Overview of SAML

What is SAML

SAML (Security Assertion Markup Language) is an XML-based protocol standard for sharing/exchanging security information about identity, authentication and authorization across different systems. allowing for a web-based, cross-domain Single-Sign-On (SSO) experience.

SAML helps reduce the administrative overhead of distributing multiple authentication tokens to the user which makes Single-Sign-On (SSO) technology possible by providing a way to authenticate a user once and then communicate that authentication to multiple applications.

Glossary of common terms

- A **Service Provider (SP)** is any entity that provides services, typically the services for which users seek authenticated, including in the form of an Website / Application . In this case our ConcreteCMS website. The Service Provider uses the assertions that it receives from an Identity Provider to authenticate users and then provide access to the requested federation resources.
- An **Identity Provider (IdP)** is the entity providing /administers

the identities informations, it stores and confirms identity, including the ability to authenticate a user, typically through a login process. such as **Okta** or **OneLogin** ...

- 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 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.

How does SAML work

The SAML workflow below reflects the process when the user navigates to our ConcreteCMS website first, is redirected to the Identity Provider for login, and redirected back to us .

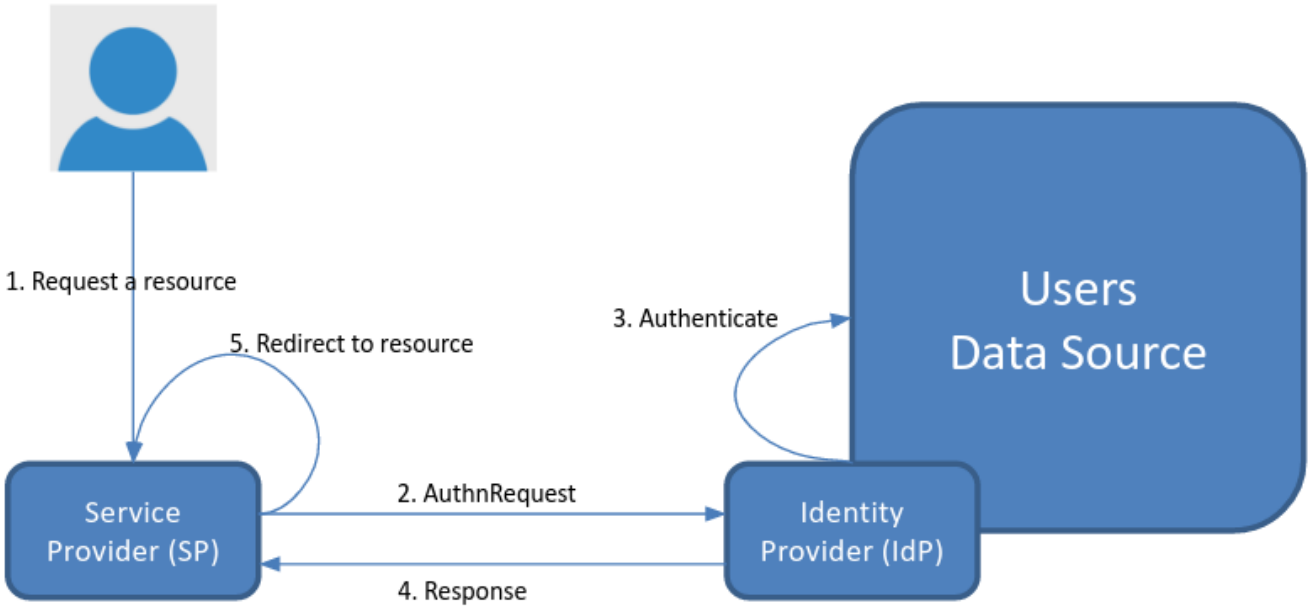
A SAML Request is sent to the Identity Provider, user authenticates against the Identity Provider and then information about user, is sent to our Service provider in a SAML Response, wich validates it and authenticate user .

There are two SAML authentication workflows: **IdP initiated SAML authentication** and **SP initiated SAML authentication**.

> Our ConcreteCMS service provider package support only **SP initiated SAML authentication**.

A typical SAML authentication process for authentication (**SP initiated SAML authentication)** works this way:

- The service provider requests authentication information about that specific user from the end user's identity provider.
- The identity provider responds to the SAML request with a SAML formatted, digitally signed response that identifies the end user and may include further information indicating that the user "is" or "is not" authenticated and authorized or not to access restricted resources.
- The service provider validates the response from the identity provider and authenticates the end user to give them access to restricted resources.
- The end user accesses the service provider's content or application.



Revision #23
Created Mon, Jul 26, 2021 11:12 AM by bilel
Updated Fri, Aug 20, 2021 12:04 PM by bilel