ComponentSpace SAML for ASP.NET Primer

www.componentspace.com

Contents

Introduction

This is a brief introduction to Security Access Markup Language (SAML) single sign-on (SSO). For more detailed information refer to the SAML v2.0 specification documents at www.oasis-open.org.

The goal of SAML single sign-on is to minimize the number of times a user has to login at various web sites. It does this by having the user manually login at one site, called the identity provider (IdP), and then automatically logging in, without having to provide credentials, at one or more other sites, called the service providers (SPs).

A trust relationship must exist between the identity provider and service providers. Service providers trust that the identity provider has authenticated the user.

SAML supports two single sign-on flows - IdP-initiated SSO and SP-initiated SSO.

It also supports two single logout flows – IdP-initiated SLO and SP-initiated SLO.

IdP-initiated SSO

With IdP-initiated SSO, the user starts at the IdP site, logs in and clicks a link to the SP site which initiates SSO.

The following diagram outlines the IdP-initiated SSO flow.

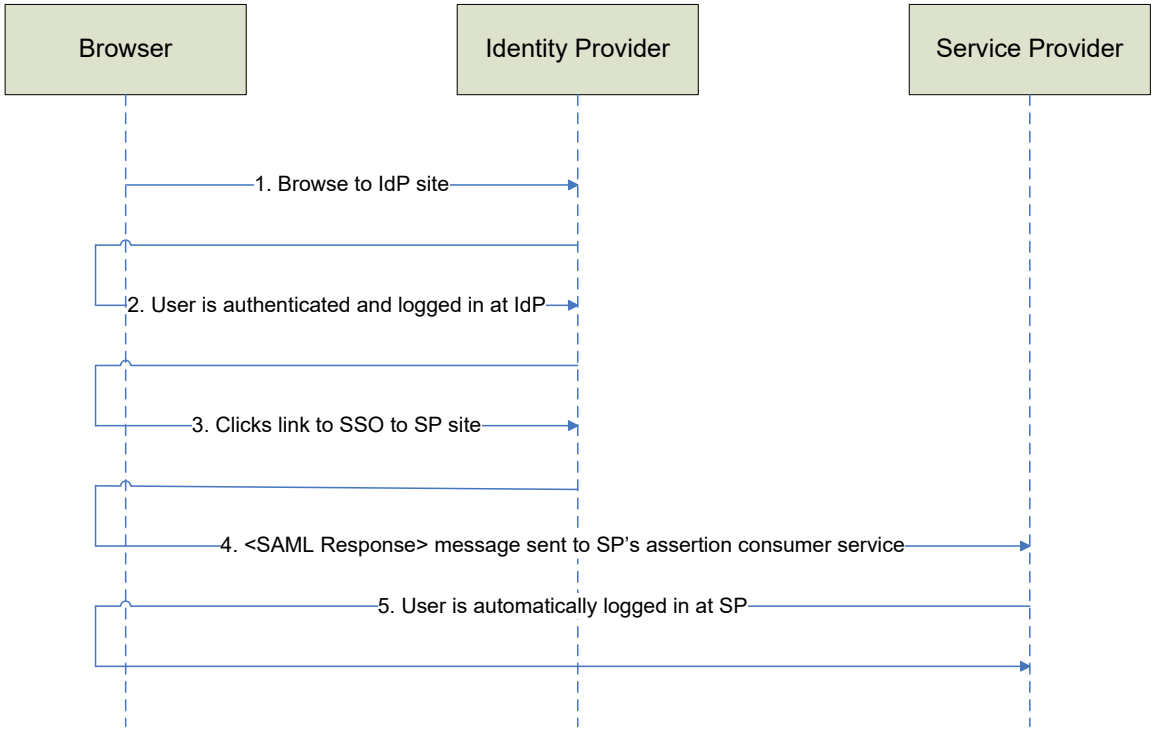

Figure 1 IdP-initiated SSO

1. The user browses to the IdP site.
2. If the user is not already authenticated at the IdP, the user must present their credentials and login.
3. The user clicks a link to the SP site.
4. The IdP sends a SAML response containing a SAML assertion to the SP.

5. The SP uses the information contained in the SAML assertion, including the user's name and any associated attributes, to perform an automatic login.

Note that steps 2 and 3 may be in reverse order.

SP-initiated SSO

With SP-initiated SSO, the user starts at the SP site and, instead of logging in at the SP site, SSO is initiated to the IdP.

The following diagram outlines the SP-initiated SSO flow.

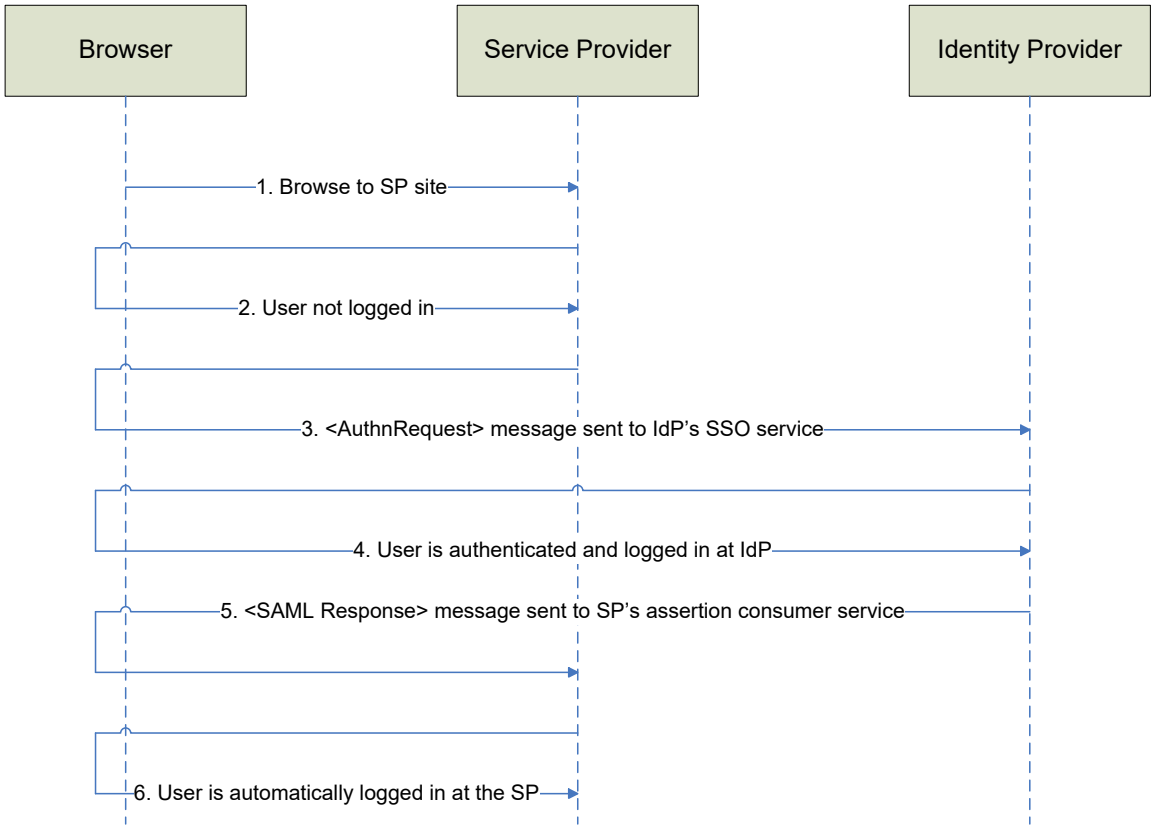

Figure 2 SP-initiated SSO

1. The user browses to the SP site.
2. The user attempts to access a protected page requiring the user to be authenticated.
3. The SP sends an authentication request to the IdP's SSO service endpoint.
4. If the user is not already authenticated at the IdP, the user must present their credentials and login.
5. The IdP sends a SAML response containing a SAML assertion to the SP.
6. The SP uses the information contained in the SAML assertion, including the user's name and any associated attributes, to perform an automatic login.

IdP-initiated SLO

With IdP-initiated SLO, the user starts at the IdP 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 IdP-initiated SLO flow.

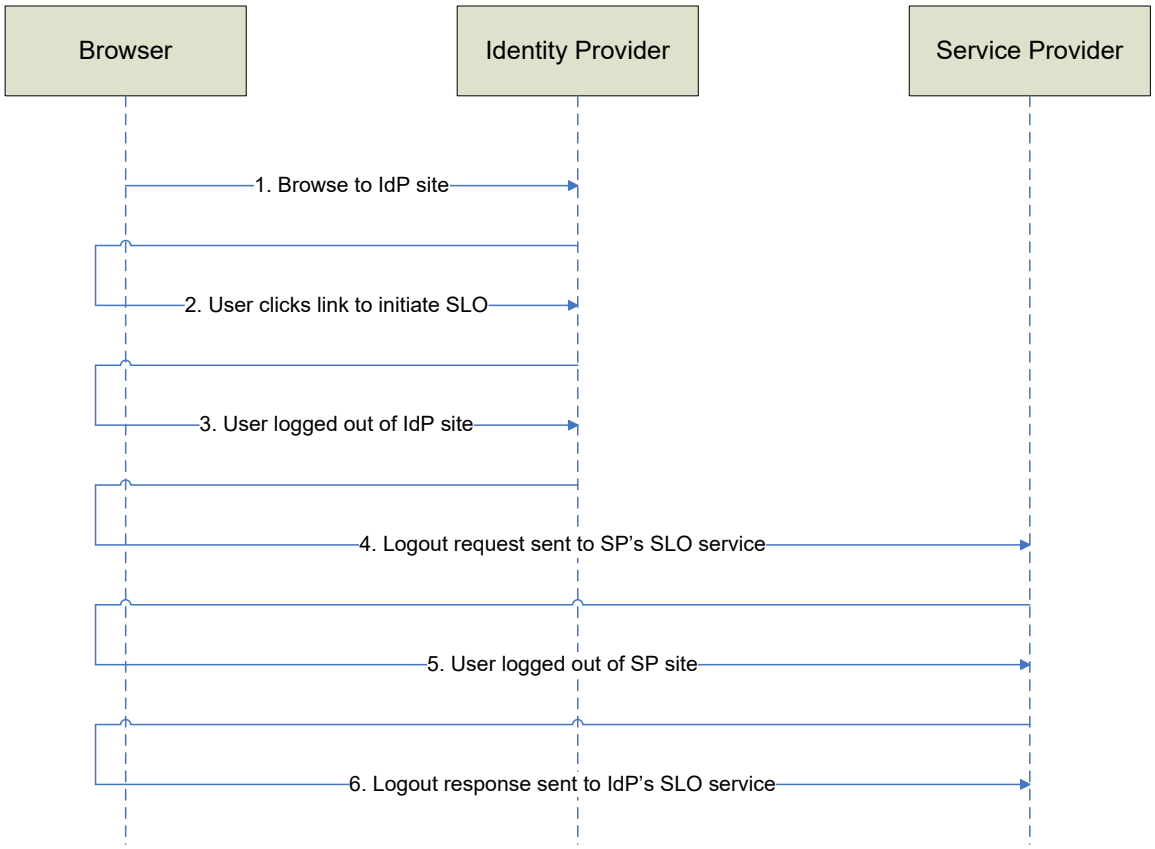

Figure 3 IdP-initiated SLO

1. The user has already SSO'd to one or more service providers.
2. The user clicks a link at the IdP site to initiate SLO.
3. The user is logged out of the IdP site.
4. A logout request is sent to the SP site.
5. The user is logged out of the SP site.
6. A logout response is sent to the IdP site.

Note that steps 4 through 6 are repeated for each service provider.

SP-initiated SLO

With SP-initiated 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.

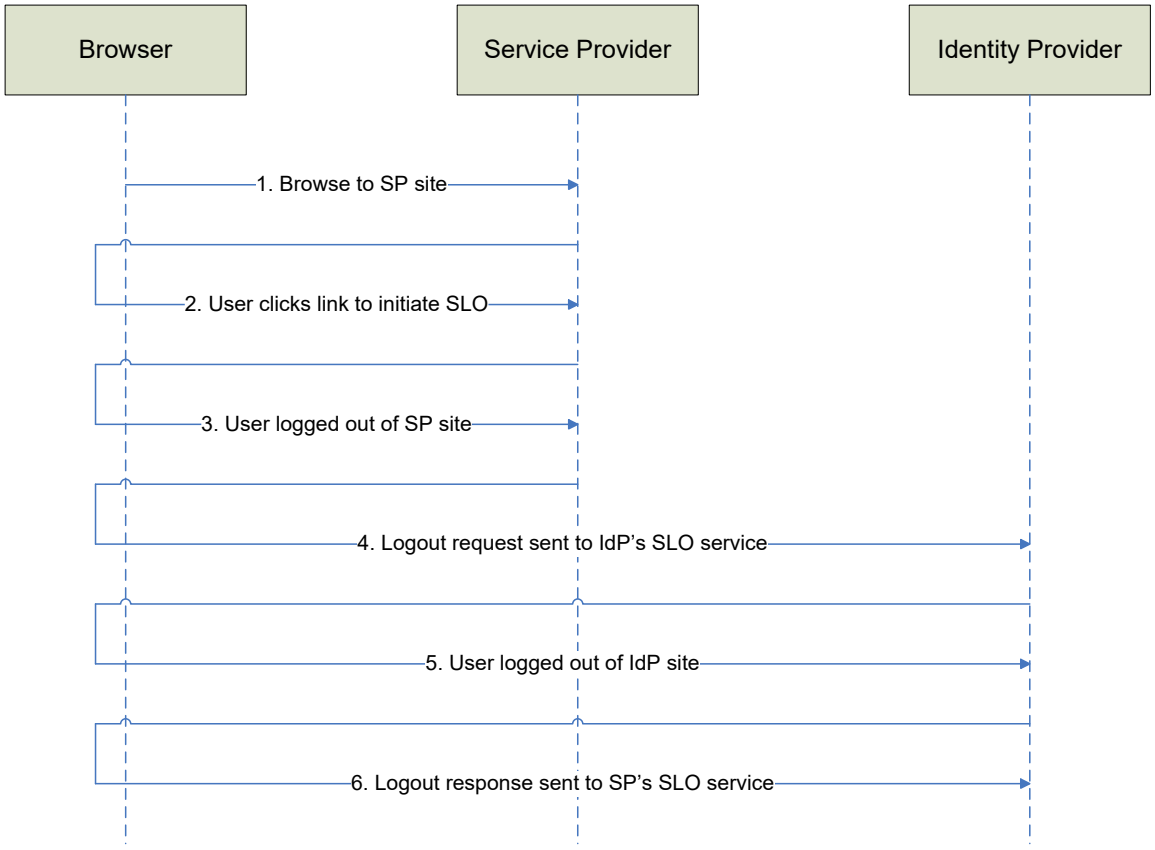

Figure 4 SP-initiated SLO

1. The user has already SSO'd to one or more service providers.
2. The user clicks a link at the SP site to initiate SLO.
3. The user is logged out of the SP site.
4. A logout request is sent to the IdP site.
5. The user is logged out of the IdP site.
6. A logout response is sent to the SP site.

Note that the identity provider sends a logout request and expects a logout response from every other service provider apart from the initiating service provider. This occurs between steps 5 and 6.

Security Considerations

Transport Level Security

The SAML specification recommends that all communications are over HTTPS.

This ensures the authentication of the endpoint as well as the integrity and privacy of information exchanged between the identity provider and service provider.

Note that passwords or other secret information should never be exchanged.

However, email addresses and other user-specific information is exchanged and should be kept private.

Transport level security is in addition to rather than instead of the security measures discussed below.

XML Signatures

XML signatures may be used to sign SAML messages, assertions and metadata.

An XML signature permits the identity of the sender to be confirmed and any changes to the signed XML to be detected. This ensures the integrity of the XML.

For example, when a service provider receives a signed SAML response from an identity provider, if the signature verification performed by the service provider is successful, then the service provider is assured that the SAML response came from the identity provider and that it hasn't been modified after signing. Therefore, having previously established a trust relationship with the identity provider, the service provider can safely consume the SAML response.

A signer signs with their private key and the verifier verifies with the signer's public key. For example, the identity provider signs the SAML response using the identity provider's private key. The service provider verifies the SAML response signature using the identity provider's public key.

It is highly recommended that either the SAML response or assertion is signed. Wherever possible, other SAML messages should also be signed.

XML Encryption

XML encryption may be used to encrypt SAML assertions, attributes and certain identifiers.

XML encryption ensures the privacy of any confidential data contained within the XML.

For example, a SAML assertion may be encrypted because it contains particularly sensitive user information.

A sender encrypts with the receiver's public key and the receiver decrypts with their private key. For example, the identity provider encrypts the SAML assertion using the service provider's public key. The service provider decrypts the SAML assertion using its private key.

XML encryption involves the creation of a random symmetric key which is used to encrypt the data. The symmetric key is then encrypted using the public asymmetric key. To decrypt, the private asymmetric key is used to decrypt the random symmetric key which in turn is used to decrypt the data. A symmetric key is used for performance reasons.

X.509 Certificates and Cryptographic Keys

XML signatures and XML encryption use asymmetric keys. These are the same type of keys used for HTTPS transport level security.

Typically, public keys are distributed in X.509 certificates.

As well as the public key, an X.509 certificate includes: a subject name; who issued the certificate; when the certificate expires; and a serial number.

Certificates may be stored in .CER files or in the Windows certificate store.

Private keys along with the associated certificate may be stored in password-protected .PFX files or in the Windows certificate store.

Private keys should never be distributed to external parties.

SAML Metadata

SAML metadata is a standard XML format for exchanging configuration information between identity providers and service providers. This occurs prior to any single sign-on activity.

It includes the name of the identity provider or service provider which is referred to as the entity ID.

It also includes URLs, certificates and various flags.

An identity provider or service provider may supply a partner provider with its SAML metadata. The partner provider will use the metadata to update its internal SAML configuration. Similarly, metadata received from a partner provider may be used to update the identity provider's or service provider's internal SAML configuration.

Its use is optional but encouraged.

If not used, SAML configuration information may be exchanged through email or some other means.