Consultation: MFA Profile v1.1

Overview

The REFEDS MFA Profile v1.1 update, proposed by the MFA Subgroup of the REFEDS Assurance Working Group, 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), whilst 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. These issues are captured in an Editors’ Notes for REFEDS MFA Profile v1.1 to help readers understand context and constraints of this profile. Where applicable, we also include recommendations for future actions. The Editor’s Note is for reference and not part of the consultation.

Prior to this public consultation a community chat was held. The Community Chat was recorded and slides from the presentation are available.

Background

The REFEDS Multi-Factor Authentication (MFA) Profile defines a standard signal that a service provider may send to request an IdP to perform MFA during federated authentication. The IdP sends the corresponding signal in its response to indicate that MFA had occurred. The Profile also defines the criteria that an IdP must meet in order to claim successful MFA using the REFEDS MFA Profile.

The REFEDS MFA Profile is currently primarily used within SAML authentication. Its use is largely patterned from the OASIS Authentication Context for SAML.

A PDF for the consultation is available, REFEDS-MFA-Profile-v1.1-draft.pdf
Read the Editors’ Note for REFEDS MFA Profile v1.1 for additional background.

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.

Comment Log

<table>
<thead>
<tr>
<th>comment #</th>
<th>Line /Reference #</th>
<th>Proposed Change or Query</th>
<th>Proposer / Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4.3 Validity Lifetime</td>
<td>Setting a hard limit on 12 hours isn’t logical. A IdP could use different vectors (location, device, behavior) to determine if mfa is needed, and prevent MFA-fatigue by only requesting MFA when needed. When specifying a time-limit, a period greater than 24 hours is more practical, to spread the login-times over the (working) day. Proposal: Allow a maximum window of 8 days</td>
<td>Peter Havekes / SURF</td>
</tr>
<tr>
<td>2</td>
<td>5.1.3.3 ForceAuthn</td>
<td>There are use cases where a user must always preform MFA authentication. Examples are: SP’s that require MFA on each login by policy • Use MFA authentication for signing a transaction, like entering a grade list ForceAuthn is very useful in these cases. Proposal: If both ForceAuth and an AuthnContextClassRef element containing the REFEDS MFA Profile are specified, the IdP MAY force the user to use his first factor, and MUST force the user to use his second factor.</td>
<td>Peter Havekes / SURF</td>
</tr>
<tr>
<td>3</td>
<td>Section 4.1, line 60-61</td>
<td>Redaction is a bit ambiguous. My reading of it is that it disallows using two factors of the same kind (i.e. two passwords of different providers, thus disallowing solutions like alternative e-mail OTP), but would allow authentications with a single step that ensures the conditions of more than one type (i.e. certificate authentication with a smartcard, which both entails having the card and knowing the card PIN). Proposal: add a “Guidance” section further developing which interpretations of the section are right, which are not, and which are close to the grey zone. Maybe also include practical examples?</td>
<td>Francisco Aragg / RedIRIS</td>
</tr>
</tbody>
</table>
Section 5.1.3.4

This section hints that if a SP requests refeds/mfa in the authnContextClassRef, and only this one (as recommended in section 5.1.3.1), if the IDP cannot satisfy conditions of section 4.1 in the authentication, it must return a failure state and never a successful response. Also, the profile does not specify how the SP should verify that the requirement has been met: by the presence of the refeds/mfa classref on the response or implicitly by the fact of the response being successful? If it's the second case, it renders the signalling of the refeds/mfa ClassRef on the response mostly superfluous; if it's the first case, the fact of forcing an error response (instead of allowing a response without the refeds/mfa classref signal) rules out the possibility to implement a proxy use case where the principal has different factors enrolled on the IDP (refeds/mfa compliant, can be accessed independently other than from the proxy) and on the proxy, and can choose between providing the second factor at the IDP (in which case the response will already be refeds/mfa compliant) or at the proxy (in which case, the IDP would have to fail for not being able to satisfy refeds/mfa context, as the IDP is standalone refeds mfa compliant). Proposal: state clearly if this is the expected behaviour (and that the exposed proxy scenario should not be supported), or otherwise clarify that not satisfying conditions of section 4.1 is not a cause for response failure, but only to NOT signal the refeds/mfa authnContextClassRef on the successful response, leaving the SP to check that the response did not fulfill the conditions and allow it to act accordingly.

Francisco Aragó / RedIRIS

Introduction, lines 31-37

The issue here is not really about intra- vs. inter-organizational MFA signalling, but rather about deviation from this profile. I suggest rewording to something like "Deployments of this Profile must adhere strictly to its requirements and cannot override them with local policy requirements. Because this Profile cannot anticipate unique organisational authentication practices and nuances, it is strongly recommended not to use the value defined in this Profile to meet local MFA request /response needs."

David Walker / InCommon

Not present

Due to that some commercial Identity Provider softwares, for example ADFS, is handling not known authentication context classes very bad or even breaks the log in flow with a software error it would be good to add an indication that this Identity Provider is technically capable of handling the REFEDS MFA authentication class signaling, or the other way around. An entity support category sound wrong but it may be the best fit.

Pål Axelsson / Sunet

4.1 Multiple Factors, lines 59 - 63

The EU Revised Directive on Payment Services (PSD2) Strong Customer Authentication requirement has an elegant definition of MFA. Suggest we adopt that text:

PSD2 Article 4(30):

an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data

Ref: Wikipedia article on Strong Customer Authentication

Albert Wu / InCommon

5.1.3.3

The section should be normative.

In section 4.1 it is stated that when logging in the user must use a combination of at least two factors when authentication. This means that under section 5.1.3.3 it must be the full authentication even in the case of a forced authentication.

Suggestion for additional text: "If an authentication request requires a fresh authentication via the attribute ForceAuthn, an Identity Provider must perform a new authentication of the Subject as described in section 4.1."

That ForceAuthn is unspecified in SAML is irrelavant for the section.

Pål Axelsson / Sunet

5.2.2

In section 4.1 it is stated that when logging in the user must use a combination of at least two factors when authentication. This means that under section 5.2.2 it must be the full authentication.

Based on this time of authentication must be set to when the full authentication was done, not when of the factors was latest used.

Pål Axelsson / Sunet