Assurance Enhancements for the Shibboleth Identity Provider

19 April 2013

This document outlines primary use cases for supporting identity assurance implementations using multiple authentication contexts in a Single Sign-On environment and provides a list of requirements that were derived from these use cases, scoped to the Shibboleth Identity Provider software. The reader is expected to have some technical background in concepts relating to assurance, federation, and the Shibboleth Identity provider.

The Background and Identified Identity Provider Use Cases sections provide context and rationale for the enhancements described in the Requirements and Specifications section. The Requirements and Specifications section provides the technical specifications that must be addressed in a proposed implementation of these enhancements.

Background

The InCommon Assurance Program[1] offers two identity assurance profiles: Bronze which is comparable to NIST 800-63-1 Level of Assurance 1 and Silver which is comparable to NIST Level of Assurance 2. Anticipating campus certifications, the Program has been exploring implementation issues of assurance, most notably with CI Logon, National Institutions of Health and the Department of Education. The latter two organizations are required to follow the Federal Identity Credential and Access Management committee's SAML2 Web SSO Profile for requesting Authentication Contexts (e.g., assurance profiles). CI Logon, run by NCSA, has more flexibility in its requirements.

Because the InCommon Federation uses the Security Assertion Markup Language (SAML) standard as the basis for technical interchange among participants, expressing the identity assurance between the service and identity providers is done using SAML2's construct of AuthnContext. The user requests access to a service, and the SP sends an Authentication Request message containing a <RequestedAuthnContext> element to the IdP. The IdP determines whether it can satisfy the request and sends a response back to the SP.

While testing, campus implementers identified the following issues, as of version 2.4 of the Shibboleth IdP:

- If a user used her password to log in as a Bronze authnContext, she had to use the same password to re-login for Silver. Shibboleth does not know that the same authentication method is used for both Bronze and Silver, forcing re-authentication, even when a previous context's authentication would suffice.
- If a user logs in with his password, accesses a Silver-service, but has forgotten his hardware token required to assert the Silver Authentication Context, he cannot decide to accept a lower level of service by telling the IdP to go ahead and assert Bronze on his behalf. The login handler

[1] For more information , see assurance.incommon.org.

doesn't support such multi-factor use cases well.

- If an SP passed a list of Authentication Contexts [Silver, Bronze, unspecified] with the intent of having the IdP provide the highest possible Context for the user, the IdP would not process the list in a prioritized fashion, resulting in a Bronze Context sent one time, Silver another, and unspecified as well.

In January of 2013, InCommon convened the group described in the Acknowledgements section to share their testing experiences to date and assist in the development of a requirements document for an initial set of enhancements to the Shibboleth IdP to address these issues that could be 1) delivered to the Shibboleth Consortium for consideration in future IdP release and 2) used as a basis for an RFP to develop a short term solution for campuses interested in implementing assurance over-the-wire.

In summary, the testing group saw two primary SP use cases:

- The SP requests a specific Authentication Context, like Silver.
- The SP requests one of a set of Authentication Contexts, in priority order (*e.g.*, [Silver, Bronze]), that are required for different levels of service. The IdP presents a choice of authentication methods that will satisfy the request and for which the user is eligible, and returns the selected Context to the SP upon successful authentication. The SP then tailors the service provided accordingly.

In addition, the diversity in HIgher Education IdP implementations and the supporting identity management and authentication systems, suggests a certain level of configurability and flexibility in how the Shibboleth IdP supports the bullets above. To support the Silver Identity Assurance profile, an organization may determine that bringing its password infrastructure into compliance is a viable option, where another may layer on a multi-factor solution and bypass the complexity and scope of the current password infrastructure. The solution must be able to manage the use of multiple authentication systems, contexts in which they are required, and the user's ability to control their authentication method when multiple options exist.

Identified Identity Provider Use Cases

The working group identified three use cases that the final implementation should support. All make the following high-level assumptions:

- The IdP is configured to support one or more Authentication Contexts (sometimes written as Contexts in this document). These Authentication Contexts may be externally-certified identity assurance profiles, such as InCommon Silver or Bronze; a SAML-defined authnContext; or one locally defined by the IdPO.
- The IdP has access to an Identity Management System (IdMS) that maintains the Authentication Contexts for which each user is eligible.
- During a session, the IdP maintains information to track which of the current user's eligible Authentication Contexts have been authenticated and which have not. This information is referenced as a "Multi-Valued Session Object" in this document, although we do not anticipate

the creation of a new data structure. It is highly preferred that this information be accessed in structures that already maintained by the IdP.

In general, the IdP flow proceeds as follows:

A user accesses a service and the SP responds by sending an Authentication Context request for its required authentication context(s) to the Shibboleth IdP. The IdP invokes a Multi-Context Broker which

a. reviews a Multi-Valued Session Object for Currently Authenticated and Potential Authentication Contexts for which the user is eligible. The user's initial set of Potential Authentication Contexts is retrieved from the IdMS.
b. presents authentication options, if any, that satisfy the SP's request and upon interaction with the user,
c. Invokes an Authentication Method specific to the chosen authentication mechanism. Each Authentication Context will have one Authentication Method that the Multi-Context Broker will call.
d. Once the user is authenticated successfully, the specific Authentication Method will hand the session back to the Multi-Context Broker which will update the Multi-Valued Session Object and construct a reply to the SP that the IdP will send.

1. User First Login; No Active Session

Jane uses her web browser to access a Bronze SP. She doesn't have a session with the SP, so she is redirected to her campus IdP and is presented with one of the following pages, depending on configuration:

1. A standard login page containing input text fields for her username and password. She types her username and password. The IdP then queries the IdMS with Jane's username to determine which authentication mechanisms Jane is authorized to use *and* satisfy the Authentication Context that the SP is requesting. As a result, the login page automatically adjusts itself to display only those options that will work for Jane.
2. A login page with the IdP's configured authentication mechanism(s) that satisfy Bronze (the requested Authentication Context).

Jane decides which mechanism to use, and proceeds with the authentication process. After successful authentication, the IdP looks up the Authentication Contexts that her chosen authentication mechanism can associate with her IdP session (note that these values may be specific to Jane). These values are stored in her Multi-Valued Session Object. The IdP returns the Bronze Authentication Context to the SP on Jane's behalf.

If authentication is not successful, the Authentication Method will have displayed an appropriate error message, and the Multi-Context Broker will re-display the list of appropriate authentication mechanisms, until successful authentication occurs or a configured number of attempts is exceeded and the IdP returns a failure response to the SP.

2. Active IdP session; Further authentication required

Sam has an active session with the IdP and accesses a resource. The SP requests the Silver Authentication Context on his behalf.

The IdP examines Sam's Multi-Valued Session Object to determine if he is currently authenticated, but his *current* authentication level does not satisfy the requested Context. He is eligible for a *potential* Authentication Context that would satisfy the SP's request with further authentication.

The IdP initiates the Multi-Context Broker to display Sam's potential authentication mechanisms that can satisfy the SP's request.

If Sam authenticates successfully, the IdP responds to the SP with the Silver Authentication Context. The Multi-Context Broker updates Sam's Multi-Valued Session Object to include the newly authenticated Context in the list of currently-authenticated Contexts.

If Sam cannot authenticate successfully, the IdP returns a failure response to the SP.

3. Active IdP session; SP sends a list of acceptable Authentication Contexts

Susan has successfully authenticated and has an active IdP session as a result. She now tries to access a service, which prompts the SP to send a request to the IdP with a prioritized list of acceptable Authentication Contexts.

The IdP has a Multi-Valued Session Object for Susan that has information about all the Authentication Contexts for which Susan is eligible and those for which she has authenticated. The IdP examines this session object for Susan to determine if

1. Susan is already authenticated for the highest priority requested Authentication Context for which Susan is eligible. If so, the IdP responds with that Authentication Context, and the SP grants access.
2. Susan has the *potential* to authenticate for Authentication Contexts requested by the SP, but Susan is not currently authenticated for all of them. The IdP initiates the Multi-Context Broker to prompt Susan for the authentication options for which she is eligible that will satisfy the SP's request, indicating the SPs order of priority. Susan selects one of the options. Upon successful authentication, the IdP returns the selected Authentication Context to the SP.
3. Susan is *not eligible* for any of the requested authentication mechanisms. The IdP responds with failure, and the SP denies access to resource.

Requirements and Specifications

Multi-Valued Session Object

The Multi-Valued Session Object holds the set of Authentication Contexts for which the user is eligible. These are retrieved from the IdMS through the use of the Shibboleth IdP's attribute resolver.

At any time during a session with the IdP, the Contexts in the Multi-Valued Session Object will have two subsets, those Contexts for which the user has already authenticated during the session (Currently Authenticated Contexts), and those for which the user is eligible but has not yet authenticated (Potential Contexts). The Multi-Valued Session Object contains the current values of these lists throughout the lifetime of the session.

Note that the Multi-Valued Session Object is a concept used in this document to facilitate specifying these requirements. In actual implementation, it is highly desired that its function be provided through existing information maintained by Shibboleth or the IdMS.

Proposals must include the functionality described here for the Multi-Valued Session Object.

Multi-Context Broker

The Multi-Context Broker is invoked by the IdP to handle cases when the SP sends a prioritized list of Authentication Contexts, when the user does not yet have a session, or when an Authentication Context is requested for which the user has not yet authenticated. The Broker presents the user with the prioritized list of the Authentication Methods that can authenticate those Authentication Contexts. Under certain circumstances (*e.g.*, when the Authentication Method is an SSO with an already-active session) those Authentication Methods may not require further authentication.

It is preferred that the Multi-Context Broker be implemented in Shibboleth v2 as a Login Handler plugin in order to minimize impact on the rest of the Shibboleth IdP.

The behavior of the Multi-Context Broker is as follows:

1. The Multi-Context Broker is invoked with a prioritized list of Authentication Contexts that have been requested by the SP in authnContextClassRef, as described in "Native SP Content Settings" (https://wiki.shibboleth.net/confluence/x/SIBC).
2. If the user does not have a current session with the IdP and if there are one or more authentication mechanisms that are supported by IdP that can satisfy the SP's request, then the Multi-Context Broker presents the applicable options to the user, indicating the SP's priorities. See Phased Presentation of Authentication Options below for more information.
3. If the user has a current session with the IdP, then the Multi-Context Broker examines the user's Currently Authenticated Contexts and Potential Contexts that match any of the requested Contexts, plus any other Contexts that have been configured as satisfying the requested Contexts. Currently Authenticated Contexts for which the user is no longer eligible (due to revocation during the current session) are not considered.

   a. If one of the Currently Authenticated Contexts satisfies the highest priority Authentication Context requested by SP, then the Multi-Context Broker invokes that Context's Authentication Method (to ensure that its session has not expired), and, assuming success, the IdP responds to the SP with that highest priority Authentication Context.
   b. If there are no Currently Authenticated or Potential Contexts that match, then the IdP returns failure to the SP.
   c. If no Potential Context is higher than a Currently Authenticated Context, then the highest-priority Currently Authenticated Context requested by the SP is returned to the SP.
   d. The Multi-Context Broker presents to the user with the list configured user-friendly names of the Authentication Methods associated with the Authentication Contexts that satisfy the requested Contexts, indicating the SP's priorities. When two or more Authentication Contexts share the same Authentication Method, that Authentication Method is presented only once for the highest priority of those Contexts. If there is only one such Authentication Method, it is invoked without requiring user input to select it.
4. Upon successful authentication, the Multi-Context Broker populates the Currently Authenticated Contexts and Potential Contexts in the Multi-Valued Session Object appropriately, and the IdP returns the selected Authentication Context to the SP.
5. Failure to authenticate, perhaps after repeated attempts within the Authentication Method, returns the user to the list of options, after the Authentication Method has presented any appropriate error messages. Exceeding the configured number of allowed failures causes the IdP to return failure to the SP.
6. When the SP does not request any Authentication Contexts, the Context is considered "unspecified." "Unspecified" may also be listed explicitly in the request as the lowest priority of a prioritized list of Contexts. Normally, any defined Authentication Context may be used to satisfy the "unspecified" context. If, however, an "unspecified" Context has been explicitly configured, then only the Authentication Contexts that satisfy it may be used.
7. The "unspecified" Authentication Context should be asserted to the SP in the manner it was requested. In other words, if the SP's request contained no Context, then the assertion should contain no Context. If, however, the "unspecified" Context was explicitly requested, then the assertion should contain the "unspecified" Context.

The user's browser experience is one of the following:

1. redirection to the SP (if currently authenticated for the highest-priority Authentication Context),
2. when there is only one possible Context, presentation of an authentication page by the Context's Authentication Method, or
3. when there are multiple possible Contexts, presentation of a page displaying multiple Authentication Methods. In this last case, the SPs priority for each option is shown. The user selects one of the options and (if required by the associated Authentication Method) is prompted to authenticate for the selected option.

Proposals must include the implementation of a Multi-Context Broker, as described in this section.

Configuration Options

1. **Multi-Context Broker.** Configuration for the Multi-Context Broker must include the following options:
    a. **Phased Presentation of Authentication Options.** The Multi-Context Broker may be configured in one of two ways to handle the case where the user does not yet have a session established:
        i. Present all of the IdP's configured Authentication Contexts that satisfy the SP's request (without knowledge of who the user is).
        ii. Invoke the Authentication Method for an Authentication Context that has been specifically configured for the purpose of initializing the user's session. Assuming successful authentication, the Multi-Context Broker re-enters its process flow for an already-existing session.
    b. The number of failed authentications that are allowed before the IdP returns failure to the SP.
    c. General layout of pages presented to the user (*e.g.*, institutional logo, SP name and logo, informational links), as is currently configurable for Shibboleth.

2. **Supported Authentication Contexts.** The list of all Authentication Contexts supported by the IdP must be configurable with the following information:
    a. The unique identifier of the Authentication Context, as defined for the SAML authnContext object.
    b. The Authentication Method required to authenticate this Authentication Context.
    c. Other Authentication Contexts that satisfy the requirements of this Authentication Context.

3. **Supported Authentication Methods.** The Authentication Methods associated with the supported Authentication Contexts must be configurable with the following information:
    a. Any information required to invoke the Authentication Method.
    b. A user-friendly display name.

See the Appendix for an example of configuring Authentication Contexts and Authentication Methods.

Other Specifications

1. Multiple places in the document reference returning failure to the SP. This should be done in the same manner that Shibboleth currently returns authentication failures to the SP.
2. Support for the isPassive option of a SAML request is highly desired to allow an SP to determine if a user is already authenticated for a specified Authentication Context.
3. It is highly desired that no new session-persistent data be created that would affect deployment of the Shibboleth IdP, particularly in a load-balanced environment.
4. A new API will likely need to be proposed for integrating Authentication Methods with the Multi-Context Broker. It is preferred that this be done in a manner that facilitates the conversion of existing Login Handlers into Authentication Methods, for example, by leveraging a

well-known API like JAAS or by renaming the existing Login Handler API's interfaces.

5. The method of specifying configuration options in this document should be consistent with existing configuration options for the IdP. (Note that this is likely to change in Shibboleth v3. When a v3 direction is known, proposals that have the potential to facilitate a future transition to v3 are preferred.)
6. Spring WebFlow and Velocity are likely to be incorporated in Shibboleth v3. They may be used as an alternative to v2 frameworks to implement the Broker's flows and for configuring page layouts. An existing integration of Spring WebFlow into Shibboleth v2 may be found at https://github.com/dima767/Shibboleth-IDP-Postlogin-Filter and https://github.com/dima767/Shibboleth-IDP-Postlogin-Flow.
7. Integration with Shibboleth's existing use of log4j for event logging is highly desired.
8. As much as possible, these enhancements should be implemented as plugins for the existing IdP software. Nothing in these enhancements should preclude the use of existing Shibboleth functionality or its ability to be extended by other software. In particular, an institution must be able to replace or override the Multi-Context Broker with other software to achieve similar functionality.
9. Duke University, Unicon, and Ohio State University have built Shibboleth extensions that address certain of the issues described in this document. They may be reviewed as potential models for this work.

Appendix: Configuring Authentication Contexts and Authentication Methods

The following examples illustrate potential uses for the hierarchy implied by the list of "Any other Authentication Contexts that also satisfy the requirements of this Authentication Context." that is part of any Context's configuration.

Coexistence of Locally and Externally Defined Authentication Contexts

Consider an IdP with four configured Authentication Contexts:

Authentication Context	Other Contexts that Satisfy	Authentication Method
InCommon Bronze	InCommon Silver, Local Green	Username1/Password1
InCommon Silver	Local Green	Username2/Password2
Local Yellow	Local Green	Username3/Password3
Local Green		Hardware Token

- A session authenticated at InCommon Bronze will not require further authentication for InCommon Bronze SPs.
- A session authenticated at InCommon Silver will not require further authentication for InCommon Silver or InCommon Bronze SPs.
- A session authenticated at Local Yellow will not require further authentication for Local Yellow SPs.
- A session authenticated at Local Green will not require further authentication for any SP.

Further, consider the following three users:

User	eduPersonAssurance
Joe	InCommon Bronze
Annik	InCommon Bronze, InCommon Silver, Local Yellow, Local Green
Said	InCommon Bronze, Local Green

- Joe can access only Bronze and "unspecified" SPs. ("Unspecified" SPs are those that do not request any specific Authentication Context.)
- Annik can access any SP. If she does not have her hardware token with her, she may access Bronze, Silver, Yellow, and "unspecified" SPs by using passwords.
- Said can access any SP. Unlike Annik, however, Said can access only Bronze and "unspecified" SPs without a hardware token. Silver, Yellow, and Green SPs require the Green hardware token.

Note that the combination of Local Green and InCommon Silver represent a method for associating two different Authentication Methods for InCommon Silver, where one group of users authenticates for Silver with the Username2/Password2 pair, and another uses a hardware token. SPs that request InCommon Silver will get InCommon Silver when, for example, Said authenticates for Local Green. At many institutions, this might be the only use of a Local Green, as an alternative authentication method for some other Context; SPs may never request it explicitly.

Configuring Multiple Authentication Methods for InCommon Silver

Consider an institution that utilizes two different authentication methods for their implementation of the InCommon Silver Identity Assurance Profile. Some people who are eligible for Silver authenticate with a username and password, while others authenticate with a multi-factor hardware token. Some people can authenticate either way.

The institution configures the following Authentication Contexts, one for each of these authentication methods. Other than Authentication Method, eligibility requirements for InCommon Silver and InCommon Silver-Token are the same. SPs will not be told about the InCommon Silver-Token Authentication Context; its purpose is only to associate a second Authentication Method with the other requirements of InCommon Silver.

Authentication Context	Other Contexts that Satisfy	Authentication Method
InCommon Silver	InCommon Silver-Token	Username/Password
InCommon Silver-Token		Hardware Token

If Burt is a username/password user, Alyssa is a token user, and Lee can authenticate using either username/password or a token, then their user records would be configured as follows:

User	eduPersonAssurance
Burt	InCommon Silver
Alyssa	InCommon Silver-Token
Lee	InCommon Silver, InCommon Silver-Token

Acknowledgements

Editors: David Walker, Shreya Kumar, and Ann West
Contributors : David Langenberg, Daniel Fisher, Martin Smith, Charles Tompkins, Tom Barton, Mary Dunker, Warren Curry, Steven Carmody, Scott Cantor, and Tom Scavo.