WEB Initial Sign-On Requirements Draft

Draft-internet2-webiso-requirements-07.html

Ryan Muldoon, Scott Fullerton

Date: 11/12/2001

Abstract

This document outlines the requirements for the Web Initial Sign-On initiative.

1. **Requirements:**

    1. WEB-ISO shall define a data format for authentication assertions and session management tokens, to allow for multiple implementations of the standard interoperating.
    2. WEB-ISO shall support ending a session due to absolute timeouts (e.g., the WEB-ISO login session will time out eight hours after first created).
    3. WEB-ISO shall support ending a session due to inactivity time-outs (e.g., an application authenitcation session will time out after thirty minutes of inactivity).
    4. WEB-ISO shall timestamp all authentication events, to facilitate absolute timeouts.
    5. WEB-ISO assertions shall timestamp last use to facilitate inactivity timeouts.
    6. WEB-ISO shall support user authentication sessions: both a login server authentication session for network-wide authentication, and application server authentication sessions for application authentication. General context sessions are out of scope for WEB-ISO.
    7. WEB-ISO assertions shall identify the issuing server.
    8. WEB-ISO shall support ending a session (whether it be application or login) due to logout by the principal.
    9. WEB-ISO shall define an API for implementing security backends for the login service.
    10. WEB-ISO shall protect its data from observation by third parties or untrusted intermediaries, to protect the principal’s privacy.
    11. WEB-ISO shall require all data to be signed by the issuing server to assure authenticity and integrity of data. This should be done in accordance with the University’s PKI policies.
    12. WEB-ISO shall operate both in and out of an SSL environment, although SSL is required for login server interactions.
    13. WEB-ISO shall support “application zones” where each application community can define its own required level of authenitcation.

14. WEB-ISO shall support application logouts, application zone logouts, and overall session logouts, where logging out of all application zones is equivalent to an overall session logout.

15. WEB-ISO shall not require of the principal anything beyond a standard browser.

16. WEB-ISO may support emerging uses of HTTP, as found in WebDAV and J2EE Servlet environments.

17. WEB-ISO shall work across multiple DNS domains.

2. Design Scope:

1. WEB-ISO only provides a single user ID, and no other user information.

2. WEB-ISO does not provide an inter-institutional authentication solution.

3. Design Goals:

1. WEB-ISO shall support third-party authorization mechanisms – potentially several at once.

2. WEB-ISO shall support integration of inter-domain authentication mechanisms (specifically including Shibboleth).

3. WEB-ISO shall work the same way regardless of authentication method.

4. WEB-ISO shall work the same way regardless of session management implementation.

5. WEB-ISO’s authentication architecture must support a PKI environment, as well as other authentication systems.

6. WEB-ISO must be platform-neutral

7. WEB-ISO should be easily extensible. This includes a modular authentication backend that can seamlessly support many different authentication schemes at once.

8. WEB-ISO’s code should be structured in a modular way: HTML interface should be in separate HTML files, session management should be contained in a library, authentication mechanisms should be hidden from the rest of the program, etc.

9. WEB-ISO should move away from fixed data structures that pubcookie uses, and instead support a name-value pair variable support, which would allow not only common elements to be standardized, but at the same time would allow additional variables be added to the session as need be. This could potentially be namespaced XML fragments.

10. The authorization backend should also support stacking of approval based on physical location, time, or other factors.

11. Aspects of the session, such as timeout values, should be configurable based both on user input and limitations passed on from the authorization backend.

4. Issues:

1. Risk of replay attack needs further analysis. pubcookie seems to have addressed this with S/Ident. What options do we have available? Should we carry IP address info?
2. Interface to portal and other applications needs to be defined.
3. How to retrofit or otherwise build WEB-ISO connections to fairly closed systems (both server and client) needs to be addressed.

5. Recommendations:

1. WEB-ISO should be modular in design, so each piece of functionality is as independent of others as is possible.
2. Session Management should implement both cookie and non-cookie back-ends. If this is not done, cookies should be the preferred implementation choice. They are available on virtually every browser, they do not clutter the URL, and they don’t suffer from the same space limitations that alternate methods do.
3. The names of session variables should have a 'webiso_'prefix (unless where standardly-recognized variable names exist), so there are no chances of namespace clashing when integrating 3rd-party applications.
4. Suggest using the pubcookie data elements as a starting place for design.

webiso_netid	The user's NetID
webiso_loginTime	The Timestamp of when the user logged in
webiso_lastActivityTime	The Timestamp of when the user last interacted with the server
webiso_credentials	The user's Credential Type
webiso_serverID	The server's ID
webiso_version	The software version on the server
webiso_sessionType	The type of assertion this is (Login, Granting, Session)

Glossary of Terms

Data Format: A defined structure of data. This includes variable names, variable types, and the meaning behind the variables.

Principal: an entity whose identity can be authenticated: in this instance, a user.

Session: A lasting connection between a user and a server during which the state of the connection is maintained. State information in this instance includes user identity information.

Shibboleth Project: a related effort under the auspices of MACE, which is more or less about connecting local web-iso systems among institutions (cf., http://middleware.internet2.edu/shibboleth/)

Timeout: An error condition raised after a designated period of inactivity.

Timestamp: To mark an event or object with its time of occurrence or creation.

Web-ISO: Web Initial Sign-On. It is a technology that supports web-based applications to make use of session and authentication information from a prior login.

Web-ISO project: An Internet2 project under the auspices of MACE to facilitate the development of a shared open-source package that meets many sites' needs and which would also integrates well with Shibboleth