Consultation: MFA Profile v1.2

Background

(From the Editor's Follow Up to REFEDS MFA Profile v1.1 Consultation and Next Steps)

The original consultation for the proposed REFEDS MFA Profile V1.1 resulted in a number of important pieces of feedback, largely centered around two issues:

- The changes made to the meaning of the original profile identifier, principally around recency of authentication.
- The explicit recommendation to avoid the ForceAuthn option in SAML, and equivalent constructs in OpenID Connect.

The Working Group held lengthy discussions and considered various alternatives. Ultimately, we recognised that to some degree, the world has begun to move beyond the notion of Multi-Factor Authentication. The future of strong authentication points to a wider variety of phishing-resistant authentication technologies that include some single-factor approaches. Therefore, we consider this revision of the REFEDS MFA Profile a transition stop toward future work. Instead of introducing radical changes, we are proposing a more conservative set of clarifying changes to the original profile.

Compared to the original proposal we submitted for consultation, this new version:

- Maintains the semantics of the original profile identifier while adding additional clarifications.
- Softens several changes proposed in the first consultation from MUST to SHOULD.
- Includes explicit recommendations on how IdPs and SPs should interpret the SAML and OpenID features for forced re-authentication and how the time of authentication should be set.

The latter are expressed as normative, but not mandatory requirements, in recognition of the fact that some existing implementations may not be able to meet them. The language in the SAML 2.0 and OIDC specifications around re-authentication is not clear enough to justify a claim that our interpretations are the only possible ones, but the recommendations in our view fit within the plain language of the specifications, and reflect the most useful behaviour we would seek to encourage to improve interoperability.

We therefore invite a new round of feedback to this revised, and we feel simpler and less ambitious, proposal. We believe the bulk of the feedback during the first consultation is addressed with these changes.

Overview

Results from the MFA Profile v1.1 are available for review here.

A PDF for the consultation is available, REFEDS-MFA-Profile-v1.2.pdf

All comments should be made on consultations@lists.refeds.org or added to the comment log below, comments posted to other channels will not be included in the consultation review

Change Log

<table>
<thead>
<tr>
<th>comment #</th>
<th>Line /Reference</th>
<th>Proposed Change or Query</th>
<th>Proposer / Affiliation</th>
<th>Action / Decision (please leave blank)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Section 4.2, lines 76-77</td>
<td>On the wiki page guiding IdP operators on REFEDS MFA (<a href="http://wiki.refeds.org/display/PRO/Guidance+for+Identity+Provider+Operators">http://wiki.refeds.org/display/PRO/Guidance+for+Identity+Provider+Operators</a>?), in the section named “An SP is requesting MFA for a user. My IdP supports MFA, but the user in question has not activated or enrolled in my MFA solution. How should the IdP behave?”; it says: “Your IdP might inform the user that the resource they are attempting to access requires MFA, and they should enroll in MFA before continuing. You could then optionally trigger MFA enrollment if you have a self-service online MFA enrollment mechanism.” Shall such initial self-registration of the second factor based solely on the first factor still be permitted under this new version of REFEDS MFA? Or is the proposed wording of the “Factor independence” section (lines 76-77) meant to imply that even an initial self-registration of the 2nd factor on a password-only account shall be precluded under the profile?</td>
<td>Mikkel Hald / WAYF.dk</td>
<td>Yes, it is still permitted. We have changed that paragraph to say “Initial enrollment of one or more additional factors MAY take place subject to authentication by only a single factor. Subsequently, the factors used MUST be independent; this includes processes to recover, replace, or add authentication factors.” to make this clear.</td>
</tr>
</tbody>
</table>
2 Section 1, lines 34-37 I think the text "strongly recommended not to use the value defined in this Profile to meet intra-organizational MFA request/response needs" is a little bit too strong. I would like to soften it with an "if not the same requirements are met" or something like that. Pål Axelsson / SWAMID Changed to "When using this Profile, one must strictly adhere to the semantics described in Section 4. This Profile is specifically designed for a service provider and an identity provider to signal multi-factor authentication behaviour in an inter-organisational single sign-on transaction. Using the value defined in this Profile to signal compliance with an organisation's internal policies carries risk. Even if the organisation's internal MFA policy aligns with the requirements of this Profile today, organisational policy could evolve over time and become incompatible with the requirements of this Profile. Conflicting MFA signalling governed by local policies with federated MFA signalling will likely impede an organisation's ability to conform to this Profile over time."

3 Section 5.2 Some of the sub sections within 5.2 are mis-labeled as 5.1.x Albert Wu / InCommon They are fixed now

4 26 Delete "It should be noted that". Filler phrase - adds no meaning. John Scullen / AAF The phrase has been removed now.

5 31 "This Profile is specifically applicable when" > This Profile specifically applies when John Scullen / AAF Updated.

6 39 Table uses lowercase for all terms except "Multi-factor authentication". Make consistent. Also the description for MFA says: "Multi-factor refers to ...". Recommend changing to "Multi-factor authentication refers to ..." John Scullen / AAF Fixed.

7 111 Random "cv" at the beginning of the sentence to be removed John Scullen / AAF Fixed.

8 120 shall not > SHALL NOT? John Scullen / AAF Fixed.

9 128 must > MUST John Scullen / AAF Changed to SHOULD.

10 134 must > MUST? John Scullen / AAF Changed to SHOULD.

11 113, 116, 239 and 248 I'd prefer to see the actual name used instead of "this value". eg. When the REFEDS MFA Profile is used (listed/presented) ... Need the editors to check this is the correct terminology here John Scullen / AAF We believe "this value" is clear enough as the value is defined in the immediate previous paragraph(s).

12 254 shall not > SHALL NOT John Scullen / AAF Fixed

13 262 must > MUST John Scullen / AAF Replaced by SHOULD

14 262 This is looking pretty good overall. Congratulations to the authors and editors for getting it this far John Scullen / AAF Thanks.

15 Many thanks from SWITCH for this MFA profile revision. We very welcome the many clarifications. We will be able to fulfill all requirements in the future, and the SHOULDs allow us to still be compliant in a transitional period. SWITCH intends to define a flag day in 9-12 months by when the REFEDS MFA deployment on SWITCH managed IdPs & OPs will meet the new clarified requirements currently not satisfied, like the earliest time of authentication. Thomas Lenggenhager / SWITCH Great.

16 Overall, I support the changes in the 1.2 - which I interpret as primarily:
- mandating that authnInstant must be the earliest time of the factors
- forceAuthn re-authenticates all factors (with suggestions for SPs to re-send user for authentication if authnInstant is too far in the past).

Vlad Mencik / Tuakiri /REANZ

Almost. The profile is now clear on that authnInstant SHOULD be updated to the earliest time of the factors, and that all factors SHOULD be re-authenticated on forceAuthn.

The wording is chosen to make the updated version backward compatible but still clear on what the intention of the profile should be.

17 One concern: I'm not sure reusing the same profile identifier with new semantics is the right way to go. This would mean SPs cannot be sure which version of the specification did the IdP issuing the assertion follow. Vlad Mencik / Tuakiri /REANZ

Updated. The 1.2 consultation version is made to not add new mandatory semantics and not include any breaking changes from the 1.0 version of the profile. All changes regarding requirements are advisory.

18 Second concern: I'm surprised the OIDC requirements for dealing with authentication instant and forced re-authentication in sections 5.2.2.1 and 5.2.2.2 are given as a SHOULD and not a MUST. (I also observe version 1.1 of the specification used a MUST in this part, though for different wording). Vlad Mencik / Tuakiri /REANZ

We have softened the OIDC section in line with the SAML section. Both are built on Section 4 in the profile which is softened compared to the 1.1 version of the draft.

19 157-159 typo: the compound sentence is missing a pronoun to refer to the attribute: I'd insert a "which": The SAML specification allows the Comparison XML Attribute in the <RequestedAuthnContext> element, >>> which when present, may be set to values other than the default value of "exact". Vlad Mencik / Tuakiri /REANZ

Fixed.

20 180-181 typo: change "return" to "returns"
that an IdP unable to satisfy the requirements expressed return >>> returns an error if it responds. Vlad Mencik / Tuakiri /REANZ

Fixed.
<table>
<thead>
<tr>
<th>Page</th>
<th>264, 274</th>
<th>Typo: Section numbers 5.1.2.2 and 5.1.2.3 should be 5.2.2.2 and 5.2.2.3 respectively.</th>
<th>Vlad Mencl / Tuakiri / REANNZ</th>
<th>They are fixed now.</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>57, 58</td>
<td>&quot;To qualify the user to access the organisation's critical internal systems.&quot; This sounds to me as exaggeration not suitable for a normative section. The profile is about authenticating to other organisations' systems and has nothing to do with the user's home organisation's critical internal systems.</td>
<td>Vlad Mencl / Tuakiri / REANNZ</td>
<td>Paragraph removed.</td>
</tr>
</tbody>
</table>