Proposal on initial discovery of dynamic SAML 2.0 Metadata

Let's introduce federations.org as a discovery service. Every Identity Provider that supports dynamic SAML may ping this directory with it's existence and provide metadata and taxonomy to enable good navigation possibility between the thousands of IdPs listed in this discovery service.

If every SP is doing it's own discovery service, the user would have to select IdP at every SP.

User scenario step by step

User visits service A, and have not yet selected any IdP.

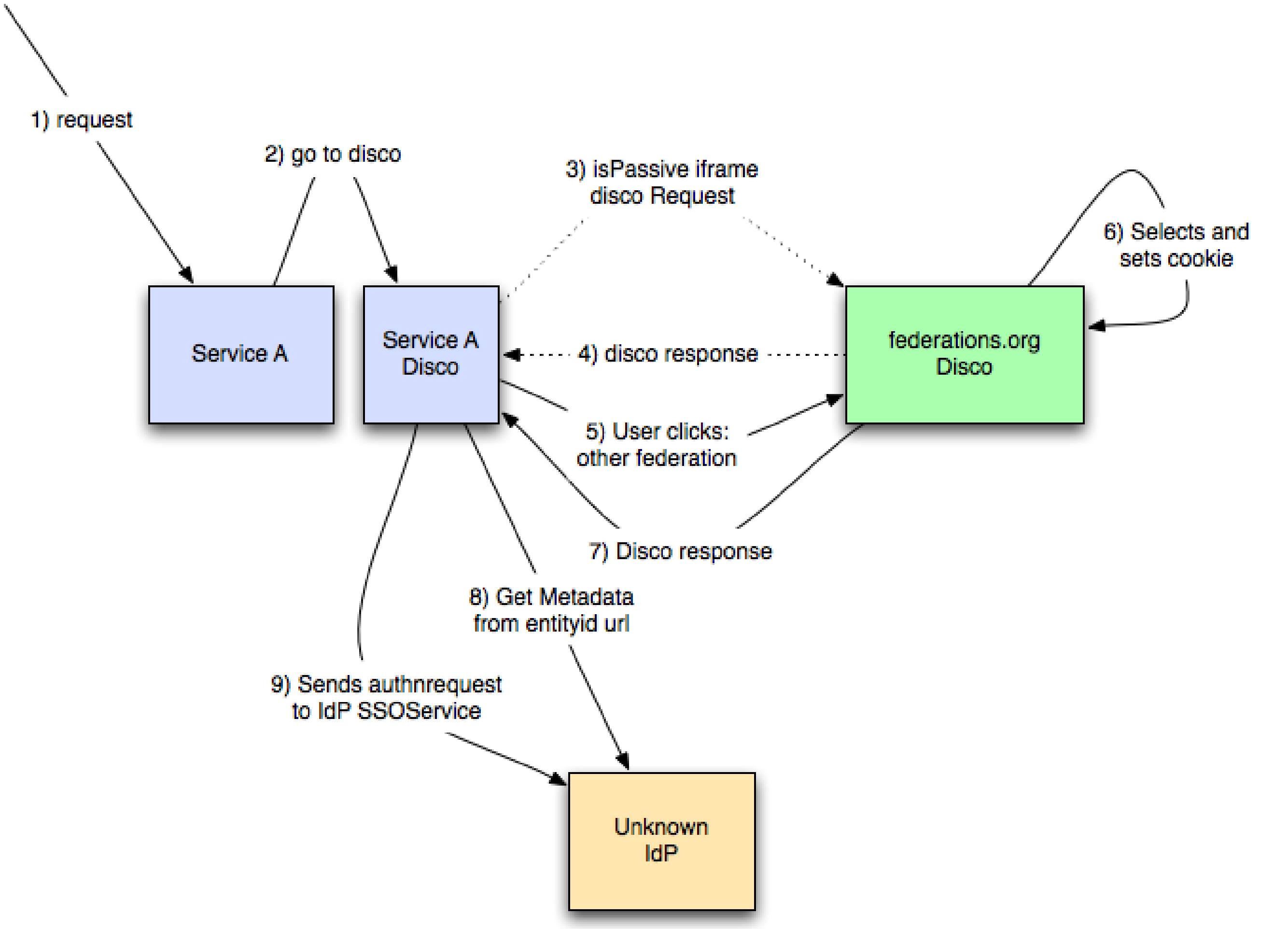
1. User goes to service A.
2. Service A has no entityid stored in a cookie, so it redirects the user to Service A Disco service.
3. The disco service shows a standard WAYF service, listing IdPs, and one of those IdPs is actually stating: "Other federation through federations.org". Clicking this will proxy the disco request to the federations.org directory of Identity Providers. The user will have to do this the first time.
4. The Service A disco service HTML page listing federations, also have a hidden iframe on the page where the src="" url is a isPassive disco request to federations.org. If the user has stored a value on federations.org (through another web page) it will redirect the iframe back to another endpoint on service A disco with the IdP entity ID.
5. The Service A disco service HTML page also have an AJAX script that periodically asks for whether an answer has returned from the passive disco request. If federations.org returned a IdP entity ID, then perform a GET request to the IdP entityID (which is an URL) and get the metadata.
6. Send the user with an AuthNRequest to the SSOService endpoint of the chosen IdP.

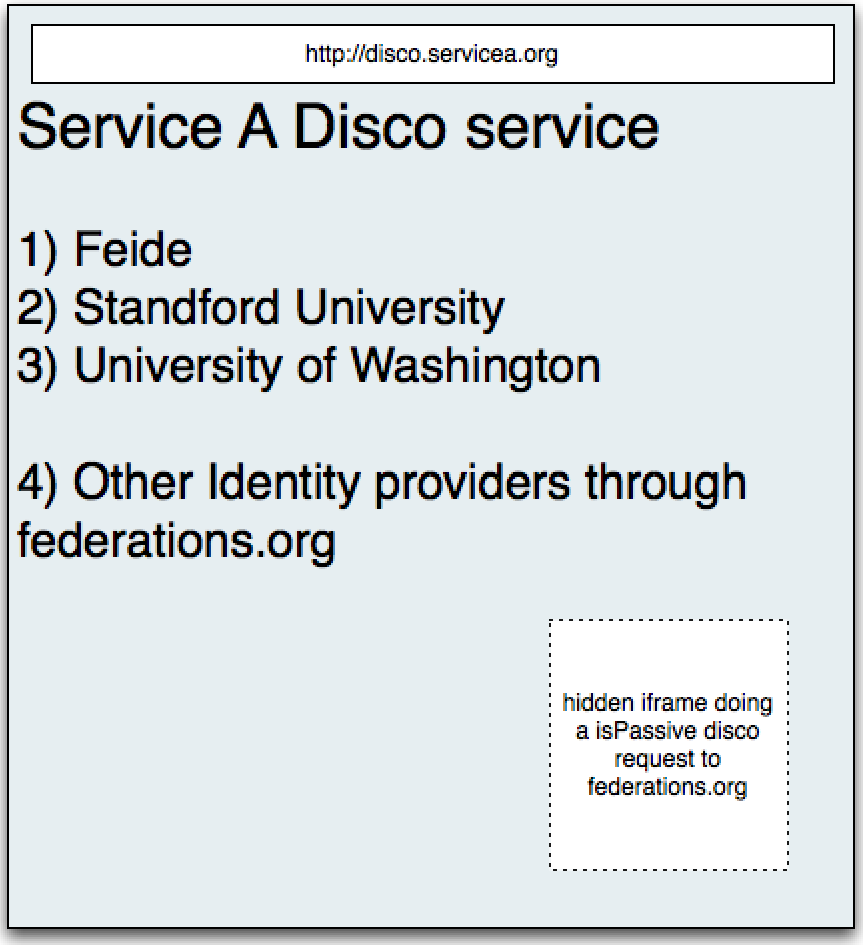
If the user did not select "Other Idetity Provider (Federations.org)" at the Service A Disco page, but selected one of the listed identity providers at the disco service, we still would like to store that information at federations.org so other SPs can read it.

This would require that we add a new parameter to the SAML 2.0 Metadata discovery protocol that allows us to set already chosen entityIDs. The cookie can be set to federations.org (from service A disco service) by a hidden iframe similar to this:

```
<iframe style="display: none" src="http://disco.federations.org?isPassive=true&SetSPentityID=feide.no" />
```

The reason why you would like to use hidden iframes instead of HTTP redirection is that you would not introduce federations.org as a single point of failure.


1) request
2) go to disco
3) isPassive iframe disco Request
6) Selects and sets cookie
Service A
Service A Disco
4) disco response
federations.org Disco
5) User clicks: other federation
7) Disco response
8) Get Metadata from entityid url
9) Sends authnrequest to IdP SSOService
Unknown IdP



http://disco.servicea.org

Service A Disco service

1) Feide
2) Standford University
3) University of Washington

4) Other Identity providers through federations.org

hidden iframe doing a isPassive disco request to federations.org