthermore, methods appropriate for PC environments, such as protection based on security questions or hardware tokens, are difficult to use in mobiles.

Safelayer's solution is ideal for mobiles as it adds transparent protection elements based on a context information risk analysis, which means the user's attention is only required when strictly necessary. One of the big advantages of this approach is that users can continue using their usual authentication method, which means their use experience is hardly affected.

In short, authentication trust is increased without having to change the method or require the systematic use of other methods such as hardware OTP tokens. In terms of the second line of authentication, the product is especially flexible as it can be implemented by sending a unique code by SMS, e-mail or even by integrating third-party methods, which gives it wide scope for adaptation to different security and usability requirements.



TrustedX Adaptive Authentication

TrustedX Adaptive Authentication is a strong authentication platform for Web and Cloud environments that provides the following benefits:

- A **layered security** approach: Multiple layers of security transparently mitigate the authentication risk by taking into account the user's profile, habits and biometrics. Users can continue using their passwords. They are only prompted for an additional factor when a certain risk threshold is exceeded, which means there is hardly any impact on the user experience.
- **Direct and straight forward integration.** Guaranteed quick and efficient set-up in applications including Google Apps, Salesforce, Microsoft 365 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/OpenID Connect, which facilitates the federation of applications using Web APIs.
- **Connection with identity repositories.** Connection with the organization's existing identity repositories, including databases, LDAP and Microsoft AD, and authentication servers via RADIUS. No additional identity or attribute management procedures are implemented. The platform acts as an identity provider and increases the security in the authentication of the users and groups located in one or more repositories.
- **Third-party identity federation and integration of arbitrary authentication methods.** Supports using identities managed and validated by third-party identity providers (e.g., social networks), invoking arbitrary authentication methods (OOB OTP, Kerberos tickets, X.509 certificates, etc.), and classifying them according to their security level.
- **Policy-based management.** Management is based on policies that allow tailoring the authentication factors to each user group (employees, collaborators, 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, centralizes the quick response to security incidents and gathers the audit information, providing data on each authentication decision that can be used in the corporate security audits.
- **Signature services scalability.** Owing to its modularity, TrustedX supports additional signature components based on digital certificates. The electronic signature supported by TrustedX meets the requirements of the EU directive on electronic signatures.

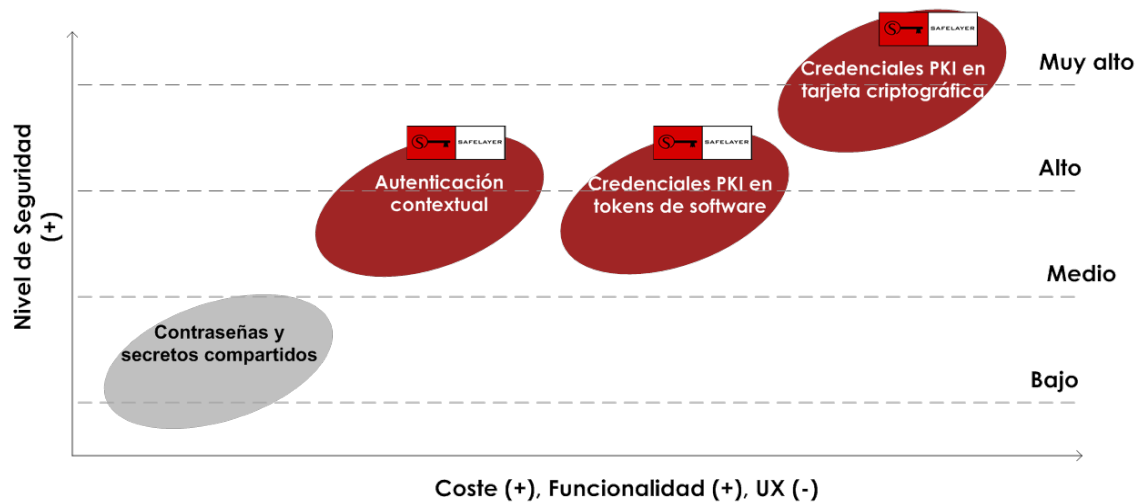


Figure 1: Position of Safelayer's Adaptive Authentication with respect to its PKI solutions.

Operation

The solution acts as an identity provider for the applications. It adds the identity attributes of the corporate repositories and other identity sources and guarantees reaching the authentication security level required in each case.

In the case of federating third-party identities, such as with social networks, the platform supports increasing the security level with adaptive authentication policies that can prompt the user for an additional authentication factor.

- **Context analysis policies.** The user's device, location and connection habits are analyzed to assess the risk of the authentication. Each policy is highly configurable and supports establishing which factors are considered and their relevance. The capture of context factors uses browser and server technologies that do not require applets or plug-ins or the installation of software in user devices.
- **Authentication method classification.** TrustedX maintains a catalog of authentication methods (supported by TrustedX or provided by third parties), each of which it associates security levels that determine the level of trust of each authentication, e.g., the methods can be classified using the four NIST LoA levels or the equivalent ITU-T X.1254/ISO/IEC 29115 levels.
- **Adaptive authentication policies** model a highly configurable and complete authentication workflow. Additional steps (e.g., a second line of authentication) can be requested when an acceptable risk threshold is exceeded (e.g., a unique code is sent in an SMS or e-mail message when the user wants to connect from a device they do not usually use).
- **Federation and single sign-on (SSO).** User authentication in multiple applications is streamlined while observing security requirements. TrustedX maintains the user's authentication session so the user does not have to re-authenticate when they change applications.

Security Factors

The risk analysis factors implemented by TrustedX to enhance the security of the first line of authentication, usually based on passwords, can be grouped under the following concepts:

- **Device and usual-context identification.** Verification that the user is connecting from a recognized device and in a usual context. Risk assessment is performed based on the correlation of device, location, and chronological parameters, etc.

- **User identification** via behavioral biometrics. Additional control for detecting if the user, voluntarily or otherwise, gave their credential to another user. This mitigates social engineering attacks.
- **Intuitive server identification.** Protection measures against phishing attacks, additional to the SSL/TLS security. Users can have customized images for each of their devices. This helps users detect fake websites designed to steal credentials.

The authentication risk assessment — executed by TrustedX and/or delegated to an external system — can be completely determinant if the user is asked to pass a set of factors. Alternatively, the risk can be assessed globally using a weighted combination of several factors. Optional factors can also be used to detect minor anomalies.



Figure 2: TrustedX management of risk assessment factors. The system allows determining which analysis factors are taken into account, which must be passed and which are optional.

The combination of the device fingerprint analysis and the use of one-time cookies constitutes a complex device identifier, as specified by the US's Federal Financial Institutions Examination Council (FFIEC).

Context and Device Identification

For "complex device identifier" based management, one-time cookies and fingerprints are used derived from multiple device parameters, including aspects of the operating system and browser configuration (current, later or earlier version; sources; installed plug-ins; etc.), geographical location and time range. TrustedX allows explicitly registering one or more usual and trusted devices, i.e., as a "something you have" authentication factor. On making such a registration, the user indicates that the device is always in their possession and under their control and, therefore, that use of it provides additional guarantees on the user's identity. As a result, a lower risk of identity fraud can be attributed to accesses performed with these devices compared to those performed with unregistered devices.

One-time double-cookie protocol

To safeguard against pharming attacks, Safelayer's solution includes an additional layer of security via a one-time double-cookie system. The first cookie (the *Hello cookie*) is linked to the name of the legitimate server's domain. The second cookie (the *DeviceID cookie*) is linked to a random path that is only known to the legitimate server that generated it.

In an advanced phishing attack, i.e., a pharming attack, the attacker manages to make the browser believe that the fraudulent server belongs to the same domain as the cookie to steal it more easily.

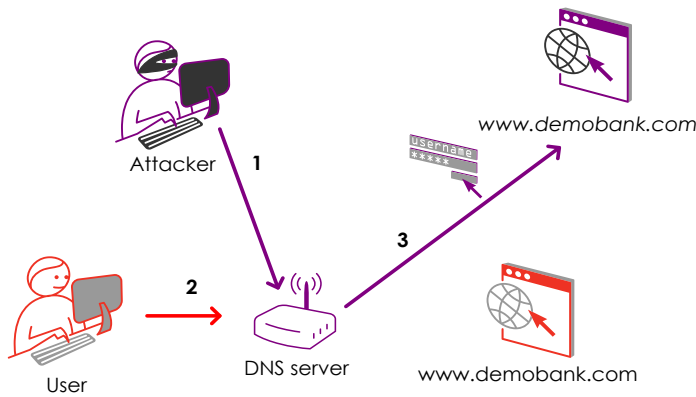


Figure 3: Phishing attacks are based on forging the DNS name system. The figure illustrates how the attacker diverts the user to a false `www.demobank.com` with the aim of tricking the user into submitting their credentials.

Thus, to identify the device, TrustedX waits to receive two cookies according to the following protocol. Firstly, the Hello cookie is received. The server uses this cookie to identify the device, which it redirects to a page with the exclusive path that the DeviceID cookie is associated to, which only the legitimate server knows. If the browser finalizes the protocol and sends the DeviceID cookie, the server can complete the device identification and, for example, display the customized image (intuitive server identification). This is how the mutual authentication process between the device and the server is carried out.

So, thanks to the one-time double cookie, fraudulent servers cannot cause the sending of the second cookie because they do not know the exclusive path it is associated to, and the phishing attack is aborted.

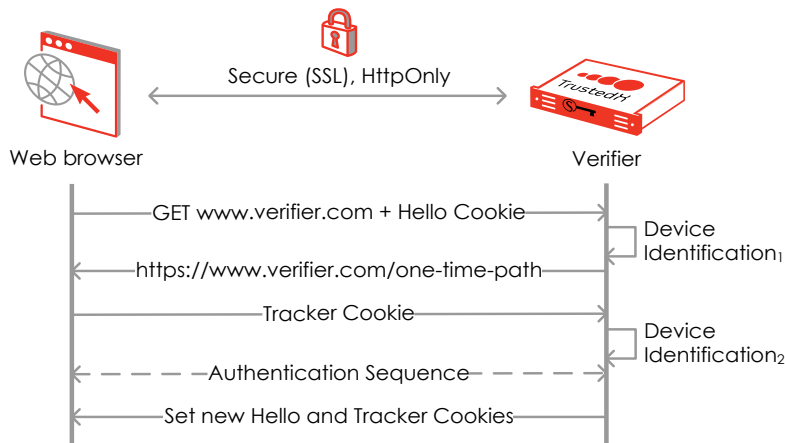


Figure 4. The one-time double-cookie protocol implemented by TrustedX.

Context analysis and capture

The user's authentication context is determined by certain characteristics and data of the environment in which the authentication process is performed, such as the device, network connection, location, time-range information and other data on the user's behavior.

If in consecutive authentications the context remains constant or only reasonable changes are made to it, the probability that the authenticated user is the legitimate owner of the credentials is greater than if the opposite occurs, i.e., the context changes notably over different authentication processes. The distance between contexts is determined in the context analysis phase and provides as a result the authentication's risk level. Basically, where there is a greater distance between contexts, there is a greater risk that an attempt of impersonating a legitimate user is occurring.



The capture of the user's context occurs at different times throughout the authentication process. A part of the capture occurs in the device in the application interface where the client enters credentials. The other part occurs in the authentication server. The process is as follows:

1. The client-side capture is performed transparently using a code that the authentication server sends securely to the browser or the user's application. This code is used to capture information on the device, such as the type and version of the browser and the operating system; screen characteristics; the device language and time range; installed plug-ins and sources; etc.
2. All these parameters are sent securely to the server, which compiles a fingerprint of the user's device. The device's fingerprint can be compared to the fingerprints of other devices the same user has used in previous authentications, which TrustedX uses to determine the degree of coincidence. For example, two different fingerprints can correspond to the same device where the browser version number has simply increased. However, the devices are considered different if the type of operating system has changed.
3. Additionally, network information including IP address and, in the near future, geolocation (latitude and longitude) are also captured client-side. This last piece of information depends on the device type. For example, in a desktop environment, the Wi-Fi network can be obtained, whereas in mobile environments, the GPS and/or GSM component can be obtained.
4. On the server side, the date and time of the authentication is captured, network information is captured again and the geolocation is also obtained from the IP address. The geographical location analysis can indicate risk situations when the system detects consecutive authentication attempts from locations that are geographically too far apart.

All the information compiled may or may not be used in the context analysis. The operator of the authentication solution controls which parameters are considered most relevant and useful as authentication factors for each user group.

User Identifier

Just as we generate a personal and distinctive stroke when we handwrite, a series of unique characteristics can also be detected when we type or perform certain gestures on mobile devices. So, while certain context parameters are used for identifying the device, behavioral biometrics are used by TrustedX to improve user identification.

TrustedX uses behavioral biometrics to detect attackers using the credentials of legitimate users in corporate environments, where it is very easy to replicate other authentication factors such as connection time-range and location, and is even relatively feasible to obtain the credential and device of another employee. In this case, TrustedX stores a biometric pattern for the user that is compared with that obtained when the user authenticates.

Current versions of TrustedX implement the keystroke dynamics analysis from one or more devices with keyboards (either physical or on-screen). The typing-speed analysis is a non-intrusive biometric method that can be totally transparently for users and does not require additional hardware sensors. It works as follows:

- The parameters that characterize the keystroke dynamics of each user and that are used to generate each user's biometric pattern are principally:
 - i) The time each key is pressed for.
 - ii) The time between the pressing of one key and the pressing of the next.
 - iii) The time between the releasing of one key and the pressing of the next.
- These time parameters are complemented with others that help to define the user's typing pattern with greater accuracy. For example, the system monitors:
 - i) Whether upper case characters and symbols are performed with the SHIFT keys or with shift lock and whether the numbers are entered with the number pad;

- ii) The number of times the DELETE or BACKSPACE key is pressed to determine whether the user usually make mistakes when entering their credentials;
- iii) The use of the TAB key or the mouse for moving between fields in a form, and the use of the ENTER key or the mouse for sending credentials.

Typing speed is captured in the applications (e.g., with JavaScript code that can be interpreted by all browsers), which means no specific software is required. Thus, the analysis system can be enabled while users continue using their credentials as they usually would.

System Learning

To perform an analysis of the authentication context, the system must have a knowledge base on the devices and the usual behavior of the users. This allows the system to determine if the authentication is being performed under reasonable conditions or if it is an anomalous situation that might indicate a case of identity fraud.

To build this knowledge base, the authentication system must define a training period. This training process can be:

- **Explicit:** Users repeatedly introduce their credentials in an interface expressly for training, or
- **Transparent:** The system stores samples of the contexts and, optionally, biometric data on the user in consecutive authentications.

During the training period, the authentication is monitored to check and adjust the system parameters. To do this, TrustedX provides a complete set of graphical tools for detailed and real-time monitoring (see Monitoring and Auditing for more information).



Figure 5. TrustedX support specifying the length of the training for a period of time and for a minimum of user accesses.

After the initial training phase, the user's pattern is continually updated with new samples captured during authentication processes as users can continue to change their usual connection conditions over time and even their biometric patterns as they get used to entering their credentials.

As each user can access from multiple devices, their keystroke pattern may be different in each device, depending on the characteristics of each keyboard. Thus, users should be allowed to carry out training in different devices to be able to take into account the different patterns.

For smartphones and tablets that have touch screens, the keystroke dynamic capture method is exactly the same as for devices with a desktop keyboard. However, the error rates of the analysis and registration processes are higher because 1) users usually use these devices in different positions and even when moving and 2) typing is more irregular and inaccurate than on a desktop keyboard. For this reason, future versions of TrustedX will include the option to detect other biometric factors such as the recognition of movements, which are better for mobile devices, while maintaining the level of effectiveness in the identification.

Website Identification

Phishing attacks are usually triggered when the user clicks on a link in an e-mail or Web page that takes the user to a replica site designed to steal the user's credentials. In general, users without a background in security find it very difficult to detect when they are being tricked into revealing their credentials.

The U.S. Federal Trade Commission's³ consumer warning page, to which most US banks and online services refer, lists good practices for safeguarding against phishing attacks, such as checking the icons on the browser bar and making sure that the website's URL starts with " https:". However, it also states that none of these indicators is infallible against some attacker techniques because the most sophisticated false websites also try to use digital certificates issued by the trusted authorities.

TrustedX provides an additional measure to website protection using SSL/TLS to facilitate detecting false websites for the greatest number of users. Users can select a personal image that is displayed in the form for entering credentials alongside the username and password fields.

Phishing protection derives from the fact that the customized image is different for each device (i.e., for each browser in an operating system account). Thanks to the one-time double-cookie protocol, even if the false website can exactly replicate the credentials' entry form, it cannot replicate the image the user expects to see.

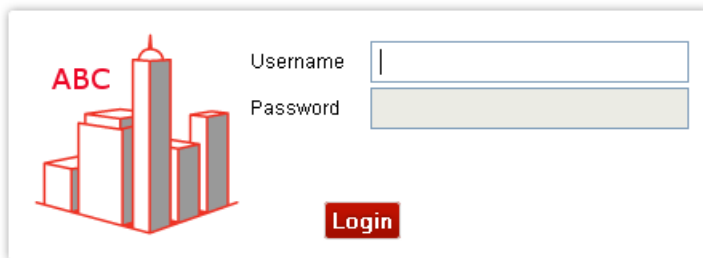


Figure 6. Website identification using an intuitive image.

In terms of use experience, if users do not see the image they expect in the login form, they will not want to enter their credentials and, therefore, the phishing attack will have been thwarted. Importantly, the customized form with the preselected image is different for each device used by the user and is displayed before the user has been identified.

Versatility and Other Methods

TrustedX can incorporate any type of credential and credential-validation protocol through the use of authentication connectors. The validation of a credential is mapped and standardized to a security level from LoA-1 to LoA-4, according to the NIST and ITU-T classifications referred to above.

By default, the Adaptive Authentication solution incorporates several authentication connectors for validating credentials. Using configurable policies, the system controls credential validation by following an authentication policy according to the requirements of each application. To do this, it implements own algorithms and also uses external support services, such as LDAP, RADIUS, OCSP, etc.

Thanks to these capabilities, the authentication process generates a dynamic and variable security level, as illustrated by the following examples:

- LoA-1: Authentication with a weak static password (e.g., Facebook's).
- LoA-2: Authentication with a strong static password provided by the organization that has more than 10 characters with letters, digits and punctuation marks.

³ FTC Consumer Alert, "How Not to Get Hooked by a 'Phishing' Scam", online, <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm>



- From LoA-2 to LoA-3: Adaptive authentication with a static password and risk analysis, additional identification and security measures and, optionally, a dynamic one-time password.
- LoA-3: Authentication with a strong static password used in a device explicitly registered by the user.
- LoA-3: Authentication with a PKI software-based credential, e.g., an X.509 certificate in a mobile app.
- LoA-4: Authentication with a PKI hardware-based credential, e.g., an X.509 certificate in a PIN-activated smart card.

These dynamic processes are modeled by authentication workflows that can entail various phases, which can include multiple credential validations, a risk analysis and the retrieval of attributes from identity repositories. Basically, authentication workflows are how the identity provider returns to the applications a set of identity attributes on the user with a given level of assurance.

Authentication Workflows

TrustedX orchestrates the authentication of the end user following an authentication flow selected from those available. Each authentication workflow is made up of a sequence of steps. The execution of each step can depend on certain conditions, such as the result of previous steps or the group the user being authenticated belongs to. Thus, each time a workflow is executed, a dynamic authentication process is achieved tailored to the user's characteristics and even the risk of identity fraud derived from the context of the authentication in question.

While the authentication workflows that an identity provider implemented by TrustedX can execute are highly flexible, the following stages are typically found in an adaptive authentication process:

1. Context capture (client-side) and first user-credential (validated by TrustedX or provided by a federated IdP).
2. First credential validation.
3. Context capture (server-side) and risk analysis.
4. Risk analysis and processing of the result analysis.
5. Optionally, capture and validation of the second user-credential.
6. Generation of the adaptive authentication response.

The process is designed to accumulate the level of trust of each of the stages: the capture and analysis of context information and the application of security enhancement measures transparent to the user being authenticated. Where the security enhancement measures are effective and the context analysis is positive, the authentication can reach a security level equivalent to LoA-3 for which only the username and password were introduced in the usual manner.

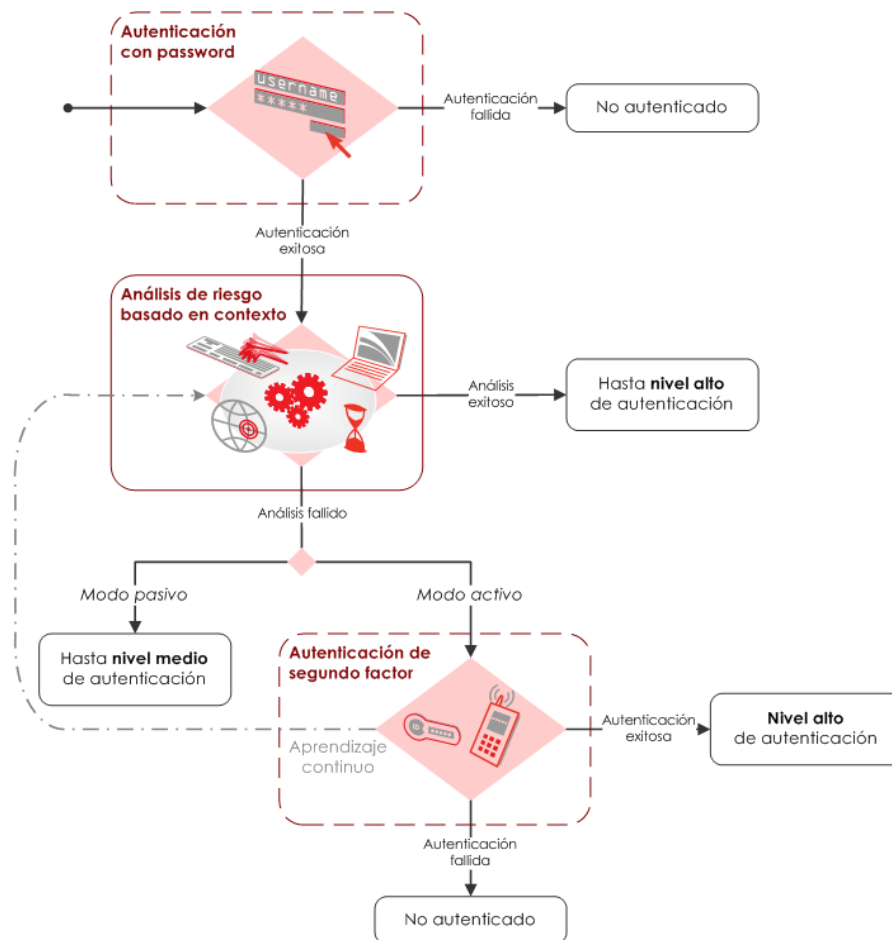


Figure 7: Example of the stages in the TrustedX adaptive authentication process.

Identity Mapping

Identity mapping entails determining which group A identity corresponds to which group B identity, which allows the federation of the different identity attribute sources. For instance, an online shop that has its own historical client database could allow its users to use their identity on a social network, such as Facebook, to improve the user experience and boost client loyalty. To link the historical identity of each client to their social identity, a provisioning procedure of the corporate database needs to be performed for this database to also include an identity attribute returned by the unique social network for each client.

Thus, the identity provider could provide two authentication workflows for the convenience of its clients. In one flow, it could identify the user via the credentials managed by the online shop itself, while in the other flow, it could delegate authentication to the social network and receive a set of unique user attributes (email, social network identifier, etc.), which it would use to determine the identity of the client being authenticated in its database.

Identity mapping assures that a given user is assigned the same identifier regardless of which authentication workflow is executed. In other words, it is assumed that each different user identifier obtained at the end of an authentication flow corresponds to a user with an independent profile.

Operating Options

TrustedX can perform the following roles according to which stage of the authentication process is being executed:

- **Contextual authentication.** The current first line of authentication is maintained. TrustedX performs the context analysis of the authentication and informs the application. Based on the calculated risk level, the application decides what action to take and continues the authentication cycle (e.g.: block access, request an additional factor, etc.).
- **Adaptability management.** The current first line of authentication is conserved, and TrustedX strengthens the security with the adaptive authentication algorithm. In this scenario, TrustedX scales to the LoA requested by the different applications completing the authentication process required by the applications.
- **Adaptive authentication.** TrustedX manages the complete authentication cycle, i.e., the first line of authentication, the risk analysis and the second line of authentication when required. In this scenario, the application delegates the entire authentication process to TrustedX, and TrustedX scales it to the LoA required.

Architecture and Integration

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

TrustedX is available in appliance format for both hardware and virtual environments approved by Safelayer. The system requires an external database system for managing the configuration data and storing data on profiles, log records and auditing.

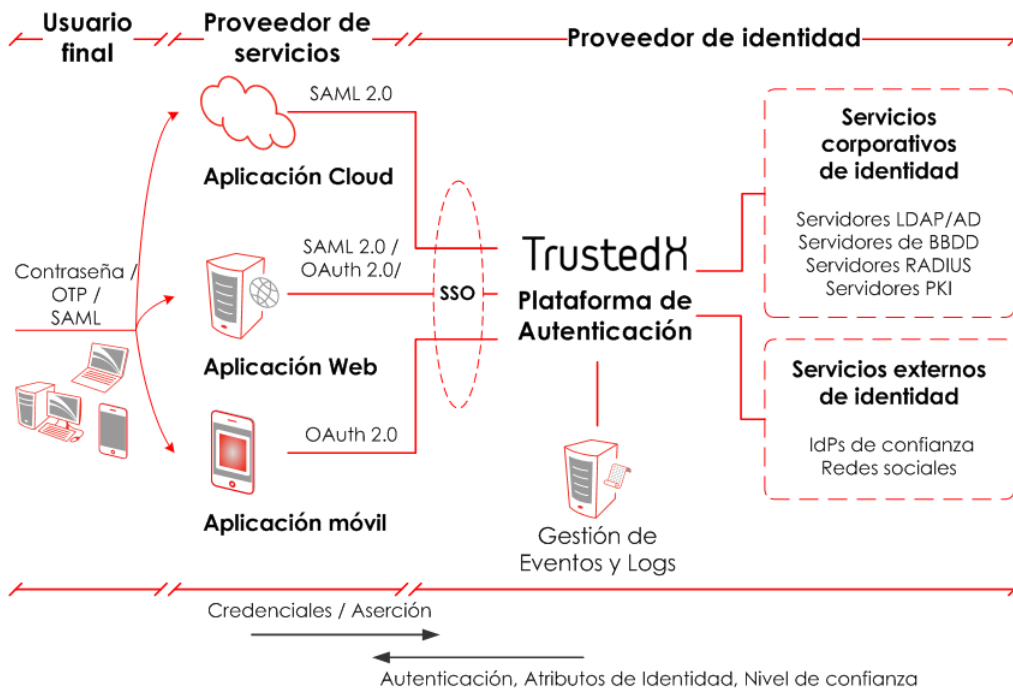


Figure 8: System architecture.

Regarding integration with applications (relying parties, RP) TrustedX's adaptive authentication service is the base on which the system develops its value-added functions such as authentication, obtaining 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. In both cases, the capture of contextual information and/or behavioral biometrics is performed using JavaScript code provided to the user device (browser). Depending on the integration strategy, this is done either directly from the TrustedX server or from the Web application (RP) to which the function was delegated.

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.
- **Delegated authentication** to other, already deployed, identity and authentication providers. In this case, TrustedX delegates the insertion of credentials and, optionally, the capture of the user's context in the external authentication service via specific connectors.

The connectors can be developed and delivered by Safelayer in the product, or they can be developed and incorporated by third parties. A connector can be stored and executed inside or outside of the TrustedX system, depending on the execution selection or requirements of the given deployment. The connectors incorporated by default in the system are 1) user and password against LDAP and 2) user and password against RADIUS.

Other connectors provided by Safelayer permit the use of a) user and password against Windows Domain supporting Kerberos and/or NTLM, b) PKI certificate against recognized certification authorities, c) user and password based on out-of-band SMS or email message, d) user and password against Facebook, etc. These connectors are incorporated in the product via system plug-ins imported and activated by license.

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:

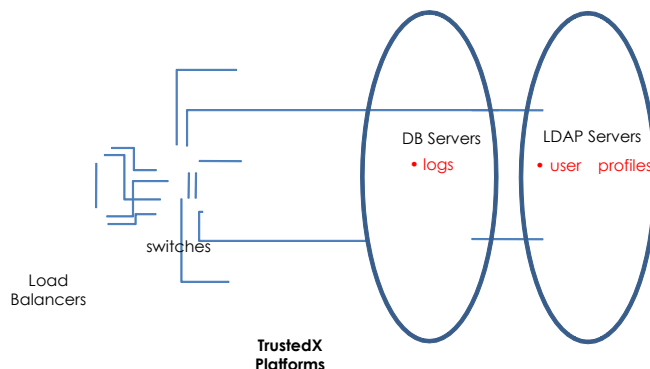


Figure 9. TrustedX high-availability deployment.

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 2.0 and OAuth 2.0/ OpenID Connect

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

- **Management of identity attributes.** The solution supports using different identity database and LDAP/AD-type repositories found in production. The solution assumes the existence of an external user provisioning system that incorporates and updates the users and their identity attributes.

- **Selection of identity attributes by application.** The platform supports defining the set of identity attributes sent to each relying party (RP) in the authentication response. These attributes can be extended to all attributes found in the identity repository.
- **Session and single sign-on (SSO) management.** The Adaptive Authentication solution incorporates SSO functions for all the applications, regardless of the integration protocol they use. This means that the session started by a user in the IdP is uniformly maintained for any application in the IdP's domain, which is ideal for creating a uniform integration environment between on-premise and Cloud-based corporate applications.

The IdPs implemented by TrustedX Adaptive Authentication can enable OAuth 2.0 / OpenID Connect and SAML 2.0 interfaces. On the one hand, TrustedX Adaptive Authentication is primarily considered an OAuth 2.0 provider as it offers version 2.0's Authorization Code Grant flow and a specific User Info endpoint for querying the attributes of the authenticated user. On the other hand, it supports using SAML 2.0's Web Browser SSO profile as an integration element in SaaS applications (Salesforce, Google Apps, etc.), which provision themselves with a reduced subset of identity attributes.

Proveedores de identidad

CN=Identity Provider

Editar

Nombre distintivo * CN=Identity Provider

Descripción Proveedor de identidad

Nombre informal

Nombre de dominio * example-domain.com

Configuración del acceso Atributos de identidad OAuth 2.0 SAML 2.0 Almacén de claves Personalización de la interfaz de usuario

Mecanismos de autenticación * Grupo de mecanismos adaptativos

Política de autenticación adaptativa * Política de autenticación adaptativa de usuarios

Primera línea de autenticación

Estrategia de integración * Interfaz gráfica estándar

Segunda línea de autenticación

Estrategia de integración * Interfaz gráfica estándar

Single sign-on * Basado en el nivel de autenticación

Ver XML Usado por Cancelar Eliminar Guardar

Figure 10: Each IdP can support one or more protocols, allow SSO and define its own authentication workflow.

During the execution of a workflow and in its role as an identity provider, TrustedX compiles identity attributes from both local repositories and IdPs managed by third parties. TrustedX provides a mapping system between the local format of all these identity attributes (e.g., LDAP) and the format of the OpenID Connect or SAML 2.0 service used by the RP and can also redefine or even compile new attributes with this information. For instance, the IdP can compile the "email" attribute by concatenating the username and the IdP's domain as follows: {userId}@{domain}.

The IdP returns the same identity attribute schema to all the RPs, although for each RP it is possible to redefine the user's identifier attribute so that each RP receives customized information even though the IdP carries out user authentication in the same way. For instance, after an IdP has executed the same flow, the user identifier for Google Apps might be an email address while the DNI ID number could be used for a corporate Web application.

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 real complexity of the system.

The RESTful model lets integrators and programmers incorporate TrustedX's adaptive 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.

Mobile Devices

TrustedX's authentication solution is Web based. This means it is unique and uniform in all device environments in which there is a Web browser, e.g., in desktops or any mobile device, including smartphones, tablets, Web TVs, video game consoles, etc.

Furthermore, the solution is valid for pure Web applications and native applications where the operating system that executes the native application provides a browser linking and invocation method (MS-Windows, Linux, iOS, Android, etc.). In the most common mobile operating systems, iOS and Android, as the browser is already embedded in the system, explicitly making system calls for own use is supported.

In mobile environments, applications can be developed using three different technology scenarios.

- **Web:** The user agent (client) is the browser and all the logic and application content are in the server. In this scenario, the Adaptive Authentication solution is already supported as it is a Web solution.
- **Hybrid:** The user agent (client) is an application that has part of the logic and content. This application is developed using Web techniques based on a framework that includes a browser embedded in the application.
- **Native:** The user agent (client) is an application that has part of the logic and content. This application is developed using the native language supported by the operating system (e.g., Objective C in iOS or Java in Android). In this case, the link to the authentication solution can also be carried out via the browser that the system allows to invoke natively or via the use of an SDK.

In short, using Web technology by means of an authorization/authentication REST API based on OAuth means we can provide a solution that is uniform for all device environments.

Monitoring and Auditing

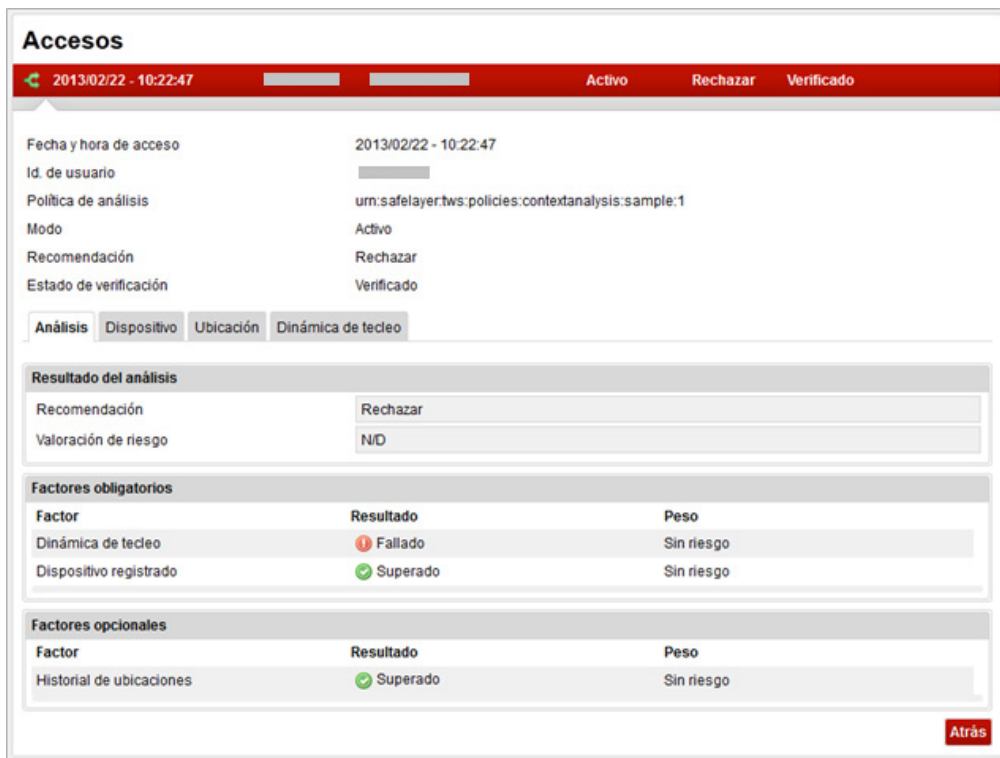
One very important aspect of security in general and of authentication in particular is the logging (generation and storage), search, recovery and analysis of events and presentation of conclusions (reporting) for i) security auditing, ii) reports on regulatory compliance, iii) monitoring and security 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, Business Intelligence 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.

Authentication Risk Analysis

As stated in the previous sections, the solution captures the user's authentication context and analyzes it to calculate the risk level associated to the user's authentication process, which is basically the level of risk of identity theft.



Accesos

2013/02/22 - 10:22:47 Activo Rechazar Verificado

Fecha y hora de acceso: 2013/02/22 - 10:22:47
 Id. de usuario: [redacted]
 Política de análisis: urn:safelayer.tws:policias:contextanalysis:sample:1
 Modo: Activo
 Recomendación: Rechazar
 Estado de verificación: Verificado

Análisis Dispositivo Ubicación Dinámica de tecleo

Resultado del análisis

Recomendación: Rechazar
 Valoración de riesgo: N/D

Factores obligatorios

Factor	Resultado	Peso
Dinámica de tecleo	❌ Fallado	Sin riesgo
Dispositivo registrado	✅ Superado	Sin riesgo

Factores opcionales

Factor	Resultado	Peso
Historial de ubicaciones	✅ Superado	Sin riesgo

Atrás

Figure 2-11. Detailed data on each access in real-time: an analysis summary.

The user context information includes data on the quality of the credential, identification, device characteristics and environment, user biometric identification and behavior, time-range and location data. For each authentication process, the system logs user context information and the results of the analysis and the authentication.

This means that a history of the authentication context of each user and the results of applying the intelligence algorithms for the analysis of this data is available. This information accumulates and is used in the analyses of the new authentication processes. Furthermore, the individual accesses of each authentication process can be browsed and displayed by applying search filters.

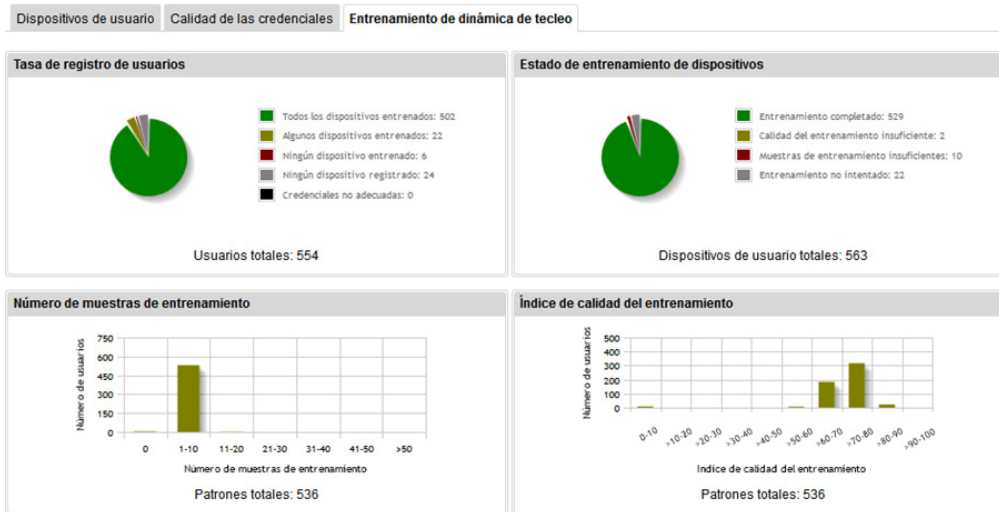


Figure 2-12. User profile reports.

The more the system is used, the more information, i.e., intelligence, there is that can be applied in the adaptive authentication process. The system uses certain context information (e.g., the correlations between device, location and time-range) to learn and adapt on its own. A user who normally authenticates with a certain device is not the same as a user who usually connects with a certain device from a certain location and/or in a certain time-range. In the first case, the potential theft of the device cannot be detected. In the second case, however, it can be detected if the location and/or time-range differ from those in the history of the user contexts.

The intelligence can also be applied for manually tuning the system and better adapting it to the user community it serves. For example, you can apply an adaptive authentication policy that has the typing speed biometric enabled to a community of users. You can obtain intelligence reports on users that have trained their biometric patterns, the quality of the training, the false rejection and acceptance rates for the authentications performed, the quality of the character set used in the password, etc. All this information lets administrators adjust system parameters, generate user alerts, and improve training programs so that the overall efficiency of the system can be improved (greater levels of security and maximized usability).

The risk analysis system of the user authentication context has thresholds that can be manually adjusted in non-deterministic context parameters. The intelligence support to the user context and the associated risk is included in the solution and does not require any external intelligence tool.

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.

At the global organizational (or service provider) level, TrustedX also provides data that can be used in the accounting of the use of the IT assets provided. Furthermore, the access control rules can be used to limit the consumption of these assets according to the user context.

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

The Adaptive Authentication solution generates multiple sources of information. Its monitoring can be used to generate alerts that can require 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 (Nagios, OpenNMS, IBM Tivoli or HP Network Management Center) can be used to map the network of servers dedicated to the Adaptive 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) the "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 with 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.

© Copyright 1999-2014 Safelayer Secure Communications, S.A. All rights reserved.

TrustedX Autenticación Adaptativa

This document and the software described in it are supplied under license and may be used or copied only in accordance with the terms of the license. This document is for informational use only. Safelayer Secure Communications S.A. assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. The content of this document is subject to change without notice.

The copyrighted software that accompanies this document is licensed to the end user for use only in strict accordance with the End User License Agreement, which the licensee should read carefully before using the software. Except where permitted by the license, no part of this document may be copied, reproduced or stored in any form or by any means, electronic or mechanical, by recording or in any other way, without the express permission of Safelayer Secure Communications, S.A.

TrustedX and KeyOne are Safelayer trademarks. All other names may be trademarks or registered trademarks of their respective owners.

Safelayer Secure Communications, S.A.

Telephone: +34 93 508 80 90

Fax: +34 93 508 80 91

Web: www.safelayer.com

