The Multi-Context Broker

David Walker
David Langenberg

Multi-Context Broker (MCB)

- Project to enhance Shibboleth's ability to orchestrate among multiple authentication contexts, including those requiring multi-factor authentication
- Initiated to address needs identified by CILogon, the National Institutions of Health, the Department of Education, and others

What Are We Trying to Accomplish?

- Authentication method (including multi-factor) based on SP requests
- Authentication method based on user certifications and restrictions
- Assurance profiles based on SP and user
- Assurance profile hierarchies
- Prioritized requests for multiple authentication contexts

Authentication Context

- An Authentication Method plus any other relevant criteria for an assertion
- Configuration
  - Authentication Method
  - Other Contexts satisfied by this Context
  - Well-known name
  - (“Other relevant criteria” represented in user records)

Example: AuthN Method by SP

- Two Authentication Contexts
  - **PasswordContext** with username/password authN method
  - **MFAContext** with multi-factor authN method
- SPs requiring PKI request **MFAContext**.
- SPs requiring username/password request **PasswordContext**
- Users are presented with the authentication method that matches the requested Context

User Certifications and Restrictions

- “Other relevant criteria”
- IdMS has multi-valued attribute holding list of Contexts that user can authenticate to.
- Contexts that can be asserted for a user are the listed Contexts, plus any satisfied by those listed.

Example: AuthN Method by User

- Two Authentication Contexts
  - **PasswordContext** with username/password authN method
  - **MFAContext** with multi-factor authN method
    - **MFAContext** satisfies **PasswordContext**
- Most users given **PasswordContext**
- Users *allowed* to use PKI given **MFAContext** and **PasswordContext**
  - They may be presented with a choice of authentication methods
- Users *required* to use PKI (perhaps by their choice) are given only **MFAContext**

Example: InCommon Bronze and Silver 1

- Two Authentication Contexts
  - **BronzeContext** with username/password authN method
  - **SilverContext** with username/password authN method
    - **SilverContext** satisfies **BronzeContext**
- Users are certified for **BronzeContext** and/or **SilverContext**, based on identity proofing, registration, *etc*. This is stored in the IdMS.
- Users authenticate once per session

Example: InCommon Bronze and Silver 2

- Two Authentication Contexts
  - **BronzeContext** with username/password authN method
  - **SilverContext** with multi-factor authN method
    - **SilverContext** satisfies **BronzeContext**
- Users are certified for **BronzeContext** and/or **SilverContext**, based on identity proofing, registration, *etc*. These are stored in the IdMS.
- Users who have authenticated for **BronzeContext** will need to reauthenticate (with multi-factor) for **SilverContext**, but not the converse

More Information

- Assurance Enhancements for the Shibboleth Identity Provider
  - https://spaces.internet2.edu/download/attachments/37650957/AssuranceReqShibIdP-19Apr2013.pdf
- Project Status
  - Currently doing acceptance testing and correcting bugs
  - https://spaces.internet2.edu/x/LgFtAg

Demonstration

Questions? Comments?