Consultation: MFA Profile v1.1

This consultation is now closed.

(The consultation opened on 14 November 2022 and closed on 15 January 2023 at 17:00 CET)

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

comment #	Line /Reference #	Proposed Change or Query	Proposer / Affiliation	Action / Decision (please leave blank)
1	4.3 Validity Lifetime	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	Peter Havekes / SURF	Please see Editor's Follow Up to REFEDS MFA Profile v1.1 Consultation and Next Steps.
2	5.1.3.3 ForceAuthn	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.	Peter Havekes / SURF	Please see Editor's Follow Up to REFEDS MFA Profile v1.1 Consultation and Next Steps.
3	Section 4.1, line 60-61	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?	Francisco Aragó / RedIRIS	While the FAQ is expected to include additional guidance, the committee is not intended to provide ongoing governance to maintain any authoritative decisions of which specific MFA methods (and combinations of methods) is acceptable. However, we will take this recommendation back to the steering committee.

4	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	Please see Editor's Follow Up to REFEDS MFA Profile v1.1 Consultation and Next Steps. The technical details of this Proxy scenario are outside of the scope of this profile. We welcome contributions in an updated MFA Profile FAQ to clarify how to configure MFA when proxies are involved in a deployment.
5	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	We have made updates to the Profile text according to suggestion here.
6	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 techhnically capable of handling the REFEDS MFA authntication class signaling, or the other way around. An entiy support category sound wrong but it may be the best fit.	Pål Axelsson / Sunet	We believe there is value in capability signaling using entity categories. Although introducing an entity category is outside the scope of this Profile. We suggest charting a capability signaling entity category working group to explore this idea.
7	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	We amended the Profile to include the following: "The authentication of the user's current session MUST use a combination of at least two of the four distinct types of factors, that is something a user knows (e.g. password), something a user has (e.g. a hardware device containing a credential such as specific phone or security token), something a user is (e.g. biometric identification, such as a fingerprint or facial recognition), or something a user does (e.g. behaviours such as typing pattern, mouse movement, etc)."
8	5.1.3.3	The section shoul 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	Please see Editor's Follow Up to REFEDS MFA Profile v1.1 Consultation and Next Steps.
9	5.1.2/5.2.2	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 5.1.2/5.2.2 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	Please see Editor's Follow Up to REFEDS MFA Profile v1.1 Consultation and Next Steps.
10		IMO the refeds MFA profile should aim to provide a standard MFA policy that is practical to implement for the IdPs in our community. As noted in the introduction it is expected that an IdP that does MFA already has a local policy and that it will hinder adoption if the refeds MFA profile is too strict. The refeds MFA profile should therefore aim to set a resonable minimum and and limit requirements to what is absolutely required while on the other hand offering enough to be attractive and usable by SPs. Setting clear expectations to IdPs and SPs and non normative Implementation advice will be really useful in the adoption process. The proposal already does this quite well. There are places where the profile IMO is more strict than necessary: • 4.3 Validity Lifetime – this precludes implementations that use a MFA session lifetime of more than 12h and balance that with other controls. This seems restrictive. Do we know what is typically used? • 4.2 Factor Independence –	~~David St Pierre Bantz / U Alaska~~	Please see Editor's Follow Up to REFEDS MFA Profile v1.1 Consultation and Next Steps.
11	4.3	Asserting authN context https://refeds.org/profile/mfa should provide assurance from the IdP to SP that the principal has in fact authenticated with multiple factors within the current IdP SSO session. While many seek to minimize the impact of requiring MFA by allowing use of "remember me" for much longer lifetimes, that (1) inherently weakens assurance level, particularly but not exclusively with kiosks or other shared devices, (2) leads to inconsistent user experience as prior use of 'second' remembered factor will inevitably get "out of sync" with SSO session lifetimes, and (3) reducing forceAuthn to a request for new password/'first' factor only. Assurance, consistent user experience, and a robust forceAuthn function all point to disallowing 'remember me' to meet the refeds mfa profile altogether.	David St Pierre Bantz / U Alaska	Please see Editor's Follow Up to REFEDS MFA Profile v1.1 Consultation and Next Steps.
12	3. Profile Identifier	Keeping the profile identifier despite the „breaking change“ (a citation from the Editors' notes) with the 12 hour validity lifetime window is not logical. The „constraint to not modify the Profile identifier“ as mentioned in the Editors' notes needs to be waived due to this change that is not a simple clarification. Especially regarding lines 51-53 that refer to additional identifiers for future versions. Introduce a new identifier already now for v1.1 because only that way an SP/RP will be able to know for sure that the IdP/OP supports v1.1 with its strict validity lifetime window and not v1.0 without one.	Thomas Lenggenhager / SWITCH	Please see Editor's Follow Up to REFEDS MFA Profile v1.1 Consultation and Next Steps.
13	6. References, line 307-310	Reference [ITU-X.1254] nowhere used in the draft v1.1.	Thomas Lenggenhager / SWITCH	Orphaned reference removed from updated Profile.

14	Editors' notes, section „Version Numbering for this Update“	The quote „we are still relatively early in this Profile’s adoption“ is not applicable for the SWITCHaai Federation. It has 35 SAML IdP, 75 SAML SPs,1 OIDC OP and 6 OIDC RPs that make use of v1.0 of this profile.	Thomas Lenggenhager / SWITCH	Please see Editor's Follow Up to REFEDS MFA Profile v1.1 Consultation and Next Steps.
15	Editors' notes, section „Version Numbering for this Update“	The Editors' notes states "we had a constraint to not modify the Profile identifier in this update". From where? The existing profile is already being used, and the updated profile introduces breaking changes. It is therefore the UK federation's opinion that the profile identifier should be modified for version 1.1.	Alex Stuart /UK federation	Please see Editor's Follow Up to REFEDS MFA Profile v1.1 Consultation and Next Steps