xtendx®
corporate media solutions

simplex SAML2 Authentication

API & Example

contact xtendx:

support@xtendx.com

Table of Content

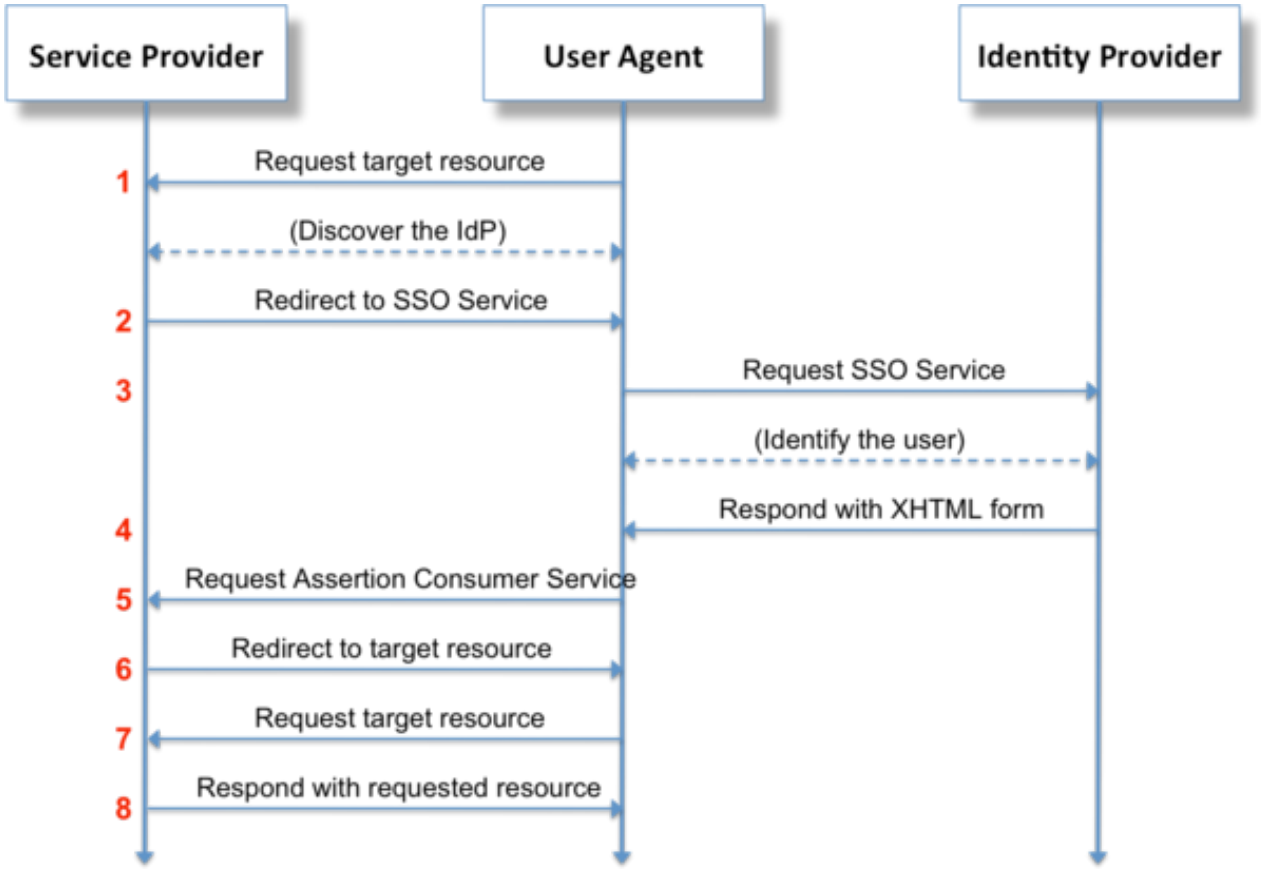
Description

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

At simplex, SAML2 is used in conjunction with a customer identity Provider server like ADFS, OAuth, PingFederate, etc.

Principle

The basic principle is that the user - upon visiting a specific simplex video link - is not authenticated against a simplex login database but gets redirected to and authenticated by the customer identity provider. No direct connection between identity provider and (service provider) exists:



Benefits and Drawbacks

This allows a so called Single Sign On.

- The user experience is high because no login/password must be entered.
- No sensitive data is transmitted to/from the simplex servers.
- Access is as secure as the customer identity provider.
- What device/location a user is accessing from, if access to the identity provider is given, so is the access to simplex projects.

Options:

- SAML for groups allows access control for a group of single users which is defined in the ADFS (Requires SMS 3.3.0. & PRO 2.0.3).

Drawbacks:

- A one time setup configuration is required on both identity provider and service provider sides.

Installation & Activation

1. Identity provider & service provider **Manifests** for stage & prod environments are prepared and synchronized.

2. On simplex side, SAML2 needs to be activated for a specific customer or author level.