Suggested Profiling

Significant profiling of SAML should be unnecessary because the Shibboleth software already provides sufficient coverage of the options that might come up. The ECP client role does not impose significant implementation costs, so it should be adoptable in full.

ID-WSF, on the other hand, is a much more complex set of specifications with many options and advanced features. For our purposes, we will profile this down severely in the initial stages. We can admit new options as they become needed.

We propose the following:

- Disallow all optional ID-WSF SOAP Binding header blocks, leaving only the minimal required set to be compliant.
  - As a consequence, the IdP will not maintain state with proxying services (though it might maintain state with the **proxied-to** services for logout purposes).

- Support only the `urn:liberty:security:2006-08:ClientTLS:peerSAMLV2` and the `urn:liberty:security:2005-02:TLS:Bearer` security mechanisms for authentication of services to the IdP. This avoids a requirement for complex signature creation on the part of the ECP client, and allows for either bearer or holder-of-key authentication via a SAML assertion.
  - Should message signing be a desirable approach, the `urn:liberty:security:2006-08:TLS:SAMLV2` mechanism can be implemented, but this will require profiling WS-Security sufficiently to keep the work manageable.

- Require that the EndpointReference information for the IdP's SSOS signal either that no security token is required (unlikely), or that the enclosing assertion in which the EndpointReference appears is to be used. Embedding additional tokens or referencing other external tokens will not be supported.