A note from the editors of REFEDS MFA Profile V1.1:

To the MFA Profile reviewers,

First, thank you for taking the time to review and provide feedback for the latest revision to the REFEDS MFA Profile.

The original REFEDS Multi-Factor Authentication (MFA) Profile was published in June 2017. Since its publication, the R&E community has provided a lot of valuable feedback on how the Profile should evolve to facilitate even wider adoption. Some of them were captured in an updated FAQ.

This Profile update continues our effort to make the REFEDS MFA Profile clearer and easier to adopt. With V1.1, we focused on clarifying key implementation details and making the Profile usable with multiple messaging protocols (SAML and OIDC), while staying true to the intent of the original Profile. Along the way, we encountered issues that needed to be addressed, but fell outside the scope of this update. This document captures those issues. Where applicable, we also include recommendations for future actions.

Now we need your help: we need you to give us feedback on whether this is the direction you'd like to see the REFEDS MFA Profile evolve. Tell us how well this Profile update reflects your expectation on the profile.

Read the draft Profile document first. As you review that document, use this document as a companion guide. It should provide some insight into our discussions and rationale for including (or not) certain elements in this update.

Thank you again. We look forward to hearing from you.

Best regards,

The Profile editors / REFEDS MFA Profile Subgroup

Content

Under Section 1. Introduction

Relationship to institution-specific MFA signalling needs

We included this paragraph to clarify when it is (and isn't) appropriate to use the identifier defined in this Profile to signal MFA. This will likely need additional explanation in an accompanying FAQ.

Under Section 3. Profile Identifier

Version Numbering for this Update

The MFA Profile editors group (Editors) has chosen Version 1.1 as a tentative version number of this Update. This is a controversial and potentially confusing choice. The primary goal of this update is to clarify the intent of the original REFEDS MFA Profile to make implementation more consistent. In doing so, we have introduced details (e.g., 4.3 Validity

Lifetime) that could be interpreted as breaking changes: a current implementation of REFEDS MFA Profile may not satisfy the requirements laid out in this Update.

Normally, a breaking change like this would call for a new identifier to be defined. It would also require incrementing the Profile's major version number. However, given we are still relatively early in this Profile's adoption, and that we had a constraint to not modify the Profile identifier in this update, we felt it was reasonable, this time only, to reuse the same identifier.

The decision to reuse the existing profile string may require extra work for Federation operators and SPs, because the Profile doesn't provide a way for peers to know which version of the REFEDS MFA Profile the IdP is asserting compliance with.

E.g., Fed Operators may need to add an "attestation" process for IdPs to confirm they are complying with the updated version of the Profile (perhaps beyond a certain date).

Ongoing Profile Maintenance and Versioning

Given the rapid changes in the authentication space, we anticipate this Profile will require more frequent attention to ensure it maintains pace with technology changes, evolving threat vectors, and community's need for strong authentication. The Editors recommend establishing a regular review cycle to update the Profiles as needed. Going forward, the Editors recommend following a versioning scheme where breaking changes - like those included in this update - are clearly signalled by incrementing the Profile's major version number.

Under Section 4. Authentication Requirements

4.2 Factor Independence

We received this comment from an early reviewer:

> *This [the requirement for factor independence] is stated as an absolute, yet perfection is often hard to achieve. Is it reasonable to permit a "good" if not perfect mitigation to protect one factor from accessing the other?*

Given that one of the main complaints we were responding to is that the Profile is unclear on how deployers should go about meeting its requirements, we chose to leave the more "absolute" description of the requirement in place.

The editors also considered adding further language around requirements for recovering/resetting individual factors. After much discussion, we concluded that dictating constraints on deployments may unrealistically limit implementations. We thus leave such topics to supporting documentation.

4.3 Validity Lifetime

Note that this section establishes a maximum session length for both the IdP authentication sessions overall and for factor-related sessions such as Duo "Remember Me" option. This is one of the more notable "breaking changes" introduced in this revision.

Under Section 5. Protocol Specific Bindings

5.1.2 and 5.1.3.3 SAML 2.0 Binding - AuthnInstant and ForceAuthn

A question that comes up frequently in reference to the REFEDS MFA profile is how to respond to "ForceAuthn" - which is a request to *"authenticate the presenter directly rather than rely on a previous security context" and to "require explicit user interaction during authentication to the identity provider"* (to quote SAML standards material) - when the authentication process involves two completely independent factors. This question often arises around the use of the Duo product (which is pervasively deployed in higher ed) and its "Remember Me" option.

There are two questions that arise when using Duo:

1) Does relying on Duo's "Remember Me" session constitute "authenticating the presenter directly".
2) Regardless of the answer to #1, How would an IdP signal that "all factors were recently re-authenticated"?
    a) Because users can generally initiate unsolicited assertions at the IdP, an SP's ForceAuthn signal can frequently be bypassed. This usually requires SPs to inspect the IdPs assertion to determine whether all factors were authenticated (in case the ForceAuthn signal was bypassed).
    b) The only information in a standard IdP's assertion that conveys "time of authentication" information is the AuthnInstant, and that is single valued.

The Editors discussed three potential options for how IdPs should be required to respond to ForceAuthn:

1. Leave the behaviour unaddressed. (This is the approach of the current profile).
2. Define that "AuthnInstant" when presented in combination with an asserted REFEDS MFA authncontext MUST indicate the time of the *oldest* authentication challenge across all factors.
    a. This would allow an SP to inspect the Assertion from an IdP and determine whether or not each factor had been authenticated against sufficiently recently.
3. Define that "AuthnInstant" can reference the authentication time of any single authentication challenge.

126 a. In this case, ForceAuthn cannot be relied upon to directly invoke all
127 authentication factors (e.g., in the Duo case, "Remember Me" may be used
128 for the Duo portion of the authentication), though it can be used

129 The Editors chose option 3. This was mostly chosen because it's the easiest option for an
130 IdP Operator to implement, but also because of the divergent community opinions around
131 the validity of Duo's "Remember Me" token as a "direct authentication" action. The language
132 in the Profile is written to be a more general requirement, but the Duo use case is what
133 primarily motivated the discussion.

134 Note also, the requirements in section 4.3 define a time limit for how long authentication
135 challenges (including "Remember Me") meet the profile requirements.

136 5.2 OIDC 1.0 Binding

137 The OIDC 1.0 Binding section is brand new to this Profile. There remains a number of
138 outstanding questions to be addressed. We have and are actively seeking input from OIDC
139 experts to help with that effort. Example questions include:

140 - Implications and usage of the `max_age` request parameter.
141 - Use of the `acr_values` request parameter, which acts as a non-essential claims
142 request (i.e., does not strictly require use of MFA).

143 Additional Observations

144 Strong Authentication vs "MFA"

145 The Editors note that while this Profile specifically references "multi-factor authentication",
146 the real intention behind the Profile is to signal the need for "stronger authentication". While
147 signing in with multiple factors is one way to achieve stronger authentication than
148 passwords, alternate "single factor" techniques exist to achieve equivalent strength. The
149 community may wish to reconsider the choice to solely use "MFA" to characterise "strong
150 authentication" in future revisions of this Profile.

151 Expressing QoA via AuthnContext

152 It may be worthwhile to produce separate resource/material to expand on the notion of
153 "Quality of Authentication": explain what it is, why conveying "QoA" is preferable to
154 expressing "method of authentication", particularly since improving "QoA" is the foundational
155 premise of this Profile.

156 In earlier drafts of this revision, we included this text describing how the "REFEDS MFA"
157 profile differs in intent from the originally defined SAML authentication contexts. This info
158 didn't seem directly pertinent to the requirements in the profile, but is perhaps useful in
159 evaluating some of the decisions proposed in the original and updated profiles.

160 ***Why is this relevant/important?***

When SAML was developed, it was imagined that referring to precise details of authentication methods - such as specifying whether a SmartCard was used as part of user authentication - was a sensible approach and the original context class reference URIs defined in the standard reflect this thinking.

As time went on, it became clear this was too difficult to manage for ongoing use. It became more common to use general "categories" of authentication - such as "an MFA challenge was part of the authentication" - that would be more stable over time.

The REFEDS MFA Profile is an example of such a general category.

Error Handling discussions

During the Profile update, the Editors debated at length whether to include error handling instructions in the specification.

Our current position is that while error handling is an important topic, this detail should be captured in a supplemental implementation guide or FAQ. For example, the following are some general scenarios:

- RP/SP requests REFEDS MFA, OP/IdP doesn't understand it and tosses an HTTP 500 (bad? good?)
- RP/SP requests REFEDS MFA, OP/IdP doesn't understand it responds with a protocol-specific error (good? bad?)
- RP/SP requests REFEDS MFA, OP/IdP understands it but is unable to perform MFA, responds with a protocol-specific Error (good? bad?)
- What is the correct/expected behaviour for an IdP when responding to a request it does not / cannot support beyond what the standard addresses. And is there any difference expectation between SAML and OIDC IdP's responding to such errors.

SP requests REFEDS MFA, IdP understands it but is unable to perform MFA, responds with SAML Authn Assertion with something other than REFEDS MFA value (what happens?)

Earlier Working Material

The following links point to earlier discovery materials the Group compiled to organise/prioritise the Profile revision work.

MFA Profile Priorities - The REFEDS MFA Subgroup recommendations to update the REFEDS MFA Profile.

Working document for MFA Profile Priorities