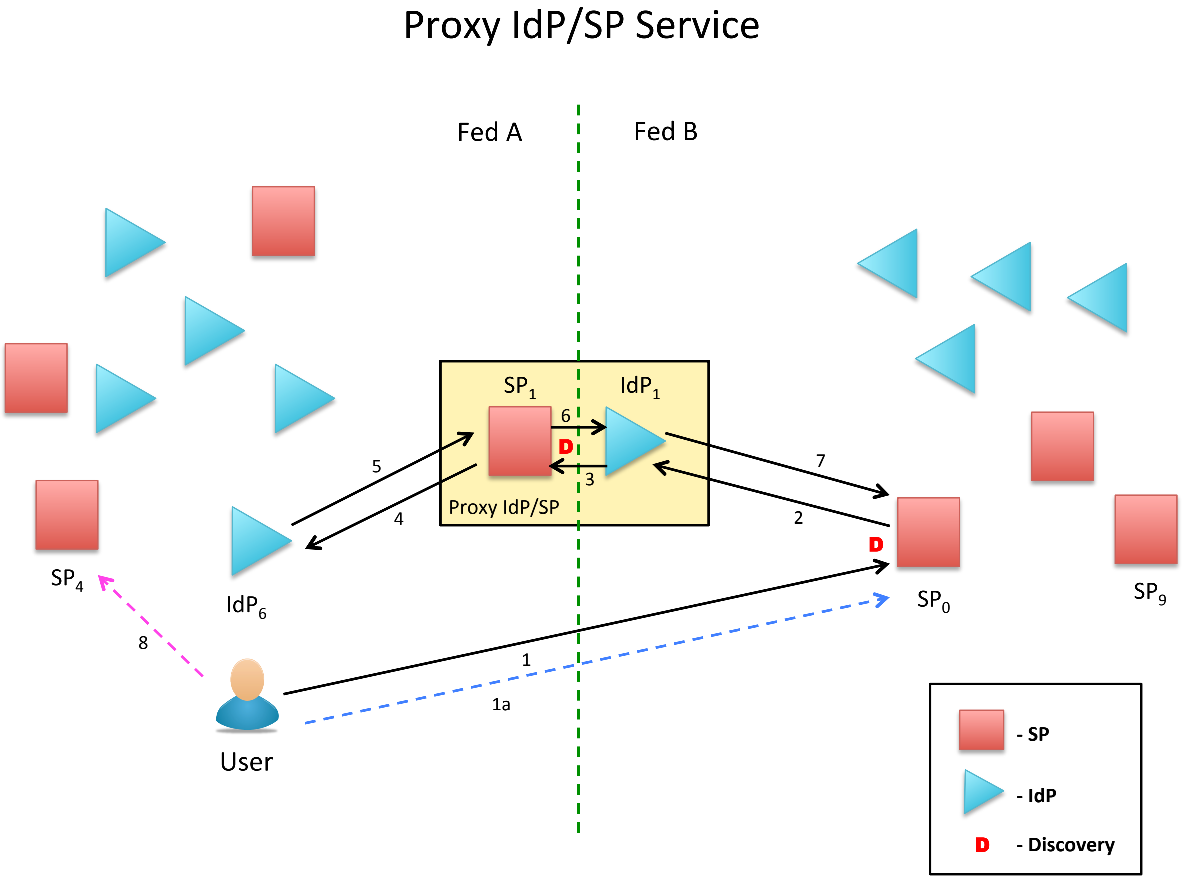
Proxy IdP/SP Service

Mark Scheible
MCNC
IAM Solutions Architect

Process*

1. User accesses resource protected by SP_0
2. Discovery service (D) identifies User's IdP as IdP_1 and redirects
3. IdP_1 transfers request to SP_1 (within Proxy) and discovery service (D) identifies IdP_6 as user's IdP
4. SP_1 directs User to IdP_6 for authentication/attributes at home institution
5. After User logs in, IdP_6 generates SAML assertion and returns User to SP_1
6. SP_1 transfers assertion to IdP_1 which generates its own assertion
7. IdP_1 returns User to SP_0 with SAML assertion from IdP_1



* For larger diagram & process see Slides 5 & 6

Notes

1. IdP_1 MUST be in Federation B's Metadata (a federation B entity)

2. User must go through two discovery services at least once - one for target SP and one for Proxy SP

3. Key issue of trusting the Proxy by both Federations

4. Somewhat mitigated by the fact that most SPs have bilateral agreements with IdP institutions

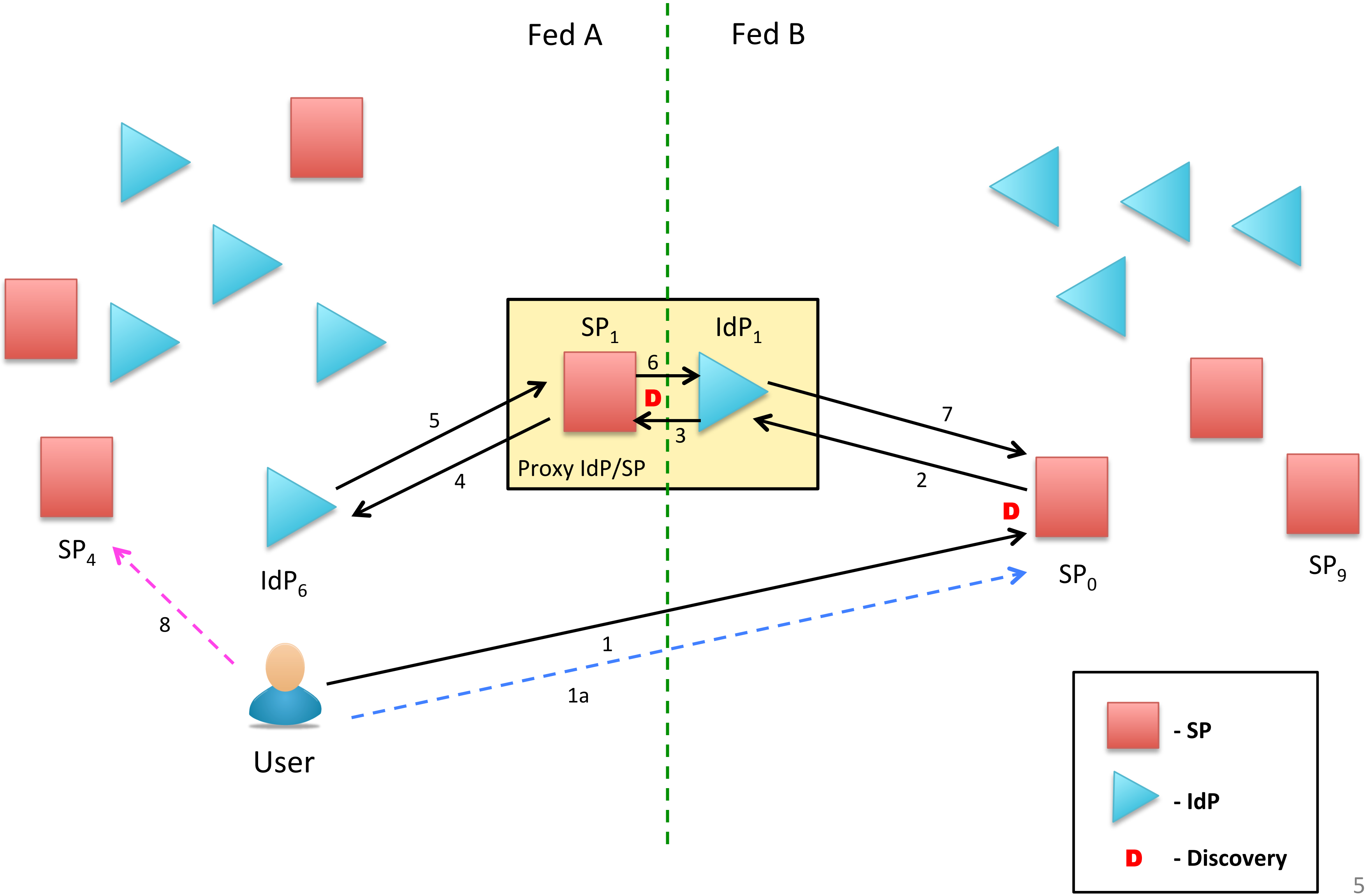
5. Could a cookie be used to capture the IdP for the Discovery Service(s)? (Generated by first pass through Proxy?)

6. Use of Proxy IdP/SP eliminates need to add all Federation A Entities into Federation B (and the reverse, if it applies)

7. Other?

Supplemental Slides

Proxy IdP/SP Service



Process

1. User accesses resource protected by SP_0
2. Discovery service (**D**) identifies User's IdP as IdP_1 and redirects
3. IdP_1 transfers request to SP_1 (within Proxy) and discovery service (**D**) identifies IdP_6 as user's IdP
4. SP_1 directs User to IdP_6 for authentication/attributes at home institution
5. After User logs in, IdP_6 generates SAML assertion and returns User to SP_1
6. SP_1 transfers assertion to IdP_1 which generates its own assertion
7. IdP_1 returns User to SP_0 with SAML assertion from IdP_1