Good Federation Citizenship

IAM Online
May 28, 2014

Jim Basney, National Center for Supercomputing Applications
Eric Goodman, University of California Office of the President
Keith Wessel, University of Illinois at Urbana-Champaign
Thank you to InCommon Affiliates for helping to make IAM Online possible

Brought to you by Internet2’s InCommon in cooperation with the Higher Education Information Security Council
Good Federation Citizenship

IAM Online
May 28, 2014

Jim Basney, National Center for Supercomputing Applications
Eric Goodman, University of California Office of the President
Keith Wessel, University of Illinois at Urbana-Champaign
Before

Many Managed Accounts

Multiple ID’s

ID #1

ID #2

After

Destinations

One Home Account

Single ID

InCommon VERIFIED

InCommon VERIFIED

InCommon VERIFIED

InCommon VERIFIED
Overview

- It’s your IdP
  - You control the configuration
  - Understand the impact of your configuration decisions
- If you want to be able to interoperate with the widest variety/common denominator of partners, here’s what you want to do with them
What’s a good federated citizen?

- For IDPs
  - Support for commonly-used security profiles
  - Implementation of federation best practices
  - Don't publish or support features that don't work as specified!
- For SPs
  - Standard interactions with IDPs
  - Good federated error handling
  - Appropriate session handling
  - Use SAML2
- For Organizations
  - Push vendors to join InCommon
  - Publish a POP and keep it up to date
Poll - Who are you? (with results)

- I operate my institution’s IdP: 49
- I operate one SP: 10
- I operate multiple SPs: 20
- Other: 15

From the chat, “other” included:
- those who operate multiple IdPs
- those who operate Shib and CAS IdPs
What’s in it for me?

- Easier, faster integrations
- Services and sessions behaving as expected
- Better user experience
Impacts of Federation (App View)

“Traditional” Application Responsibilities
Impacts of Federation (App View)

Application Responsibilities (With Federation)
SSO considerations

- Session lifetime
  - Short sessions make SSO less useful (or at least less single)
  - Long sessions change user authentication into device authentication
- No matter which way you go, make sure you understand the implications
- Consider user education for SSO
- Support kiosk settings for IdP's
Poll – SSO Session Length (with results)

- No single sign-on support (always force password entry): 1
- SSO lasts 20 minutes or less: 1
- SSO lasts more than 30 minutes up to 120 minutes: 24
- SSO lasts more than 2 hours and up to 7 hours: 18
- SSO lasts more than 7 hours and up to 1 day: 15
- SSO lasts longer than 1 day: 2
- We have custom/mixed SSO session lengths: 1

From the chat:
- 7 hours was due to SharePoint logging people out and mitigating user login fatigue via ADFS bridge
- “no SSO sessions” result of just beginning Shib rollout
Session Initiation

- Forced Re-authentication
- Passive Authentication
- Lazy Sessions
Forced re-authentication

- Allows requesting user re-authenticate
  - For “higher sensitivity” apps
  - If account is suspect
  - Required for audit purposes in some circumstances
- Breaks SSO experience
- IdPs: Support this!
  - But make sure you actually re-authenticate the user
- SPs: Don't abuse this!
  - But make sure you verify the re-auth happened if you ask for it
Forced re-authentication

- Be prepared to handle SAML errors
- More discussion (InCommon)
  - https://spaces.internet2.edu/x/doS8Ag
- Shibboleth Documentation
  - https://wiki.shibboleth.net/confluence/x/SIBC
  - https://wiki.shibboleth.net/confluence/x/doFC
  - https://wiki.shibboleth.net/confluence/x/zIBC
Poll – Forced re-authentication

- **IdP Operators**
  - Support forced re-authentication: 15
  - Do not support forced re-authentication: 13
  - Not sure if we support re-authentication: 24

- **SP Operators**
  - Currently invoke forced re-authentication: 3
  - Plan to/would use re-authentication: 8
  - No plans to use forced re-authentication: 5
Passive authentication

- Requires UI (i.e., login prompt) *not be* invoked at IdP
- Allows authenticated users without requiring login
- Requires SP/DS to know or guess user’s IdP
- As with Forced Re-authentication, can fail
- Prepare to deal with SAML Errors
- Docs: [https://wiki.shibboleth.net/confluence/x/hYFC](https://wiki.shibboleth.net/confluence/x/hYFC)
Poll – Passive authentication

- IdP operator
  - Support isPassive: 8
  - Do not support isPassive: 8
  - Not sure if we support isPassive: 33
- SP operator
  - Invoke isPassive today: 1
  - Have future plans for isPassive: 1
  - No plans for isPassive: 7
- From chat:
  - use cases for passive: allows for “autologin” to services
  - our Moodle instance uses it to work around a database issue
  - google apps uses passive auth
Lazy session support

- Allows anonymous access to pages
- Users can initiate authentication, but requires explicit action
- Commonly seen in public wikis and similar sites
- Docs: [https://wiki.shibboleth.net/confluence/x/bYFC](https://wiki.shibboleth.net/confluence/x/bYFC)
- Note potential confusion:
  - Lazy sessions are also called “Passive Sessions”
  - “isPassive” (previous topic) is passive Authentication check
Logout

- Support SLO endpoints!
  - SPs should call IdP's SLO URL if published
  - When possible, allow the SLO profile to return control to the SP to display a logout page
  - Though it’s not perfect, IDP logout works best when all IDPs support it and all SPs use it
- Not the same as a IdP “logout URL”
  - SPs won’t automatically use a logout URL.
  - If not in metadata, SPs won’t even know about it.
Logout

- Closing browser doesn’t always work any more
- Forced re-authentication is not a replacement for IDP logout
- We’re not advocating for federation-wide single logout

- Currently InCommon Metadata lists 29 SLO IdP endpoints
  - See metrics at: [https://spaces.internet2.edu/x/W4DYAg](https://spaces.internet2.edu/x/W4DYAg)
Poll – Logout

- IdP operator
  - Support SLO endpoint: 7
  - Do not have SLO endpoint because shib support too new: 26
  - No SLO endpoint – think it is a bad idea: 3
  - Not sure if we support SLO endpoints: 17

- SP operator
  - We invoke SLO endpoints when available: 2
  - Prefer SLO control return to the SP when complete: 0
  - Do not invoke SLO endpoints when available: 8
A note on back channel protocols

- Used for Artifact Resolution, Attribute Query and SOAP Logout
- Commonly used in SAML1, much less common in SAML2
- Think twice then think again before enabling back channel profiles
  - Verify functionality if you’re going to list endpoints!
A note on back channel protocols

- Current advertising:
  - 556 ArtifactResolutionService endpoints in IdP metadata
  - 477 AttributeService endpoints in IdP metadata
  - (From https://spaces.internet2.edu/x/W4DYAg)
- Look for alternate port support (usually 8443) to identify
- More perspective (from InCommon):
  - https://spaces.internet2.edu/x/4YHYAg
Poll – Back channel protocols

- **IdP operator**
  - We have use cases requiring broad back-channel support: 3
  - We support back channel because of SAML1 SPs: 13
  - We do not support back-channel protocols: 18

- **SP operator**
  - We have use cases requiring broad back-channel support: 2
  - We do not use back channel even if supported: 7
Federation Challenge: Scaling to the “Long Tail”
Attribute release

- Consider the “long tail” of federation when crafting your default attribute release policy (https://spaces.internet2.edu/x/zo6KAQ)
- Support the Research and Scholarship category to enable access to collaborative services for researchers and scholars (https://spaces.internet2.edu/x/-IKVAQ)
- Don’t strand the user due to attribute release problems
  - Always return the user to the SP to handle errors (https://spaces.internet2.edu/x/x4HYAg)
Poll – Attribute release (Poll)

- We release some attributes to all InCommon SPs: 27
- We only release attributes to specific SPs: 24
  - Note, those supporting “R&S” were listed here
- UI control is returned to supported SPs: 1
- Unsupported SP requests generate error at IdP: 7
User experience and metadata

- Publish user interface elements in metadata for consistency across IdP-SP ([https://spaces.internet2.edu/x/2YGKAQ](https://spaces.internet2.edu/x/2YGKAQ))
- Incident response: publish a security contact, use it when reporting security incidents to partners ([https://spaces.internet2.edu/x/8o6KAQ](https://spaces интернет2.edu/x/8o6KAQ))
- Error handling: IDPs publish an error URL, SPs use it ([https://spaces.internet2.edu/x/xa6KAQ](https://spaces интернет2.edu/x/xa6KAQ))
- InCommon stats:
  - IdPs with NO errorURL: 232
  - IdPs with errorURL: 122 (12 probed unsuccessfully)
Things to come

- Don’t expect universal support of these things yet
- Multi-factor authentication with a standard authentication context
- User consent (e.g., uApprove)
  - Especially useful for addressing FERPA concerns
  - LARPP: https://spaces.internet2.edu/x/RILYAg
- Multi-Context support
Acknowledgements

- People who provided behind-the-scenes input into the topics (but should not be blamed for any faults in the presentation!)
  - Tom Scavo, InCommon
  - Scott Cantor, OSU
  - Scott Koranda, UWM/LIGO
Conclusion and questions
Evaluation

Please complete the evaluation of today’s webinar

Call for Proposals Deadline This Friday, May 30

Identity Week 2014 will take place at the Technology Exchange

Advance CAMP, CAMP, Trust and Identity

October 26-30, 2014 - Indianapolis, Indiana

http://events.internet2.edu/2014/technology-exchange/
InCommon Shibboleth Installation Workshops
Single Sign-on and Federating Software

July 24-25 – Indiana University – Indianapolis, IN

September 29-30 – New Jersey Institute of Technology – Newark NJ

November 10-11 – University of Utah – Salt Lake City

Details and registration at www.incommon.org/shibtraining