The Multi-Context Broker Model

The Multi-Context Broker Model is a useful way to think about the Shibboleth IdP's orchestration among multiple authentication methods in support of multifactor authentication, as well as multiple authentication contexts and assurance profiles. This document is a brief tutorial about the MCB Model and how it can be used. Recipes for configuring the MCB Model in IdPv3 are available from Orchestrating Multiple Authentication Methods and Contexts - The Multi-Context Broker (MCB).

A Couple of Short Stories

Dick and the Two Factors

Dick's campus Identity Provider (IdP) supports two forms of authentication, one requires Dick to enter a user name and password, and the other also requires Dick to prove he is in possession of his cell phone. Some Service Providers (SP) require user name and password, and some also require the cell phone. The campus has decided, however, that the cell phone method can always be used, even when only user name and password is requested by the SP. When Dick browses to an SP requiring user name and password, he is prompted accordingly, and he is no longer prompted for the rest of his session, unless he browses to an SP requiring the cell phone method. In that case, his cell phone alerts him for confirmation, and he then is no longer prompted for any SP during the rest of his session.

In order to provide Dick with choices to protect his online identity, Dick's campus allows him to opt out of ever authenticating without using the cell phone method. After choosing that option, he is always prompted to use the cell phone method, even when it is not required by the services he uses.

Assuring Jane

Jane uses her web browser to access a Service Provider (SP) that requires the InCommon Bronze assurance profile. The SP redirects her to her campus Identity Provider (IdP), the MCB verifies she is certified for the Bronze profile, and she is presented with a list of authentication methods it provides that will satisfy the requirements of InCommon Bronze. Jane chooses one of those methods and authenticates. Jane's IdP returns the Bronze assurance qualifier to the SP. As Jane browses to other Bronze SPs during her current session, her IdP provides the Bronze assurance qualifier to those SPs without requiring additional interaction for authentication.

During her session, Jane browses to a Service Provider that requires the InCommon Silver assurance profile. At Jane's campus, the Silver assurance profile requires a different authentication method than Bronze, so (after verification that Jane is certified for the Silver profile) Jane is prompted for Silver authentication.

This is only a little of what the Multi-Context Broker Model can do. For example, if the first SP Jane used required the Silver profile, she would not be prompted to authenticate for later Bronze SPs during the current session, as the Silver profile satisfies all the requirements of the Bronze profile. We'll have to dive a little deeper, though, to describe this.

Defining Some Terms

- **Authentication Method.** A method for authenticating the identity of the current user. Examples are username/password, X.509 client certificates, one-time password devices, *etc*. In the context of the MCB and Shibboleth, this is a specific instance of such a method. For example, the UC Irvine's UCInetID system (which is based on Kerberos software) is an Authentication Method, whereas the generic Kerberos software is not. (In this document, "Authentication Method" is often shortened to "Method" for brevity.)
- **Authentication Context.** The context of the authentication event that results in a SAML assertion sent from the IdP to an SP. Authentication Context is comprised of an Authentication Method, plus any other relevant criteria, such as the identity proofing and registration processes used to issue credentials to the current user. In SAML, only the name of an Authentication Context is sent between IdPs and SPs; the Authentication Method and other criteria associated with that name are documented separately. It should be noted that it is often the case the multiple Authentication Contexts form a hierarchy, in the sense that one Authentication Context's criteria may satisfy the criteria of another Authentication Context. For example, InCommon Silver satisfies the criteria for InCommon Bronze. (In this document "Authentication Context" is often shortened to "Context" for brevity.)
- **Assurance Profile.** Criteria related to the trustworthiness of SAML assertions, such as InCommon Bronze and Silver. Assurance Profiles are represented in SAML as Authentication Contexts.

What Is the Multi-Context Broker Model?

The Multi-Context Broker Model helps to guide configuration of the Shibboleth IdP's ability to orchestrate among multiple Authentication Contexts, including those requiring multifactor authentication. To do this, it considers information from multiple sources:

- The Authentication Contexts requested by a Service Provider (SP), in priority order,

- The Authentication Contexts that the current user is certified to use, stored in the Identity Management System, and
- The hierarchy of Authentication Contexts, representing where one context satisfies the requirements of another.

When the MCB receives a request from an SP:

1. It compares the SPs requested Authentication Contexts against the Contexts the user is certified to use *plus* any Contexts that are satisfied by the user's certified Contexts to determine the feasible Contexts that can be used for this transaction.
2. The IdP selects one of the feasible Contexts and authenticates according to that Context's Authentication Method. Upon successful authentication, the IdP returns the SP-requested Authentication Context that has been satisfied. (Note, the IdP maintains session state to enable single sign-on. Once the user has authenticated with a particular Authentication Method, that Method will not require further user interaction for the rest of the session, unless the SAML "force authentication" option is specified.)

Note that the process described above assumes knowledge of the identity of the current user. When the current user is not already known to the MCB (*i.e.*, this is the start of a new session), the IdP can present the user with a configured Authentication Method to determine their identity, then the process described above is invoked.

Example Uses for the Multi-Context Broker

This section briefly describes a few potential uses for the Multi-Context Broker, indicating what would need to be configured to implement them. For detailed configuration information, please see Orchestrating Multiple Authentication Methods and Contexts - The Multi-Context Broker (MCB).

Authentication Method Selected by SP Request

Users are presented with the authentication method, either password or multifactor, that matches the requested Context. All users can use either method.

- Two Authentication Contexts
  - **PasswordContext** with some username/password Authentication Method
  - **MFAContext** with some multifactor Authentication Method
- All users are given **PasswordContext** and **MFAContext.**
- SPs requiring MFA request **MFAContext.**
- SPs requiring username/password request **PasswordContext**

Authentication Method Selected by Relying Party Configuration for SP

If an SP does **not** explicitly specify a RequestedAuthnContext, then a default can be identified in relying party configuration. If that default is for **MFAContext**, then that would have the same effect as the SP requesting **MFAContext.** See Configuring the IdP for the Multi-Context Broker Model for more information.

Authentication Method Selected by User Certification

Authentication methods are controlled within the IdMS. SPs request **PasswordContext** (or do not request an Authentication Context). Users are prompted for username/password or MFA, depending on their certifications within the IdMS. This is a method for requiring certain users to use MFA, or for providing "user opt-in" similar to that provided by Google and other cloud providers.

- Two Authentication Contexts
  - **PasswordContext** with some username/password Authentication Method
  - **MFAContext** with some multifactor Authentication Method
  - **MFAContext** satisfies **PasswordContext**
- Most users given **PasswordContext**
- Users allowed to use MFA given **MFAContext** and **PasswordContext**
  - They may be presented with a choice of authentication methods
- Users required to use MFA are given only **MFAContext**

InCommon Bronze and Silver with One Authentication Method

InCommon Bronze and Silver share a common username/password authentication method. Users authenticate once per session with the single Authentication Method, and SPs receive the requested Context (or failure), based on user certifications.

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

InCommon Bronze and Silver with Two Authentication Methods

There are two authentication methods, one for Bronze, and one for Silver. Users who have previously authenticated for **BronzeContext** will need to re-authenticate for a subsequent **SilverContext** request, but users who have previously authenticated for **SilverContext** will not need to re-authenticate for a subsequent **BronzeContext** request.

- Two Authentication Contexts
  - **BronzeContext** with some username/password Authentication Method
  - **SilverContext** with some other Authentication Method
  - **SilverContext** satisfies **BronzeContext**
- Users are certified for **BronzeContext** and/or **SilverContext**, based on identity proofing, registration, etc. These are stored in the IdMS.

InCommon Bronze and Silver with Two Authentication Methods, Silver Requiring a Second Factor

> **Second Factor Only Technologies**
>
> Second factor only technologies like U2F and Duo are not full-fledged Authentication Methods, as described in this document. The MCB Model, and IdPv3, consider an Authentication Method as something that tells you who the current user is. Second factor only technologies do not do this; you tell them who you think the current user is, and they tell you if they agree with that (increasing your confidence in who the current user is).
>
> For this reason, the user must have been authenticated with a first factor before a second factor method can succeed. For now, this requires configuration of an initial authentication method, as described in Configuring the IdP for the Multi-Context Broker Model and/or custom authentication flow scripting. The Shibboleth community, however, is working to enhance IdPv3's ability to accommodate second factor only technologies.

There are two authentication methods, one for Bronze, and one for Silver. All users are required to authenticate for **BronzeContext** at the beginning of their session with the IdP. Users will need to provide their second factor for a subsequent **SilverContext** request, but they will not need to re-authenticate for a subsequent **BronzeContext** request.

- Two Authentication Contexts
  - **BronzeContext** with some username/password Authentication Method
  - **SilverContext** with some second factor only Authentication Method
  - **SilverContext** satisfies **BronzeContext**
- Users are certified for **BronzeContext** and/or **SilverContext**, based on identity proofing, registration, etc. These are stored in the IdMS.
- **BronzeContext**'s Authentication Method is configured as the initial authentication context.

Sample Configurations

- David Langenberg's Replicating Multi-Context Broker Functionality (Duo + Username/Password with user-opt-in forcing Duo) for InCommon Silver and Duo Security MFA

How Do I Configure the IdP for the Multi-Context Broker Model?

- Configuring the IdP for the Multi-Context Broker Model provides recipes for configuring the MCB Model.
- Please ask questions and report bugs to users@shibboleth.net.

History of the Multi-Context Broker

During 2012, the InCommon Assurance Program explored implementation issues of assurance, most notably with CILogon, National Institutions of Health and the Department of Education. The latter two organizations are required to follow the Federal Identity Credential and Access Management committee's SAML2 Web SSO Profile for requesting Authentication Contexts (*e.g.*, assurance profiles). CILogon, run by NCSA, has more flexibility in its requirements.

While testing, campus implementers identified the following issues, as of version 2.4 of the Shibboleth IdP:

- If a user used her password to log in as a Bronze authnContext, she had to use the same password to re-login for Silver. Shibboleth does not know that the same authentication method is used for both Bronze and Silver, forcing re-authentication, even when a previous context's authentication would suffice.
- If a user logs in with his password, accesses a Silver-service, but has forgotten his hardware token required to assert the Silver Authentication Context, he cannot decide to accept a lower level of service by telling the IdP to go ahead and assert Bronze on his behalf. The login handler doesn't support such multifactor use cases well.
- If an SP passed a list of Authentication Contexts (*e.g.*, [Silver, Bronze, unspecified]) with the intent of having the IdP provide the highest possible Context for the user, the IdP would not process the list in a prioritized fashion, resulting in a Bronze Context sent one time, Silver another, and unspecified as well.

In January of 2013, InCommon convened a group section to share their testing experiences to date and assist in the development of a requirements document for an initial set of enhancements to the Shibboleth IdP to address these issues that could be 1) delivered to the Shibboleth Consortium for consideration in future IdP release and 2) used as a basis for an RFP, jointly funded by InCommon and the NSTIC-funded Scalable Privacy Project, to develop a short term solution for campuses interested in implementing assurance over-the-wire.

In summary, the testing group saw two primary SP use cases:

- The SP requests a specific Authentication Context, like Silver.
- The SP requests one of a set of Authentication Contexts, in priority order (*e.g.*, [Silver, Bronze]), that are required for different levels of service. The IdP presents a choice of authentication methods that will satisfy the request and for which the user is eligible, and returns the selected Context to the SP upon successful authentication. The SP then tailors the service provided accordingly.

In addition, the diversity in hIgher education IdP implementations and the supporting identity management and authentication systems, suggests a certain level of configurability and flexibility in how the Shibboleth IdP supports the bullets above. To support the Silver Identity Assurance profile, an organization may determine that bringing its password infrastructure into compliance is a viable option, where another may layer on a multifactor solution and bypass the complexity and scope of the current password infrastructure. The solution must be able to manage the use of multiple authentication systems, contexts in which they are required, and the user's ability to control their authentication method when multiple options exist.

Under the guidance of Ann West and David Walker, the RFP was issued in July, 2013, based on the specifications in Assurance Enhancements for the Shibboleth Identity Provider (19 April 2013), was awarded to Paul Hethmon, and implementation began. Acceptance testing for the MCB completed in January, 2014, and the MCB was released in February, 2014. The acceptance testers were David Langenberg of the University of Chicago, Keith Wessel of the University of Illinois, and Mike Wiseman of the University of Toronto.

With the release of IdP Version 3 in late 2014, the MCB team's focus shifted form software development to documenting the MCB Model and how it can be configured in IdPv3.