RFP for Shibboleth IdP
Draft v3

Issue 1: User has multiple credentials (say multiple passwords or multi-factor), and the credentials may allow different levels of access or correspond to different profiles. Before a user is logged in, which options should be presented from the IdP to the user?

Background: Before a user has been authenticated, the IdP does not know anything about the users possible levels of assurance. All the IdP knows is the requested level/levels of Assurance from the SP.

Proposed Solution: Based on the levels of assurance requested by the SP, the IdP presents the user with a login handler in the form of a dynamically configurable login page, listing the available acceptable methods of login. The user chooses their preferred (or applicable) authentication method and proceeds to enter credentials to authenticate. The IdP authenticates the user and responds to the SP with the appropriate level of assurance.

Enhancement 1: Login Handler
A login handler that presents the user with a list of appropriate authentication mechanisms to choose from. The list of authentication mechanisms is configurable and can be any of the following options:

1. The list of all possible authentication mechanisms
2. The list of mechanisms allowed for the acceptable assurance profiles requested by the SP
3. The list of authentication mechanisms displayed is the overlap of mechanisms that are valid for the user and are acceptable for the SP. This may require some initial information from the user to dynamically generate the list.

Use Case 1: Functional

1. User attempts to access resource managed by SP
2. SP sends a request to IdP with the allowed levels of authentication for the resource.
3. If the User does not have an active session
    a. IdP initiates login handler to display authentication mechanisms list for User Selection
    b. User authenticates using selected mechanism
    c. On successful authentication, IdP responds to SP with appropriate authentication level
    d. SP grants access to resource
    e. If Authentication is unsuccessful, login handler displays list of appropriate authentication mechanisms again, till successful authentication occurs
4. If the User has an active session
    a. If the IdP determines from the multi valued session object that the user is not capable of requested assurance level.
        i. The IdP responds with the current assurance level, which is not a match
        ii. The SP denies access to resource.
    b. If the IdP determines from the multi valued session object that the user is capable of requested assurance level.
        i. IdP initiates login handler to display authentication mechanisms list for User Selection
        ii. User authenticates using selected mechanism
        iii. On successful authentication, IdP responds to SP with appropriate authentication level
        iv. SP grants access to resource
        v. If Authentication is unsuccessful, login handler displays list of appropriate authentication mechanisms again, till successful authentication occurs

Use Case 1: Technical Implementation

5. User attempts to access resource managed by SP
6. SP sends a request to IdP with the allowed levels of authentication for the resource.
7. If the user does not have an active session with the IdP
    a. Based on the configuration, IdP communicates with/initiates the login handler to display the appropriate list of authentication
    b. Login handler presents a formatted web page listing appropriate authentication mechanisms.
    c. User selects applicable authentication mechanism and enters credentials
    d. IdP authenticates user if credentials are valid and responds to the SP with the corresponding level of assurance.
    e. IdP updates the multi valued session object to indicate the current assurance profile.
8. If the user has an ongoing active session with the IdP
    a. IdP inspects the multi valued session object associated with the user
    b. If any entry in the session object's list of currently allowed assurance profiles is amongst the profiles being requested by SP,
        i. then IdP responds with the requested profile to the SP and
        ii. SP grants access to resource.
    c. else, the IdP determines from the multi valued session object whether the user is capable of requested assurance level.
        i. If so, then the IdP communicates with/initiates the login handler to display only those authentication mechanisms applicable for the requested level(s) of assurance.
        ii. Login handler presents a formatted web page listing possible authentication mechanisms.
        iii. User selects applicable authentication mechanism and enters credentials
        iv. IdP authenticates user if credentials are valid and responds to the SP with the corresponding level of assurance.
        v. IdP updates the multi valued session object to include the newly authenticated profile in the list of currently allowed assurance profiles.
    d. If the IdP determines from the multi valued session object that the user is not capable of requested assurance level.
        i. The IdP responds with the current assurance level, which is not a match
        ii. The SP denies access to resource.

Question: Is there a need for a multi valued session object if we are using the the custom login handler?
Answer: Yes, When the user has an active session and the SP requests an authentication level that is applicable for the user, the IdP either directly responds or performs further authentication and responds with the assurance level. The multi valued session object prevents unnecessary re-login requests to user.

Issue 2: For a given resource, the SP may have a list of allowed Assurance levels. In the current design, when the SP sends a list of allowed assurance profiles to the IdP, the IdP does not parse the list in order of priority.

Enhancement 2: Prioritized List Parsing
A logical way for an IdP to parse a prioritized list of requested Assurance levels sent by the RP and respond accordingly. Parsing should be in the order specified by the SAML object.

Use Case 2: Functional

1. SP sends a prioritized list of acceptable assurance levels and order of parsing the list to IdP
2. If there is an active session of the user with the IdP,

a. The IdP examines the user's information to determine if any of the requested assurance profiles, in order, match any entry from the list of *currently allowed* Assurance profiles.
    i. If there is a match
    ii. then IdP responds with the requested profile to the SP and
    iii. SP grants access to resource.
b. The IdP examines the user's information to determine if any of the requested assurance profiles, in order, are in the *potential* list of profiles.
    i. If so, then the IdP communicates with/initiates the login handler to display appropriate authentication mechanisms
    ii. User selects applicable authentication mechanism and enters credentials
    iii. IdP authenticates user if credentials are valid and responds to the SP with the corresponding level of assurance.
    iv. IdP updates user information in current session to include the newly authenticated assurance pfofile to the list of *currently allowed* assurance profiles.
c. If the IdP determines from the user's information that the user is not capable of requested assurance level.
    iii. The IdP responds with the current assurance level, which is not a match
    iv. The SP denies access to resource.

4. If there is no active session of the user with the IdP
    a. The IdP invokes the login handler to present the user with a list of appropriate authentication mechanisms (based on configuration)
    b. User selects appropriate authentication mechanism
    c. On successful authentication, the IdP responds to the SP with the corresponding assurance profile.
    d. SP grants access to resource.

Use Case 2: Technical Implementation

SP allows multiple Assurance levels for resource.

3. SP sends a prioritized list of acceptable assurance levels in a single request to the IdP. The order and priority are specified in the SAML object.
4. The IdP examines list and
5. If there is an active session of the user with the IdP,
    a. The IdP examines the user's multi-valued session object, to determine if any of the requested assurance profiles, in order, match any entry from the list of currently allowed Assurance profiles.
        i. If there is a match
        ii. then IdP responds with the requested profile to the SP and
        iii. SP grants access to resource.
    b. The IdP examines the user's multi-valued session object, to determine if any of the requested assurance profiles, in order, are in the potential list of profiles.
        v. If so, then the IdP communicates with/initiates the login handler to display only those authentication mechanisms applicable for the requested level(s) of assurance.
        vi. Login handler presents a formatted web page listing possible authentication mechanisms.
        vii. User selects applicable authentication mechanism and enters credentials
        viii. IdP authenticates user if credentials are valid and responds to the SP with the corresponding level of assurance.
        ix. IdP updates the multi valued session object to include the newly authenticated assurance pfofile to the list of currently allowed assurance profiles.

d. If the IdP determines from the multi valued session object that the user is not capable of requested assurance level.
    v. The IdP responds with the current assurance level, which is not a match
    vi. The SP denies access to resource.IdP responds with the first match of assurance level from the prioritized list.

5. If there is no active session of the user with the IdP
    a. The IdP invokes the login handler to present the user with a list of authentication mechanisms determined by the entire list of allowed assurance profiles.
    b. User selects appropriate authentication mechanism
    c. On successful authentication, the IdP responds to the SP with the corresponding assurance profile.
    d. SP grants access to resource.

Enhancement 3: Multi-valued Session Object
A multi valued session object allows the IdP to keep track of all the different assurance levels associated with the user's session.

Note: In the Use Case discussed below, Profile A is considered a stronger Assurance level than Profile B.

Use Case 3: Functional
Multiple Passwords for different Assurance levels.
Different users may have a password that allows them Profile B access and a separate password for Profile A access.

1. User requests access to resource. SP requests Profile B from IdP.
2. IdP responds to SP with Profile B
3. In the same IdP session, the User now requests access to some other
4. SP requests Profile A from IdP.
5. IdP examines user information through the multi-valued session object to determine that user is capable of Profile A, with more authentication.
6. IdP invokes the login handler to present the User with appropriate authentication mechanisms.
7. User Selects appropriate authentication mechanism and enters credentials
8. On successful authentication, IdP responds to SP with Profile A and updates user information to set the current session status as Profile A.
9. SP grants access to resource.

Use Case 3: Technical Implementation
Multiple Passwords for different Assurance levels.
Different users may have a password that allows them Profile B access and a separate password for Profile A access.

10. User logs in with Profile B password, as resource requires Profile B. SP requests Profile B from IdP.
11. IdP responds with Profile B, but also has visibility, through the multi-valued session object, to the fact that the user is allowed Profile A access with more authentication. This information is maintained in the multi-valued session object as the currently allowed and potential assurance levels associated with user and required authentication mechanisms respectively.
12. In the same IdP session, the User requests access to resource that requires Profile A password.
13. SP requests Profile A from IdP.
14. IdP examines the multi-valued session object to determine that user is capable of Profile A, with more authentication.
15. IdP invokes the login handler to present the User with applicable authentication mechanisms available for Profile A.

16. User Selects appropriate method and enters second password (or corresponding authentication mechanism)
17. On successful authentication, IdP responds to SP with Profile A and updates session object to set the current session status as Profile A.
18. SP grants access to resource.

Description of the multi-valued session object

The multi-valued session object maintains the following information:

1. All *currently allowed* Authentication levels of the User
2. *Potential* Authentication levels allowed for user
3. Extra authentication mechanisms needed for higher levels of authentication, if applicable for User.

NOTE: At the IdP level, knowledge of the relative hierarchy or strength of Assurance profiles is maintained. (This is currently done for Silver and Bronze, therefore not mentioned as an enhancement.) Hierarchy of assurance profiles, indicating which are "higher" than others. The authentication required for a profile may be satisfied by an existing SSO session with the authentication method for a "higher" profile.

Generic Behavior:

When the IdP receives a request for a particular Assurance level:

1. If User has no active session,
    a. IdP invokes login handler to display all applicable methods of authentication as a list to User.
    b. User makes selection from list and enters corresponding credential information.
    c. If the user passes authentication, the IdP responds with the requested assurance level
    d. If the user does not pass the selected authentication method, the login handler displays the list to user again, for making a selection of different authentication mechanism, till successful authentication occurs.
    e. IdP also updates the session object to reflect *currently allowed* authentication level and *potential* authentication levels with information for custom login handler to use when redirecting.
2. If User already has an active session,
    a. IdP examines the session object's list of *currently allowed* assurance levels through the multi-valued session object.
    b. if any entry from the list of *currently allowed* assurance levels matches the requested assurance level, IdP responds with requested assurance level.
    c. else the IdP examines session object's *potential* Assurance levels.
        i. If requested Assurance level exists in the session object's *potential* allowed Assurance levels, then the IdP uses the custom login handler to redirect user for higher authentication.
        ii. On successful authentication, IdP returns requested Assurance level.
        iii. If requested Assurance level does not exist in the session object's *potential* Assurance levels, the IdP responds with any of the *currently allowed* authentication levels, which is not a match.
        iv. SP denies access to resource.

Currently Allowed levels of Assurance: Based on the successful authentication mechanism, for the user's current session, this field contains all the assurance levels that the user authentication mechanism allows.
Potential levels of Assurance: Based on information about the user, this field stores all the assurance levels that the user is capable of, but with extra authentication than the authentication mechanisms used for that session already allow.