Protocol Signaling for WorkDay MFA Use Cases

While signaling is out of scope for this work group, an understanding of how signaling occurs when the SAML protocol used by InCommon can help understanding of how an MFA profile will be used. For each of the following use cases, we describe how they would be (or would not be) addressed in the Multi-Context Broker (MCB) Model for the behavior of an IdP when multiple authentication methods are available.

- Risk based on the initial authentication
- SP initial request – All users for the SP/IDP combination need to be MFA
- IDP rule based – Logic in the IDM/IDP side know that the user should be stepping up authentication
- SP follow up request – User authenticated with single-factor, but now needs MFA

Risk based on the initial authentication

The MCB Model assumes that each user is certified for specific authentication contexts, and each authentication context has an associated authentication method. Those certifications are stored in the IAM. This mechanism can be used to require, for example, that certain users must use MFA. More complex risk assessment strategies, however, would require custom code, although that code could, in many cases, be implemented as a "scripted attribute," so that the IdP can use continue to use the same mechanism. **(Out of scope for the MFA Interoperability Profile.)**

SP initial request – All users for the SP/IDP combination need to be MFA

This is a direct application of our MFA profile. The SP requests the MFA profile as an authentication context, and the IdP invokes whatever specific authentication method it has associated with that profile. The SP is signaled in the response as to whether the request was successful. **(In scope for the MFA Interoperability Profile.)**

IDP rule based – Logic in the IDM/IDP side know that the user should be stepping up authentication

Assuming this use case is needed when the SP does not request an authentication context, then the MCB Model allows for the specification of a default context to be used for that SP. If the intent is to override an SP's request, then custom code would be required. It may also requiring violating the specification of the SP's requested context, so is not recommended. **(Out of scope for the MFA Interoperability Profile.)**

SP follow up request – User authenticated with single-factor, but now needs MFA

From the IdP's point of view, this is the same as SP initial request above. The SP requested the MFA profile at the time it is needed, essentially creating another session with the IdP, and the IdP responds accordingly. **(In scope for the MFA Interoperability Profile.)**