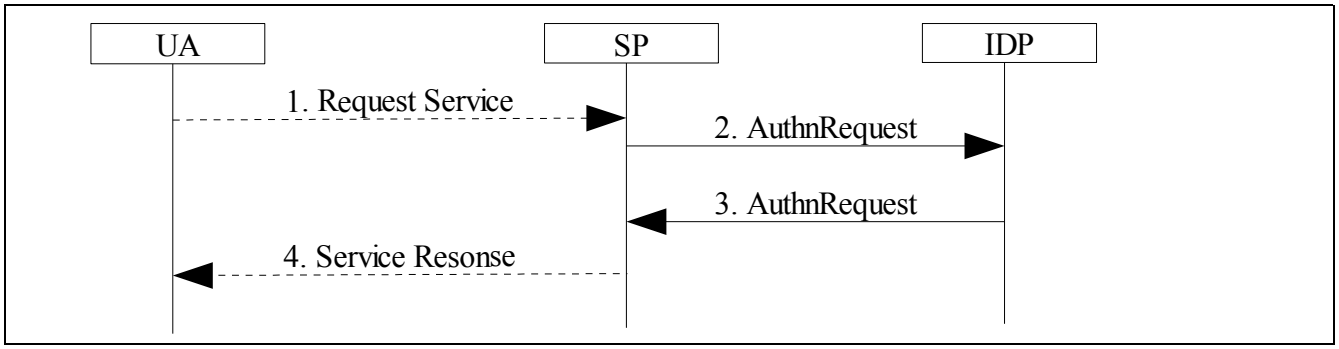
SOAP SSO Profile Proposal

A SOAP-based SSO profile of the Authentication Request protocol in [SAMLCore] is proposed to cover the following use cases :
- Support SP access by a user when redirect/ECP based interactions are not possible.
– SP initiated authn when user is offline.

Required Information

Identification: urn:oasis:names:tc:SAML:2.0:profiles:SSO:SOAP
Contact information: TBD
SAML Confirmation Method Identifiers: The SAML V2.0 "bearer" confirmation method identifier, urn:oasis:names:tc:SAML:2.0:cm:bearer, is used by this profile.
Description: Given below.
Updates: None

The general SSO flow is shown below :



Step 1 : User accesses SP. This step is optional.

Step 2 : SP determines IDP and sends a SAML AuthNRequest to it.

Step 3 : IDP verifies AuthNRequest, sends back a AuthNResponse

Step 4 : SP creates local security context and offers service to the user.

There are several variations on the basic flow:
a) User already authenticated at IDP
b) User not authenticated at IDP
c) Account linking/nameidentifier exchange
d) ForceAuthN
e) SP requested AuthContext

Notes:
1) SOAP Binding is expected to be the basis of this profile.
2) As with other profiles, actual authentication at SP and IDP is out of scope – however certain guidelines will need to be supplied to cover cases where SP/IDP ends may not have access to a traditional browser like UA.
Another consideration is to add ability for SP to communicate context to the IDP such as :
– Subject for whom authN response is desired
– Additional data (eg in one usecase an encrypted MSISDN needs to be communicated) for IDP to understand the context of the request.

To be covered :
IDP discovery
MetaData updates
How this relates to ID-WSF SSO service.

Single Logout

Comparison with ID-WSF SSO Service

Liberty ID-WSF Authentication, Single Sign-On, and Identity Mapping Services Specification describes two SSO profiles that are related to this proposal.

From the intro of the the SSO Service (SSOS) :
The ID-WSF Single Sign-On Service (SSO Service, or SSOS) provides requesters with an ID-WSF-based means
896 to obtain *SAML 2.0 authentication assertions* enabling them to interact with *SAML 2.0 Service Providers* (SPs)
897 [SAMLCore2]

As a result both the profiles clearly distinguish between three interacting entities : a “client/requester”, a relying party (SP) and an IDP – the “client/requester”.
Profile 1 (ECP SSO profile) is designed for intelligent clients (LUADs) - its an extension of SAML2 ECP profile – steps 4 thru 5 use SOAP call (instead of http) to obtain the AuthNresponse from the IDP.
Profile 2 (SAML Token Service profile) covers the case where the client issues a AuthNRequest (instead of the relying party in most other profiles) to access the SP.

This proposal shares the use of SOAP binding for exchanging a AuthNResponse for a AuthNRequest with these profiles – however it differs from them in the absence of intermediaries – ie, the SP/relying party directly interacts with the IDP.

It should be possible to leverage the “SAML Token Service profile” to a large extent.
