LTI SSO issues

LTI SSO

The proposal from Dr Severance is based on the basic idea that the TC sends along enough information to the TP so that it (the TP) can re-establish the “same” SSO session as the TC has. In the SAML case this amounts to providing the entityID of the IdP so that the TP doesn’t have to run a full discovery flow.

In the interfederation case this is probably enough provided that the TC and TP both include the IdP in their trust. However, the flow should take care of the case when the TP is unable to find information about the IdP entityID. In this case the TP should probably return an error to the TC since in this case the launch would fail to complete.

This idea has been used before with some success. The difference in this case is that the application is running inside an iframe which changes the situation notably from a security perspective.

Displaying IdP login dialogues in an iframe is generally seen as a bad idea. The TP can of course use iframes if it “knows” that the SSO session will be established wo user intervention but this is not possible in general unless the tool is launched very soon after the TP SSO session was established.

In a page with multiple iframe tools this means launching even those tools that are not directly visible (eg those that are hidden behind “tabs” or other navigational controls).

Using a modal “popup” dialogue if/when interaction with the IdP is needed may seem like a good way around this but this would violate iframe security constraints and most won’t be possible to implement.

Here is an example that illustrates the problem:

1. User logs in to the TC. During login a session is established with the user IdP and the TC records the entityID of the IdP.
2. The user works in the TC but doesn’t launch any tools that require SSO/login. The user session with the IdP expires during this time.
3. The user (who still has an active session with the TC) launches a tool that requires SSO.
4. The TP gets the entityID and initiates an SSO session with the entity that the TC provides.
5. Since the IdP-session has expired the user is now required to login again which results in a dialogue with the IdP inside the iframe. This may be confusing and ugly and may even be explicitly blocked by the IdP.