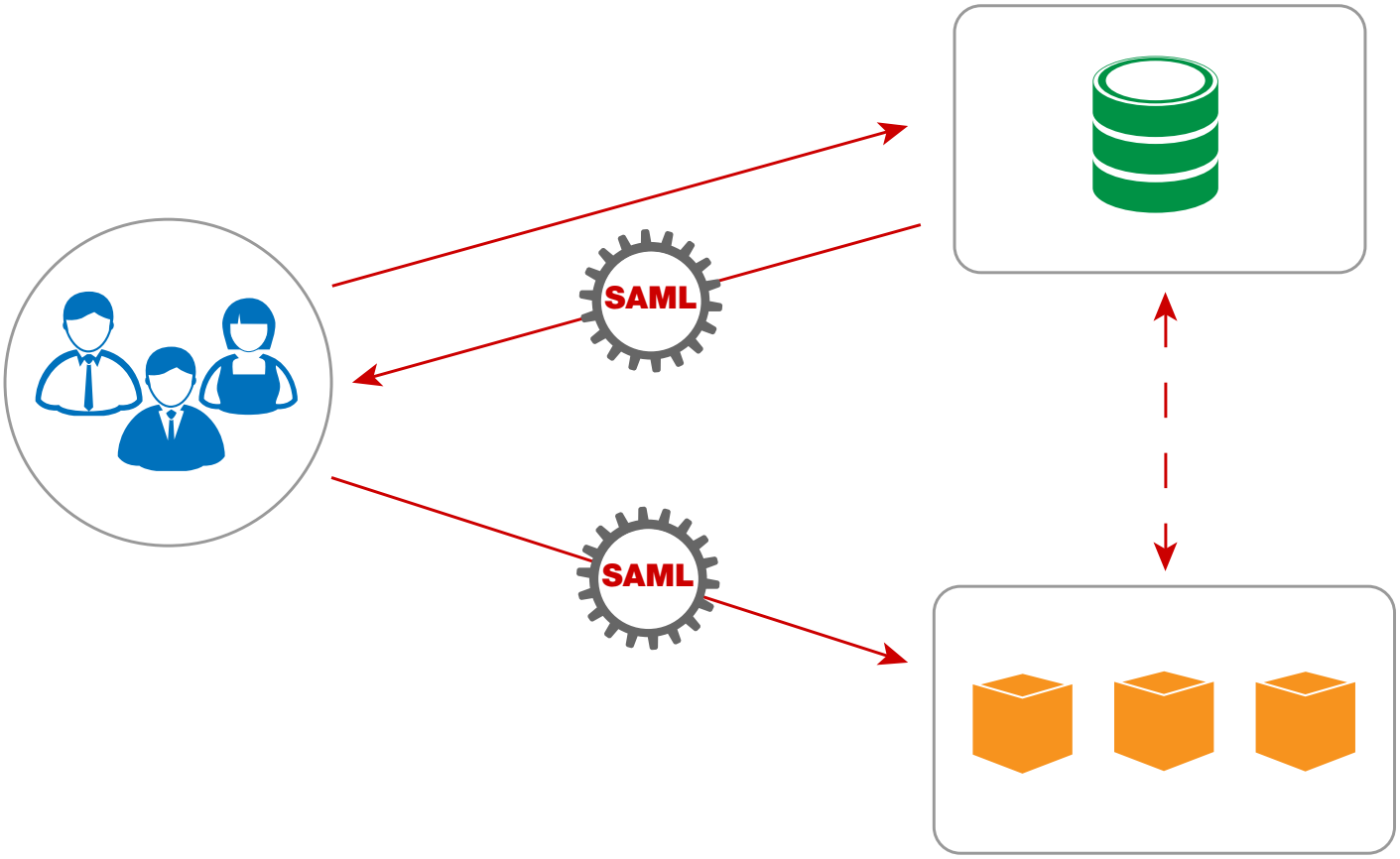
WHITE PAPER

Introduction to SAML



FORUM SYSTEMS
THE LEADER IN API AND CLOUD GATEWAY TECHNOLOGY

Introduction to SAML

SUMMARY:

In this white paper, you will learn:

- What is SAML and how it works.
- The Benefits of SAML.
- How SAML is used by enterprise organizations for SSO.
- Some of the challenges associated with implementing SAML.

Introduction

In today's world of rapidly expanding and growing software development; organizations, enterprises and governments are able to conduct business faster and a more efficiently with the aid of web-based applications. Many of these applications are mission critical for organizations. And because of this, the need for integration and interoperability has become that much more important. The internet and migration to cloud architectures has made access to applications much easier too.

With greater accessibility, the risk of breach becomes higher as well. So, how do you keep access to these applications secure? You could implement a username and password for each one. Although this seems like the most logical route, it ends up being the least secure. By forcing each application to store and sync identities, you're creating new potential vulnerabilities. With this approach, you are relying on the application to store the identities in a safe and secure location. If one application is compromised then all of the applications are compromised.

These challenges lead to the need for federated identity management. Federated identity management (FIdM), in terms of information technology, is the use of standards-based policies and protocols to manage and enforce individuals' access to applications across multiple domains. FIdM enables business partners to allow secure access to internal resources without having to assume the burden and risk of storing user identities that belong to their business partners. As a result of federated identity management, single sign-on was born. Single sign-on, or SSO is the ability for individuals to sign into multiple applications with one set of credentials. Although, there are multiple standards of federated identity management, including: OAuth, SAML, OpenID, and proprietary solutions. Security Assertion Markup Language, or SAML has emerged as one of the most versatile and frequently used.

This white paper will explain what SAML is, the benefits of SAML, and how it works. We will also explain how SAML is used for single sign-on (SSO), as well as some of the limitations of SAML.

What is SAML?

Created by the OASIS Security Services Technical Committee (SSTC), SAML is an XML-based framework used to authorize, authenticate and communicate attributes and privileges of a user. SAML provides the ability to send information about an authenticated user and does not require a third-party system to ever have access to the user's credentials.

SAML has gone through a few iterations and is today considered a proven and mature standardized framework. The first version of SAML, V1.0 was released in November of 2002 and the latest version, V2.0 was released in March of 2005. Since then, the latest approved modifications (errata) were released in May 2012.

The Benefits of SAML

SAML has been widely adopted by enterprise organizations for three primary reasons: SAML is standardized, secure, and provides an excellent user experience.

The SAML standardized format is designed to interoperate with any system independent of implementation. This enables a more open approach to architecture and identity federation without the interoperability issues associated with vendor-specific approaches.

In the modern era of computing, security is of the utmost importance when it comes to enterprise applications. SAML is used to provide a single point of authentication at a secure identity provider, meaning that user credentials never leave the firewall boundary, and then SAML is used to assert the identity to others. This means that applications do not need to store or synchronize identities, which in turn ensures that there are fewer places for identities to be breached or stolen. SAML provides a strong layer of security by leveraging Public Key Infrastructure (PKI) to protect the asserted identities against attempted attacks.

Arguably, one of SAML's greatest benefits is the user experience it provides. SAML is used to securely communicate (assert) attributes and privileges of a user to a Service Provider. SAML does this through assertions, one of its greatest assets. Assertions enable an Identity Provider to share detailed information about the user, what application rights they have, access to multiple applications, how long they may access the application and much more. In the next section, we will explain in more detail what assertions are and how they work.

How does it work?

To properly understand how SAML works, there are three participants that need to be established: the User, the Identity Provider (IdP) and the Service Provider (SP). The User is the client attempting to access an application. The Service Provider is the owner or provider of the application and may also be referred to as the SAML relying party. The Identity Provider is the holder of record of the user's actual authentication credentials (i.e., username, password, x509, roles, etc.) and is sometimes be referred to as the SAML asserting party. As the name SAML (Security Assertion Markup Language) suggests, it is a secure means to assert the identity of a user to another system.

Within SAML's framework, there are four concepts: Assertions, Protocols, Bindings, and Profiles. To show the relationship between these concepts, please see figure 1.

Assertions

A SAML assertion is a packet of information that contains required user attributes and one or more statements about the User. SAML assertions are generated from the Identity Provider and are consumed by the Service Provider. These statements, along with the contextual information allow the Service Provider to make access control decisions about the User that was previously authenticated.

Before assertion statements are consumed, the Service Provider inspects the digital signature (DSIG) to verify the SAML token's integrity and authenticity. Once the SAML token has been verified, the Service Provider then analyzes its contents and makes access control decisions accordingly.

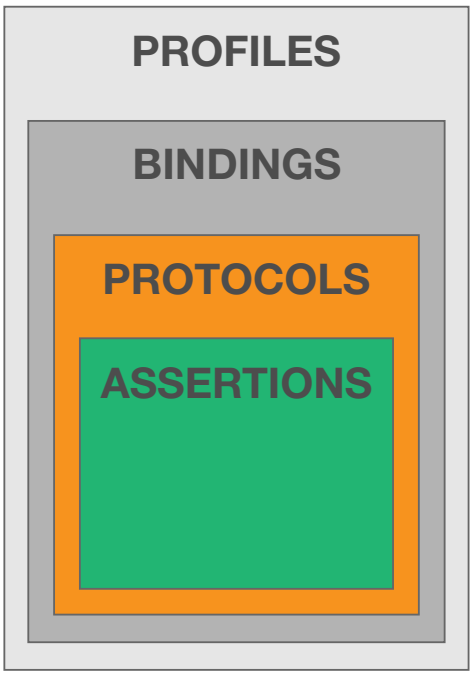


Figure 1: SAML Concepts

There are three types of assertion statements:

1. **Authentication statements** – tell the Service Provider that the subject (User) has been authenticated with the Identity Provider using a particular method at a specific time. This may also include additional information about the user in the authentication context.

2. **Attribute statements** – inform the Service Provider that the user has specific identifying attributes.

3. **Authorization decision statements** – tell the service provider what resource a User is entitled to access based on certain evidence.

To make assertion statements easier to understand, we will use the example of someone buying alcohol at a liquor store. In this example, the User is the individual attempting to buy alcohol, the liquor store is the Service Provider, the state that issued the license is the Identity Provider and the state license is the SAML token. As we mentioned before, the Service Provider must inspect the SAML token's DSIG before the contents may be consumed. This is equivalent to the liquor store clerk verifying that the license being presented is a legitimate state license that has not been tampered with. Normally, this is achieved by examining the state seal or watermark on the license.

Once the license has been verified, the liquor store (SP) then consumes the information on the license (assertion statements). The liquor store uses this information to determine whether the User should be granted or denied access to purchase alcohol.

For example, the authentication statement would state that the subject (User) has been authenticated with the issuing state via license registration (method) at the date the license was issued (time). The attribute statement would include the birthdate, picture, height, sex and other identifying attributes. And, the authorization decision statement would state that the User is able to buy (action) alcohol (resource) based on their age and photo (evidence) on their license.

Protocols

In most cases, assertions are created by the Identity Provider in response to a request made by the Service Provider. These response/requests are known as SAML protocols. There are six defined SAML protocols and they enable Service Providers to take a variety of actions. Think of SAML protocols as the rules by which the User is asserted. For example, the Name Identifier Mapping Protocol enables the SP to request an identifier from the IdP for a User that the SP may use at another SP in an application integration scenario.

Bindings

SAML bindings determine how the SAML protocol messages are transported. Typically, SAML protocols messages are carried over SOAP or HTTP.

Profiles

SAML profiles define how assertions, protocols and bindings are combined to satisfy a particular use case. Think of SAML profiles as templates, each profile uses different combination of bindings, protocols and assertions. One of the most used SAML profiles is the Web Browser SSO Profile.

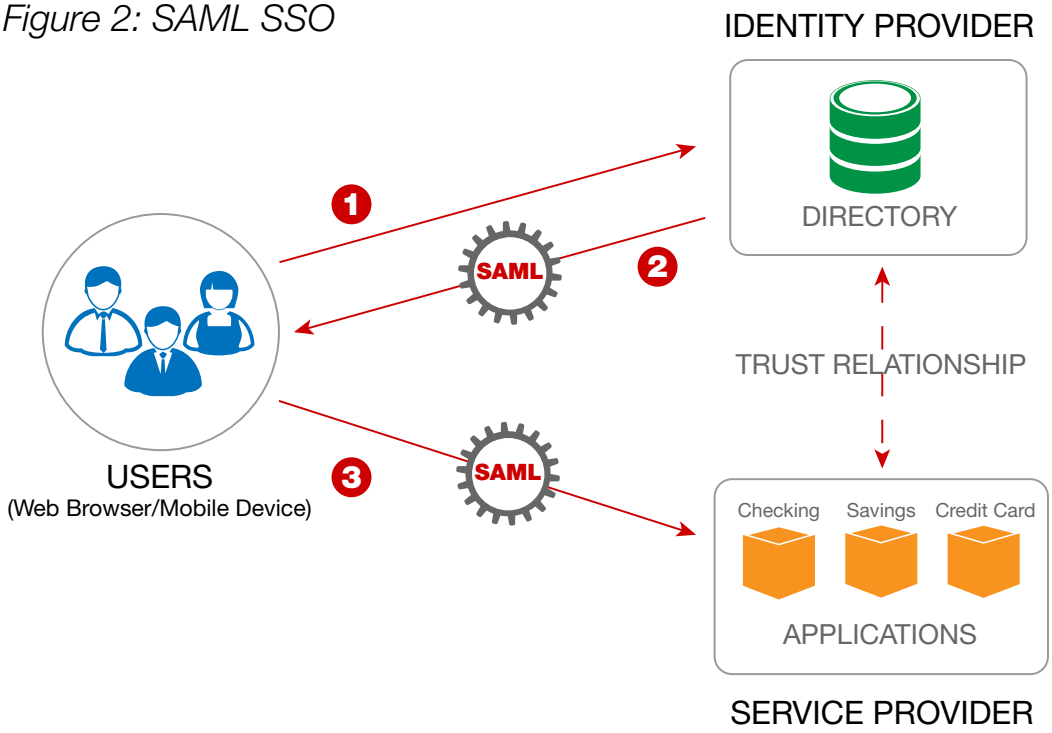
How SAML is used for SSO

SAML provides the ability for users to access multiple applications with a single set of credentials entered once. This is the foundation of federation and also of single sign-on (SSO). Using SAML, users can seamlessly access multiple applications, allowing them to conduct business faster and more efficiently.

You may not have realized this, but you use SAML SSO every day. Whether it's logging into your bank online, using a mobile application, or pretty much anywhere you are signing into a website and accessing the information therein. For the purposes of explaining how SSO works, let's use online banking as our use case. When a bank customer logs in to their bank account via the bank's website they may need to access a variety of applications from their checking and savings accounts to their credit card balance. Each of their accounts types (savings, checking, credit, brokerage, business) are often provided by different back-end applications. These applications need to be able to communicate with each other using a common authentication scheme to provide a seamless user experience that enables one login to provide access to all the parts of the online banking web portal. SAML provides the means to accomplish this.

Let's look closer at the sequence of steps to generate a SAML token, and then use it to gain access to an application or resource. Figure 2 shows the basic steps necessary for SSO using SAML.

Figure 2: SAML SSO



1. **User authenticates to identity provider using a single-factor, or multi-factor authentication.**
2. **The Identity Provider issues a SAML token to the User with assertions about the User's identity. In Mobile devices, and web browsers, the SAML is often issued as embedded BASE64 within the HTML response.**
3. **The User's browser is redirected from the Identity Provider to the location of the Service Provider. The User's browser then issues a request to the Service Provider with the SAML token embedded. The Service Provider then inspects the SAML token and its contents to determine validity based on the trust relationship with the Identity Provider. The Service Provider then provides access to the various online banking applications based on the SAML assertion statements included in the token.**

SAML SSO provides a seamless experience for the user to access multiple applications without the user or client technology requiring any changes to support the SAML exchange.

Limitations of SAML

Although SAML is the most popular method of SSO, there are some challenges imposed for the implementation of a SAML solution based on legacy end-mile implementations:

- ***SAML Aware Endpoints*** – the consumption of the SAML assertion requires decoding the SAML, parsing out the relevant aspects, then making role-based access control decisions. This can be difficult if you are putting these tasks in the hands of back-end application developers.

- ***PKI and CPU*** – The trust relationship inherent in SAML assertions includes a digital signature to verify the integrity and establish trust that it was indeed a trusted party that issued the SAML. This brings up issues of scale for cryptography as well as PKI key management

The legacy approaches to SAML involve building SAML awareness into the end-mile applications and services which in turn pass the SAML assertion over to a central identity system to process it. This can be time consuming and costly for an organization.

Fortunately, there is a modern approach to SAML SSO that eliminates all of these limitations and provides no-code simplified policy-based enablement of SAML SSO. This approach is through the use of an API Gateway which provides out-of-the box support for SAML SSO with seamless integration with identity stores and client and server technologies. Our next white paper will show how simple it is to implement SAML SSO using an API Gateway.

About Forum Systems

Forum Systems is the global leader in API and Cloud Security technology with industry-certified and patented products that secure enterprise infrastructure. Forum Systems has been an industry leader for over 13 years and has built the core architecture of its technology on the foundation of FIPS 140-2 and NDPP. Our security-first mindset enables trusted, network edge deployments for protecting critical enterprise transactions.

Forum Systems supports enterprise customers across commercial, government, and military sectors. Forum Systems technology provides leading-edge security with identity and SSO features that enable out-of-the box business solutions with code-free configuration.

References:

Security Assertion Markup Language (SAML) 2.0 Technical Overview
https://www.oasis-open.org/committees/download.php/11511/sstc-saml-tech-overview-2.0-draft-03.pdf

SAML Executive Overview
https://www.oasis-open.org/committees/download.php/11785/sstc-saml-exec-overview-2.0-draft-06.pdf

Advantages of SAML
http://saml.xml.org/advantages-saml