OASIS Security Assertion Markup Language (SAML) SSO Use Cases and Scenarios

Draft 01, 27 January 2003

Document identifier:

draft-cantor-sso-reqs-01

Location:

http://www.oasis-open.org/committees/security/docs/

Editor:

Scott Cantor, The Ohio State University and Internet2 (cantor.2@osu.edu)

Contributors:

RL 'Bob' Morgan, University of Washington
Prateek Mishra, Netegrity
Jahan Moreh, Sigaba

Abstract:

This document describes a set of possible requirements and use cases for extending the SAML 1.0 Browser/SSO profiles to encompass additional functionality and flows.

Status:

This is currently an individual submission that reflects contributions from the listed parties and other committee members, but does not reflect the consensus of the SSTC.

If you are on the security-services@lists.oasis-open.org list for committee members, send comments there. If you are not on that list, subscribe to the security-services-comment@lists.oasis-open.org list and send comments there. To subscribe, send an email message to security-services-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Security Services TC web page (http://www.oasis-open.org/committees/security/).

Table of Contents

1 Introduction

This document provides a proposed set of use cases and scenarios for a set of extensions (or possibly a framework around them) to the SAML 1.0 Browser Profiles for SSO in **[SAMLBind]**. There are no specific technical proposals included, only the scenarios that would drive them. Generally, the use cases focus on activity that would occur either before or after the exchanges that are defined by those profiles, although some of them may motivate extensions to the existing profile interactions to provide additional robustness or functionality.

The diagrams are constructed with the UML conventions described in **[SAMLReqs]**.

2 Use Cases and Scenarios

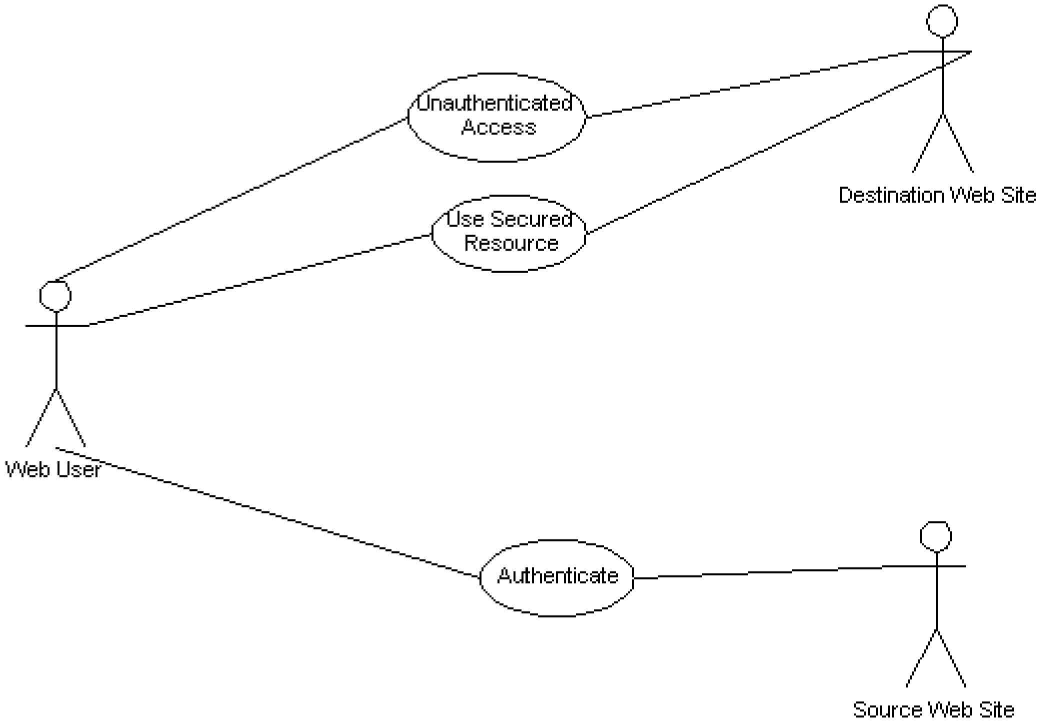
This section provides a set of high-level use cases for SAML SSO extensions, and use case scenarios that illustrate the use case. They give an abstract view of the extension. Each use case has a short description, a use case diagram in UML format, and a list of the steps involved in the case.

Note that, for each use case, the mechanics of how the actions are performed is not described. More detail provided in the detailed use case scenarios. Each of these high-level use cases has one or more specializations in the detailed use-case scenarios.

Each scenario contains a short description of the scenario, a UML sequence diagram illustrating the action in the scenario, a description of each step, and a list of requirements that are related to the scenario.

2.1 Use Case 1: SSO with Destination Site First

The SAML 1.0 SSO profiles define only a flow in which the source site authenticates a user and passes control and an authentication assertion (via push or pull) to the destination site. A common use case addressed by systems building on SAML is one in which the user first contacts a destination site without having signed on, and the user must then be sent to the source site to initiate the SSO activity before continuing.



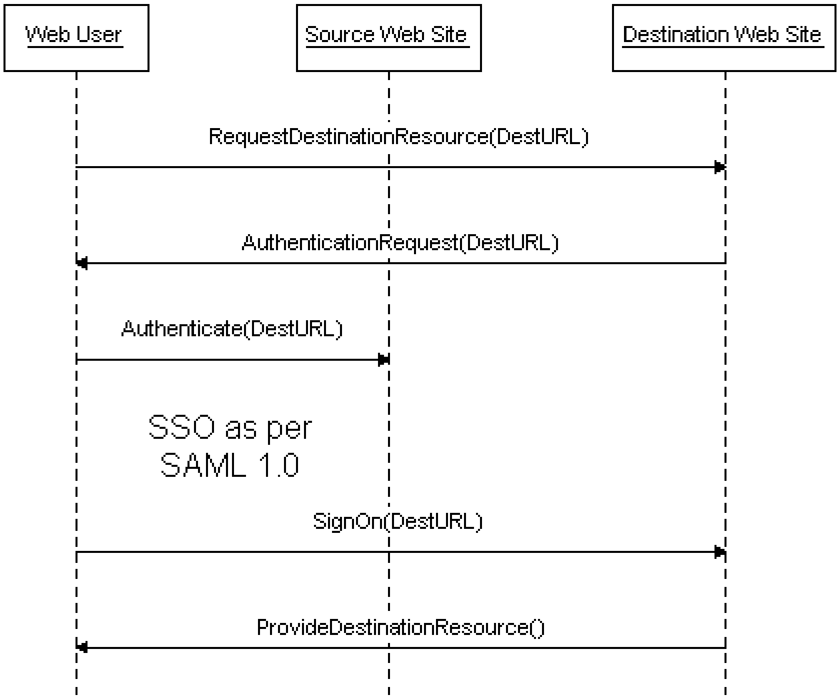
Use Case 1: SSO with Destination Site First

Steps:

1. Web user uses secured resource at the destination web site without having signed on.
2. Web user authenticates to source web site.
3. Web user uses secured resource at destination web site.

2.1.1 Scenario 1-1: SSO with Destination Site First, Pull or Push

This scenario supports the "destination site first" concept, in both the pull and push scenarios supported by SAML 1.0. The goal is a deterministic, unambiguous sequence of interactions starting from the first point of access.



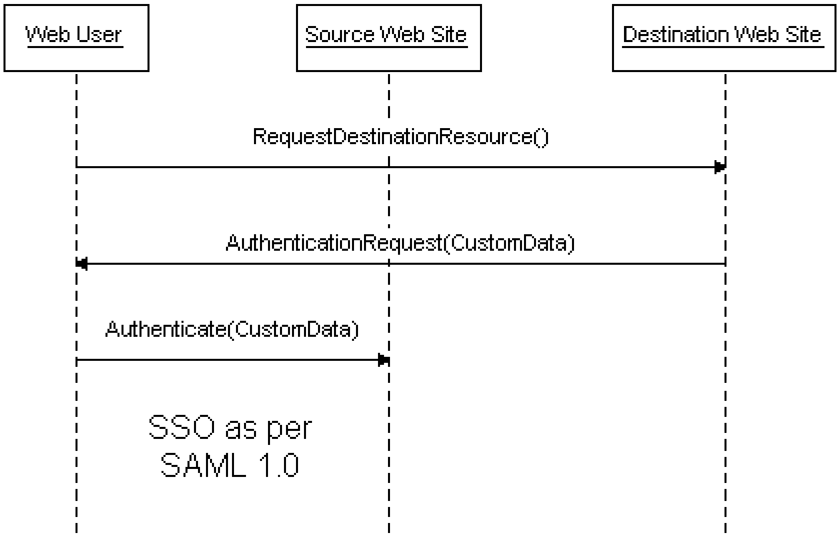
Scenario 1-1

Steps:

1. Web user requests a secured resource at destination web site, possibly without prior interaction with the site. The full address of the resource requested is denoted by "DestURL".
2. Destination web site redirects the web user to a source web site for authentication, including the "DestURL" in the request.
3. Web user authenticates to the source web site, providing the "DestURL". This begins one of the two existing SAML SSO profiles, both of which lead ultimately to the next step.
4. Web user signs on to destination web site at the completion of the SSO profile, again providing the "DestURL" address.
5. Destination web site accepts the user SSO action and returns the resource identified by "DestURL" (or rejects the attempt because of access control policy).

2.1.2 Scenario 1-2: SSO with Push Feature/Policy Customization

In this scenario, the destination web site is given the option to push data to the source web site to customize the processes, policies, or presentation of the authentication and/or SSO activity. The exact options available are immaterial to the flow.



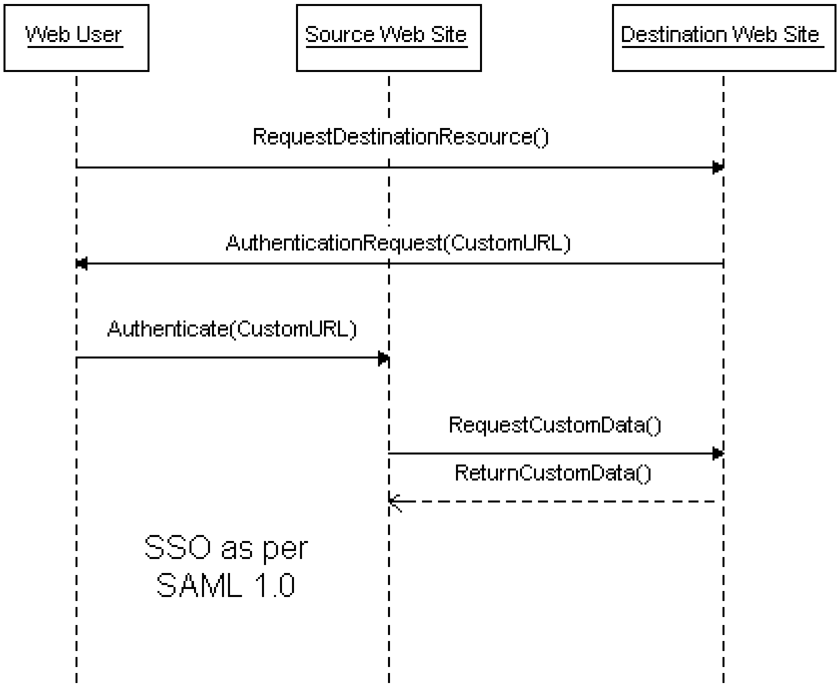
Scenario 1-2

Steps:

1. Web user requests a secured resource at destination web site, possibly without prior interaction with the site.
2. Destination web site redirects the web user to a source web site for authentication, optionally including customization data to affect the processing at the source site, based on agreed-upon semantics.
3. Web user authenticates to the source web site, the customizing data being applied as appropriate.
4. One of the two existing SAML SSO profiles is used to transfer the web user to the destination web site. Both profiles can accommodate carriage of extensions and additional data if the customization requested by the destination site necessitates this.

2.1.3 Scenario 1-3: SSO with Pull Feature/Policy Customization

In this elaboration, the destination web site is given the option to ask the source web site to pull data from it to customize the processes, policies, or presentation of the authentication and/or SSO activity. The exact options available are immaterial to the flow.



Scenario 1-3

Steps:

1. Web user requests a secured resource at destination web site, possibly without prior interaction with the site.
2. Destination web site redirects the web user to a source web site for authentication, optionally including a URL that will provide data to affect the processing at the source site, based on agreed-upon semantics.
3. Web user authenticates to the source web site.
4. The source web site pulls the customizing data from the destination web site, and applies it as appropriate..
5. One of the two existing SAML SSO profiles is used to transfer the web user to the destination web site. Both profiles can accommodate carriage of extensions and additional data if the customization requested by the destination site necessitates this.

3 References

The following are cited in the text of this document:

[SAMLReqs] Darren Platt, Evan Prodromou, et al., *OASIS Security Services Use Cases And Requirements*, http://www.oasis-open.org/committees/security/, OASIS, May 2001.

[SAMLCore] Phillip Hallam-Baker et al., *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)*, http://www.oasis-open.org/committees/security/, OASIS, May 2002.

[SAMLBind] Prateek Mishra et al., *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)*, http://www.oasis-open.org/committees/security/, OASIS, May 2002.

[SAMLGloss] Jeff Hodges et al., *Glossary for the OASIS Security Assertion Markup Language (SAML)*, http://www.oasis-open.org/committees/security/, OASIS, May 2002.