ECP the discussion continues

ECP (the discussion continues...)

DATE and TIME: Fri May 27, 2011, 10am

CONVENER: Jim Basney

SCRIBE: Jim Basney

# of ATTENDEES: 15

MAIN ISSUES DISCUSSED

- Discussion continued from yesterday.
- ECP use cases:
  - IMAP (Live@EDU example)
    - also activesync for Outlook and portable devices
    - Microsoft provides the ECP gateway, credentials go to MS, prefer to have ECP gateway at institution
  - Google support for ECP; currently need to send password hashes; outreach from InCommon to Google?
  - ECP PAM module
  - command-line & thick-client apps
  - smartphone campus apps (OSU work on this?)
  - PESC registry of web services
- ECP authentication options: HTTP Basic Auth, X.509, Kerberos
  - DOE labs doing certificate-based authentication
    - DOEGrids test IdP accepts grid certificates
  - campus adoption of certificate-based authentication
  - most campuses today do password-based
  - concern: do clients support certs? most rich clients don't?
  - consider OAuth as an authentication mechanism for ECP
  - wide adoption of certificates in HPC/grid space
- Shibboleth ECP configuration
  - https://wiki.shibboleth.net/confluence/display/SHIB2/ECP
  - https://wiki.shibboleth.net/confluence/display/SHIB2/IdP+ECP+Extension
  - https://wiki.shibboleth.net/confluence/display/SHIB2/IdPSAML2ECPProfileConfig
  - https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPSessionInitiator
    - SP Example:

```
<SessionInitiator type="Chaining" Location="/Login" isDefault="true" id="Intranet"
relayState="cookie">
  <SessionInitiator type="SAML2" ECP="true" />
  <SessionInitiator type="SAMLDS" URL="https://parsley.phys.uwm.edu
/LIGO_SAML_DiscoveryService" />
  <SessionInitiator type="SAML2" template="bindingTemplate.html" ECP="true" />
</SessionInitiator>
```

- What will the pushback be if we ask IdP administrators to enable ECP?
  - Suggestion: setup test SP environment to help them test ECP
  - IdP 2.3 support for ECP helps
  - Any risk to enabling ECP in IdP? Make sure you enable HTTPS (encrypted channel).
  - May not be ready to upgrade to IdP 2.3. (Note XSS vuln.)
- Attribute release for ECP
  - How will consent work? uApprove is browser-based.
  - Consent when you download the client?
    - Example: command-line client from Debian distribution.
  - Consent build-in to the client?
- Client configuration
  - IdP & SP discovery information
  - Downloadable configuration (from resource they want to access)
    - Bundle in discovery and consent at this point
    - Use browser as one-time on-boarding mechanism
- ECP discovery: SAML metadata?
- If SAML response is encrypted, how does ECP client handle it?
  - Does ECP client need to modify the authentication response before sending it to SP?
  - Ask Scott Koranda about this.
- How to coordinate work / discuss?
  - Use shib-dev mailing list & Shibboleth wiki.

SUMMARY FROM REPORT-OUT TO THE LARGER GROUP: Due to requests for non-browser based flows, this is getting more attention. ECP is taking off, and there is more energy around what is required to implement it. Discussion will take place on the Shibboleth-Dev list

ACTIVITIES GOING FORWARD / NEXT STEPS

- See notes from yesterday.

- Investigate consent issue

- Investigate consent issue