CONCEPTUAL INFORMATION

What is SAML?

INTRODUCTION

Companies that use single sign-on (SSO) authentication have a better user experience, higher productivity, higher system security, and lower system administration costs. Security Assertion Markup Language (SAML) is a preferred SSO authentication protocol. When SAML passes authentication tokens for the identity provider (IdP) and their applications or cloud service provider (SP), the user credentials never leave the firewall boundary, minimizing potential breach points.

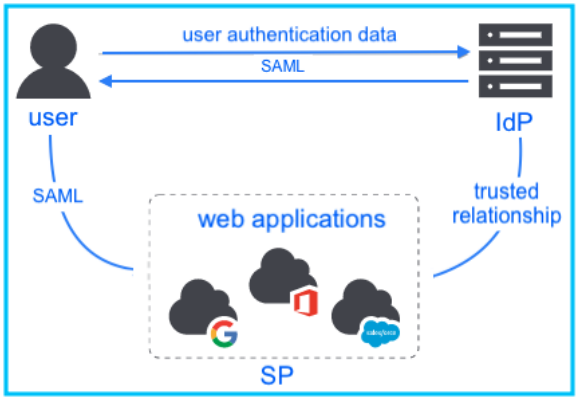
WHAT IS SAML

SAML is an XML-based, platform-independent, open-standard for transferring identity data between two parties. It provides a single point of authentication at a secure IdP. SAML removes the need to maintain multiple credentials at multiple locations.

HOW SAML WORKS

SAML works by exchanging user information, such as logins, identifiers, and other relevant attributes, between the IdP and SP. When a user tries to access an app, the IdP passes the SAML authentication to the SP, who then grants the user entry.

The diagram shows how web applications use SAML to transfer user authentication data between the IdP and the SP.



SAML BENEFITS

It's a given that fewer logins make for a better user experience. The obvious benefit to employees is that they can get to work more quickly with less frustration. The initial *unseen* benefit is increased security. When companies change from the multiple login paradigm to SSO, the following security and administration benefits also lower account management costs by:

- minimizing identity theft points
- removing fishing opportunities
- removing multiple login management

The platform-independent feature of the SAML protocol lowers costs associated with using third-party platforms.

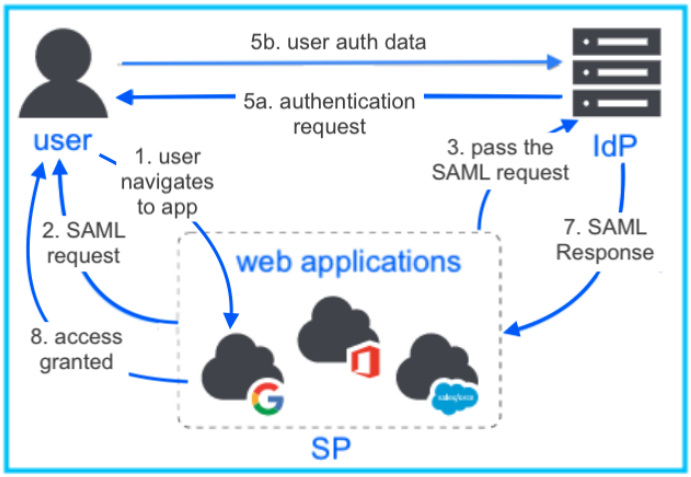
SAML Response (IdP -> SP)

The table in this section contains several SAML Responses. A SAML Response is sent by the IdP to the SP then, if the authentication process succeeds, the response contains the Assertion with the user's NameID/attributes.

SAML Responses
An unsigned SAML Response with an unsigned Assertion
An unsigned SAML Response with a signed Assertion
A signed SAML Response with an unsigned Assertion
A signed SAML Response with a signed Assertion
An unsigned SAML Response with an encrypted Assertion
An unsigned SAML Response with an encrypted signed Assertion
A signed SAML Response with an encrypted Assertion
A signed SAML Response with an encrypted signed Assertion

SAML WORKFLOW EXAMPLE

1. A user navigates to an SP's web application with an IdP.
2. The web application responds with a SAML request.
3. The browser passes the SAML request to the IdP.
4. The IdP parses the SAML request.
5. The IdP authenticates the user by prompting for a username and password or some other authentication factor. *NOTE: The IdP skips this step if the user is already authenticated.*
6. The IdP generates the SAML Response and returns it to the user's browser.
7. The browser sends the generated SAML Response to the SP's web application for verification.
8. If the verification succeeds, the web application grants the user access.



SAML RESPONSE EXAMPLE SNIPPET

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="_8e8dc5f69a98cc4c1ff3427e5ce34606fd672f91e6" Version="2.0"
IssueInstant="2014-07-17T01:01:48Z"
   Destination="http://sp.example.com/demo1/index.php?acs"
   InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685">
   <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
   <samlp:Status>
       <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
   </samlp:Status>
   <saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
       ID="_d71a3a8e9fcc45c9e9d248ef7049393fc8f04e5f75" Version="2.0"
IssueInstant="2014-07-17T01:01:48Z">
       <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
       <saml:Subject>
           <saml:NameID
SPNameQualifier="http://sp.example.com/demo1/metadata.php"

Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">_ce3d2948b4cf2014
6dee0a0b3dd6f69b6cf86f62d7
           </saml:NameID>
           <saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
               <saml:SubjectConfirmationData
NotOnOrAfter="2024-01-18T06:21:48Z"
                   Recipient="http://sp.example.com/demo1/index.php?acs"

InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685" />
           </saml:SubjectConfirmation>
       </saml:Subject>
```

SUMMARY

SAML SSO reduces serious threats, saves administrative time, and replaces a cumbersome app user experience with a positive one.

REFERENCES

How SAML Authentication Works, Holly Guevara, conference DevDay 2022, auth0.com/blog, 2022

Intro to SAML: What, How and Why, Mike Donaldson of Ping Whiteboards, 2010

SAML Explained in Plain English, /www.onelogin.com, 2022

SAML Response (IdP -> SP), /www.samltool.com

What is SAML?, Amalanathan Thushanthan, publisher Identity Beyond Borders, medium.com/identity-beyond-borders, 2019

What is Security Assertion Markup Language (SAML)?, www.oracle.com, 2021

What SAML Is and How Does It Works, IntelligentHQ, , 2019, 2022