ACTIVANTS PTE LTD **02/09/2019**

Indrajit Maurya

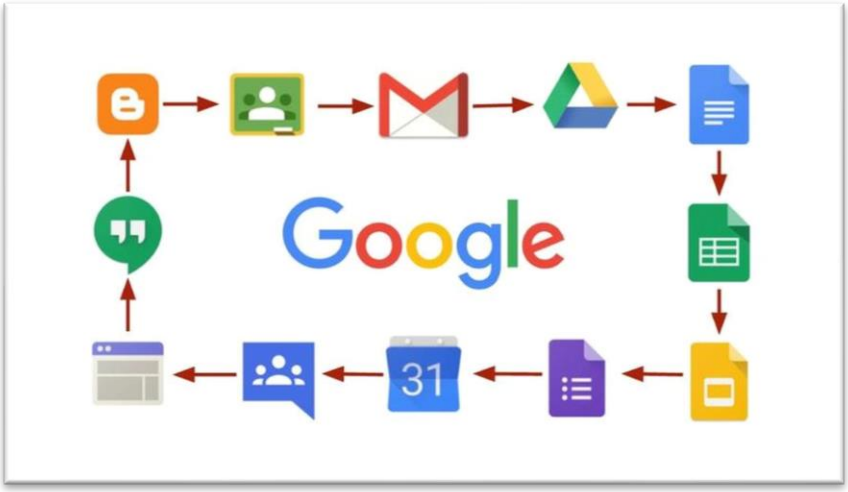
Topic: SAML (Security Assertion Mark-up Language). Modules included are

- Acting as the SAML service provider (SP)
- Acting as the SAML identity provider (IdP)
- Service provider initiated SSO
- Identity provider initiated SSO
- Setting and retrieving SAML attributes
- Logout
- SAML metadata creation and consumption
- OWIN ASP.NET Identity integration

Single Sign-On (SSO)

Single sign-on (SSO) is a service that allows a user to use one set of login credentials to access multiple applications. Considering the image below, suppose we have developed and deployed two websites at domain X and domain Y respectively. Now if users can access both the applications with same credentials and users who are already logged-in at domain X to be automatically logged-in at domain Y, this can easily be achieved by the concept of SSO.

A typical and good example of Single Sign On is Google. Google's implementation of login for their products such as Gmail, YouTube, Hangouts, Google Analytics and so on is an example of this system. Any user that is logged in one of the Google products is automatically logged in other products as well. This is the power of Single Sing On.



Protocols to create Single Sign On

- **Basic Auth:** A simple username and password schema on an app, by app basis
- **OAuth**: API security model that relies on an outside Identity Provider and key-store to grant and deny access to APIs
- **SAML**: A Web based model that allows a third-party application or services to validate the user's and retrieve details about that user.

Types of SSO configuration

Some SSO services use protocols such as **Kerberos** and the **security assertion mark-up language (SAML)**.

Security Risk and SSO

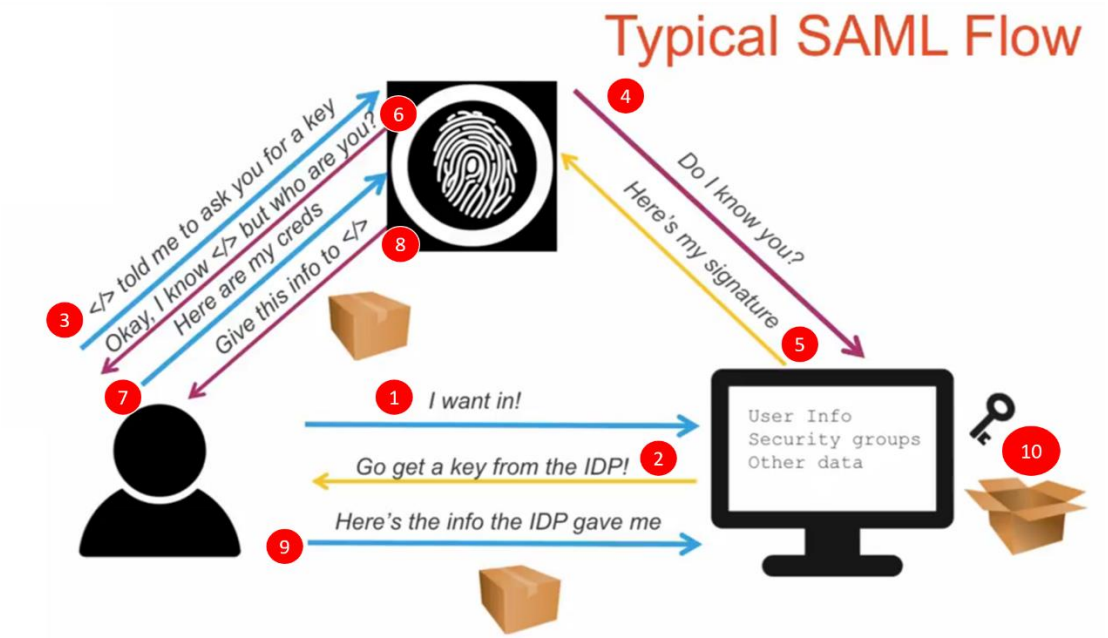
Using two-factor authentication (2FA) or multifactor authentication (MFA) with SSO will help to improve security.

SAML (Security Assertion Mark-up Language)

Description: SAML is an XML standard that facilitates the exchange of user authentication and authorization data across secure domains. SAML-based SSO services involve communications between the user, an identity provider that maintains a user directory, and a service provider.

- Security Assertion Mark-up Language (SAML) allows identity providers (IdP) to pass authorization credentials to service providers (SP).
- SAML transactions use Extensible Mark-up Language (XML) for standardized communications between the identity provider and service providers.
- It is the link between the authentication of a user's identity and the authorization to use a service.
- It maintains a secure federated identity management system.
- It enables Single-Sign On (SSO).

Typical SAML Flow

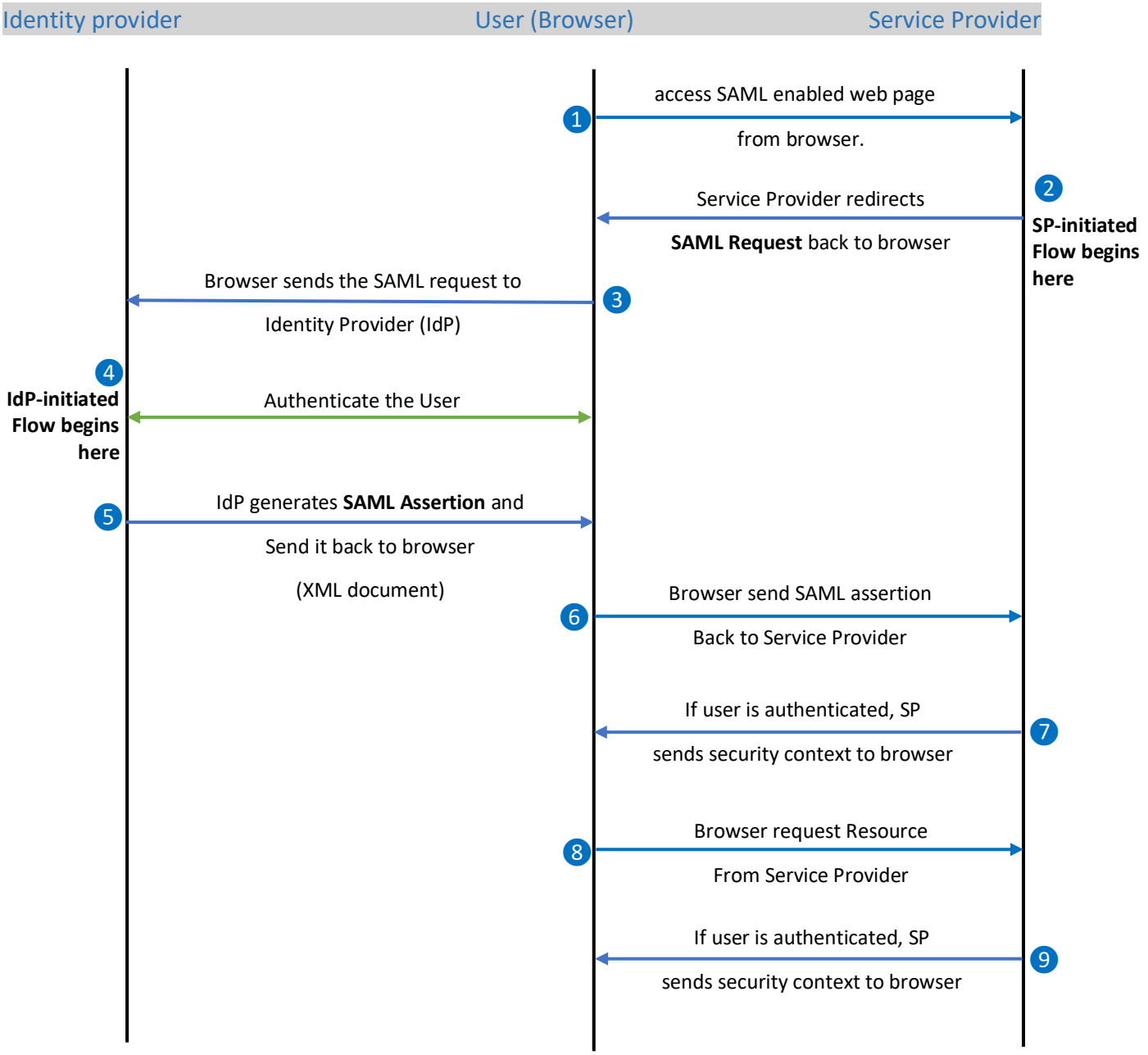


- User try to log in to web page.
- The browsers redirect the user to Identity Provider.
- The Identity Provider receives the request and verifies/checks the Web Application with the encrypted certificate either by reaching out live to the web application or in its local cache.
- The Identity provider verifies the User if not logged in and provides an encrypted package
- The Web Application with its signature key decrypts the package which contains all the information of the user.

How does SAML work?

SAML works by passing information about users, logins, and attributes between the identity provider and service providers. Each user logs in once to Single Sign On with the identity provider, and then the identity provider can pass SAML attributes to the service provider when the user attempts to access those services. The service provider requests the authorization and authentication from the identity provider. Since both of those systems speak the same language – SAML – the user only needs to log in once.

Each identity provider and service provider need to agree upon the configuration for SAML. Both ends need to have the exact configuration for the SAML authentication to work.



Service Provider (SP): A service provider is the entity providing the service – typically in the form of an application

Role of Service Provider: Upon receiving the SAML response (**SAML assertion**) from the SAML IDP, the SP validates if the response comes from a valid IDP and then parse the necessary information from the assertion.

In order to do this, the SP requires the following:

- Certificate – The SP needs to obtain the public certificate from the IDP to validate the signature. The certificate is stored on the SP side and used whenever a SAML response arrives.
- SP login URL/ ACS Endpoint – Assertion Consumer Service URL: This is the endpoint on the SP. The SP needs to provide this information to the IDP.
- IDP Login URL – This is the endpoint on the IDP. The SP needs to obtain this information from the IDP.

An **Identity Provider (IDP)** is the entity providing the identities, including the ability to authenticate a user. The Identity Provider typically also contains the user profile.

A **SAML Request**, also known as an authentication request, is generated by the Service Provider to " request" an authentication.

A **SAML Response** is generated by the Identity Provider. It contains the actual SAML Assertion of the authenticated user. In addition, a SAML Response may contain additional information, such as user profile information and group/role information, depending on what the Service Provider can support.

A **SAML Assertion** is the XML document that the identity provider sends to the service provider that contains the user authorization.

There are three different types of SAML Assertions:

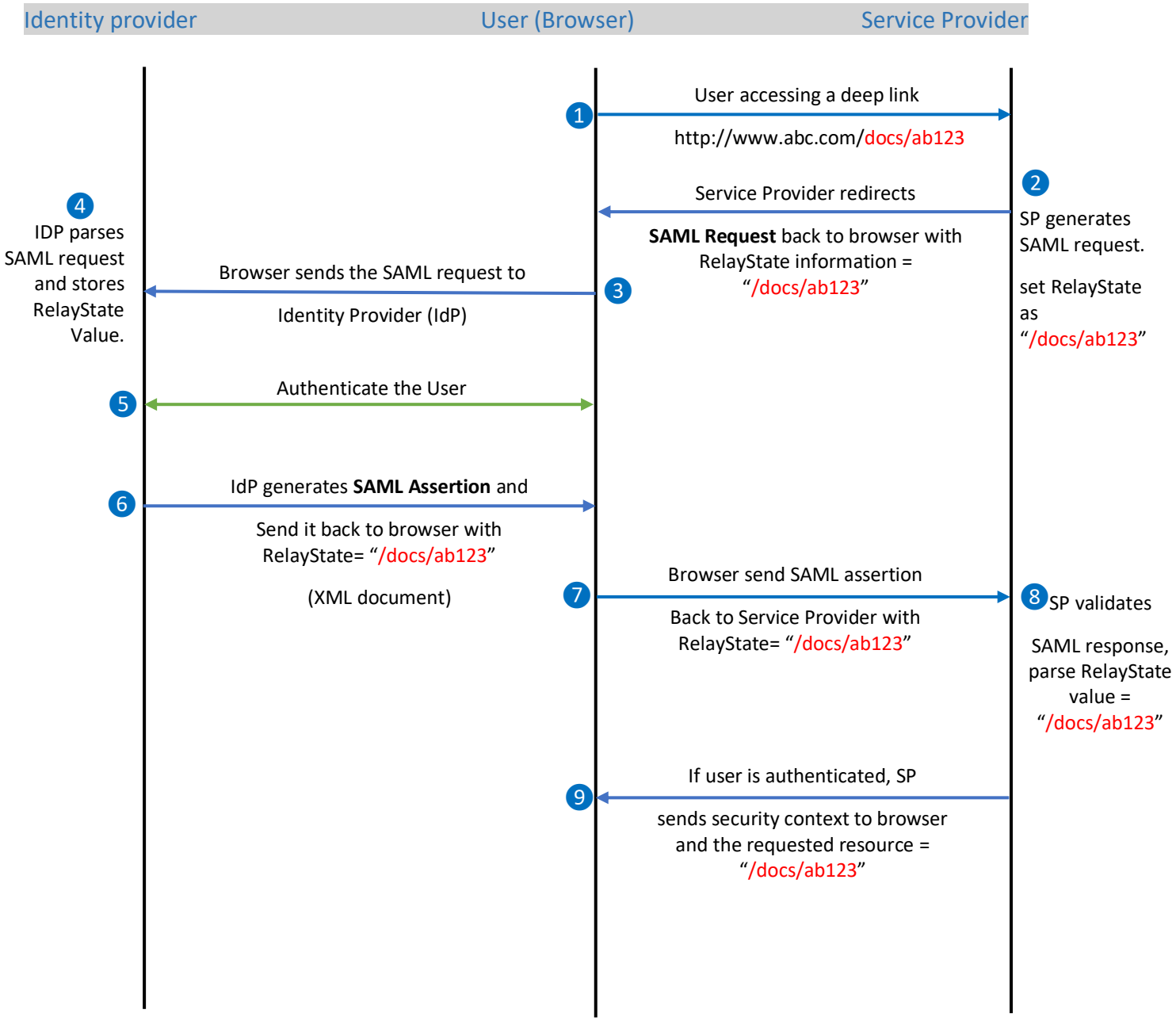
- **Authentication**: Authentication assertions prove identification of the user and provide the time the user logged in and what method of authentication they used (I.e., Kerberos, 2-factor, etc.)
- **Attribute**: The attribution assertion passes the SAML attributes to the service provider – SAML attributes are specific pieces of data that provide information about the user.
- **Authorization decision**: An authorization decision assertion says if the user is authorized to use the service or if the identify provider denied their request due to a password failure or lack of rights to the service.

A **Service Provider Initiated (SP-initiated):** when the user tries to access a protected resource or login directly on the Service Provider side, the SP-initiated flow is initiated by the Service Provider.

Understanding the SP-initiated flow

- Users tries to access a protected resource directly on the SP side.
- The SP initially does not know about the IDP.
- A developer must decide on how to make SP determine the right IDP for sending SAML request or to authenticate the user. This can be carried out by two ways
    1. Application contains a subdomain information that is mapped to the IDP. So, on accessing any resource by the user, the SP easily identifies the IDP.
    2. By gathering additional information from the user such as company id, email id etc to make SP determine and trigger to the right IDP. Here the additional information can be identifiers and not credentials.
- SAML is an asynchronous protocol by design. Meaning, after the SAML response from the IDP the SP does not know about the initial deep link that triggered the SAML request to the IDP. This is resolved using an HTTP parameter called RelayState that can be included as part of SAML request and SAML response.

Working of RelayState



An Identity Provider Initiated (IDP-initiated): This is initiated by the identity provider. In this flow the Identity Provider authenticate the user and initiates a SAML Response that is redirected to the Service Provider to assert the user's identity. Since it begins on the IDP side, there is no additional information on what resources the user is trying to access on the SP side.

Exposing SAML configuration in SP

- Using a metadata file as SAML supports metadata on both SP and IDP sides.
- IDP redirect URL (for SAML request)
- IssuerID
- IDP Logout URL

A couple of key things to note:

- The Service Provider never directly interacts with the Identity Provider. A browser acts as the agent to carry out all the redirections.
- The Service Provider needs to know which Identity Provider to redirect to before it has any idea who the user is.
- The Service Provider does not know who the user is until the SAML assertion comes back from the Identity Provider.
- This flow does not have to start from the Service Provider. An Identity Provider can initiate an authentication flow.
- The SAML authentication flow is asynchronous. The Service Provider does not know if the Identity Provider will ever complete the entire flow. Because of this, the Service Provider does not maintain any state of any authentication requests generated.
- Implementing a backdoor for secret login URL for administrators that does not trigger a SAML redirection when accessed. To be used in case of some problems in SAML configuration.