The Multi-Context Broker Model

David Walker, Internet2

History

- 2012
  - Identified need to enhance Shibboleth to support InCommon Silver and Bronze.
- 2013
  - Requirements document written and RFP issued
  - MCB implementation begins for Shib IdPv2
  - Funding split between InCommon Assurance Program and Scalable Privacy Project (for MFA)
- 2014
  - MCB implementation complete in February, 2014
  - Shib IdPv3 release in late 2014
- 2015
  - MCB team refocuses on documenting the MCB Model for IdPv3

Definition: Authentication Context

- What an IdP tells an SP about an authentication event and what led up to it
  - May include identity proofing, registration, Authentication Method, operational practices, *etc*.
- Establish common standards, potentially federation-wide
- A Context can *satisfy* another Context
- Examples
  - A specific type of Authentication Method (*e.g.*, Password, X.509, or MFA)
  - An assurance profile (*e.g.*, InCommon Bronze or Silver

More Definitions

- **Authentication Method.** A software module that authenticates a user using a specific authentication service
- **User Certification.** An Authentication Context that may be asserted for a particular user

InCommon

What a Multi-Context Broker Does

1. SP requests an Authentication Context
2. IdP/MCB considers...
   a. the SP's request
   b. the User's Certifications
   c. other contexts that can satisfy the requested context
3. IdP selects a context that satisfies all criteria
4. IdP invokes an Authentication Method, if needed
5. IdP asserts the requested Authentication Context (or returns an error)

Mapping MCB Concepts to IdPv3

- Authentication Context = type of Principal
- Authentication Method = Authentication Flow
- User Certifications
  - Multi-valued attribute containing the Authentication Contexts that can be asserted for each user
  - Retrieved from IdMS using the Shibboleth attribute resolver
- Authentication Contexts can be configured to satisfy the requirements of other Contexts

Current Status

- IdP v3.1 is in production and it is capable of supporting MCB functionality.
- IdP v3.2 will be released soon with better examples and templates for creating MCB-like Authentication Flows.
- Draft documentation is available and will be completed shortly after the release of v3.2.
- Support for IdP v2 (and the MCB software) is going away...

References

- *The Multi-Context Broker Model*
  - https://spaces.internet2.edu/x/kY5HBQ
- *Configuring the Multi-Context Broker Model in Shibboleth IdPv3*
  - https://wiki.shibboleth.net/confluence/x/sIA9AQ
- David Langenberg's *Replicating Multi-Context Broker Functionality (Duo + Username/Password with user-opt-in forcing Duo)*
  - https://wiki.shibboleth.net/confluence/x/lYA9AQ