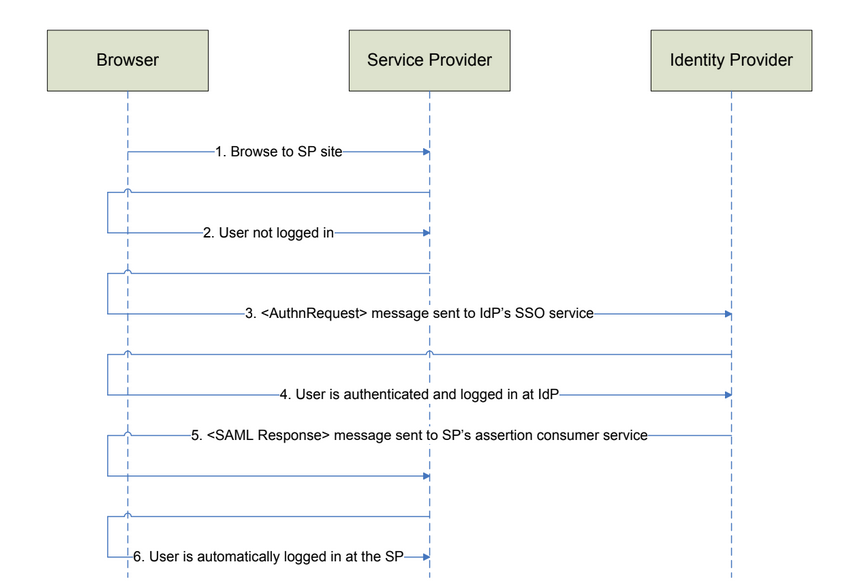
**SP initiated SSO**



In SP-initiated SSO, the user starts at the SP site and, instead of logging in at the SP site,

SSO is initiated with the IdP.

* The user browses to the SP site.
* The user attempts to access a protected page requiring the user to be

authenticated.

* The SP sends an authentication request to the IdP’s SSO service endpoint.
* If the user is not already authenticated at the IdP, the user must present their

credentials and login.

* The IdP sends a SAML response containing a SAML assertion to the SP.
* The SP uses the information contained in the SAML assertion, including the

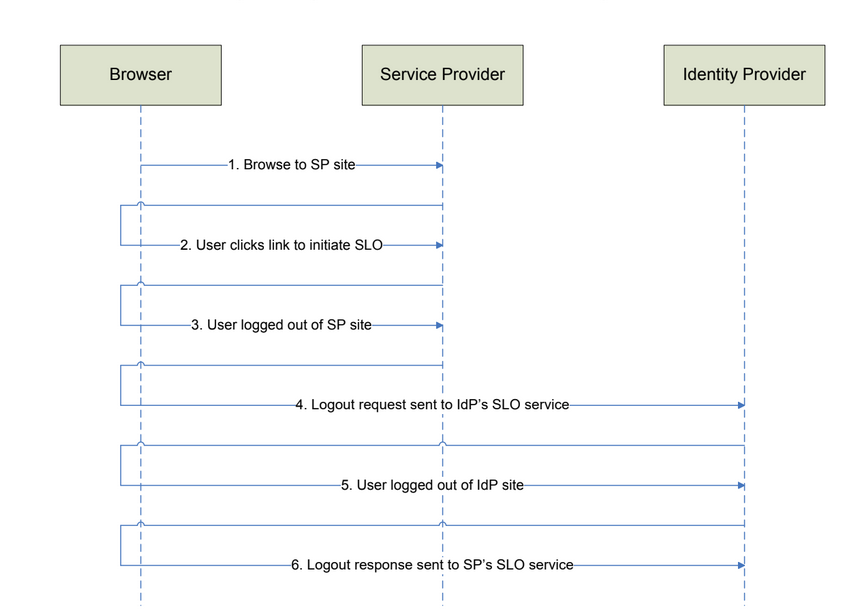
user’s name and any associated attributes, and performs an automatic login.

**SP-Initiated SLO**

In SP-initiated single logout (SLO), the user starts at the SP site, and clicks a link to

logout out of the IdP site and every SP site to which there is an SSO session.

The following diagram outlines the SP-initiated SLO flow.



* The user has already SSO’d to one or more service providers.
* The user clicks a link at the SP site to initiate SLO.
* The user is logged out of the SP site.
* A logout request is sent to the IdP site.
* The user is logged out of the IdP site.
* A logout response is sent to the SP site.

**The following diagram outlines the IdP-initiated SLO flow.ComponentSpace DLL file.**

* All the APIs.

**Add Identity Provider Certificate public key**

* In Solution Explorer, open Certificates folder, open idp.cer file
* Paste the Identity Provider Certificate inside

**Add Service Provider Certificate private key**

* In Windows Explorer, go to the project directory, open Certificate folder
* Replace sp.pfx with your Service Provider Certificate private key
* Make sure the file name still sp.pfx

**Configure SAML request and response**

* In Solution Explorer, open saml.config file
* Fill in the empty values with Service Provider and Identity Provider information

**Add Identity Provider Entity ID to Web.config**

* In Solution Explorer, open Web.config file
* Fill in the empty value for PartnerIdP key with Identity Provider Entity ID

<add key="PartnerIdP" value="YOUR\_IDP\_ENTITY\_ID" />

**What Identity Provider Requires.**

Send this information to your Identity Provider to be added into their configuration

• Base URL: "http://localhost:49864"

• Assertion Consumer Service endPoint: "/SAMLSP/AssertionConsumerService"

• SLO Service endPoint: "/loginSP"

• SP EntityID: "YOUR\_SP\_ENTITY\_ID"

• SP certificate: "YOUR\_SP\_PUBLIC\_KEY\_CERTIFICATE"

**The ComponentSpace SAML components provide easy SAML enablement of ASP.NET applications.**

**SAML assertions, protocol messages, bindings, profiles and metadata are fully supported.**