Consultation: REFEDS MFA Profile

Please note this consultation is now closed.

Background

The REFEDS MFA Profile was developed out of the work of the InCommon MFA Interoperability Profile Working Group. The group developed a Mutlifactor Authentication Profile for InCommon but with a strong recommendation that the proposal be furthered developed at REFEDS to ensure international interfederation interoperabilty for MFA signals. REFEDS is very grateful to InCommon for allowing us to reuse their work in the context of this profile development.

The MFA Profile has been further developed by the GÉANT Joint Research Activity on T&I Future Technologies and through discussion and prelminary consultation with the REFEDS Assurance Group. Particular attention has been paid to ensure the MFA Profile makes sense within the context of the upcoming Assurance Framework proposal. For more information, see the Assurance Working Group space.

Overview

The consultation opened on Tuesday 28th February 2017 and will close at 5pm CEST on Monday 27th March 2017.

Participants are invited to:

- Review and comment on the proposed REFEDS MFA Profile and its suitability for publication as a REFEDS profile. Comments on the naming convention and the requirements for signalling in the document are particularly welcomed.
- Reflect on the requirement that each factor used must be independent: is more guidance on specific use cases needed in the core text or can this be supported by FAQ documentation?

Following the consultation all comments will be taken back to the Assurance working group for review and if appropriate the Profile will then be forwarded to the REFEDS Steering Committee for sign-off and publication on the REFEDS website as per the REFEDS participants agreement.

The document for the consultation is available as an attachment to this page. Background on the Assurance Working Group is available. All comments should be made on: consultations@lists.refeds.org or added to the change log below. Comments posted to other lists will not be included in the consultation review.

Change Log

Change Log for the REFEDS MFA Profile Consultation. Please fill in your comments and change requests below. Line numbers are available in the document for ease of reference.

Number	Line / Reference	Proposed Change or Query	Proposer	Action / Decision (please leave blank)
1	Section 5, line 51-52	"listed in order of preference". While what is listed here is consistent with the SAML standard, it may not be feasible in practice to use ordering to select the correct context, especially for 2-step MFA implementations. Part of the problem I think is that there's a presumption that the list is prioritized but while that's superficially true, it isn't really true in practice, it's too hard to implement that in an IdP. I had all I could handle getting such a complex system to just make sure it didn't violate the request. It works pretty cleanly when the methods are all independent, but when Duo requires Password first, I think it's unavoidable that requesting Password is going to bypass Duo even if Password is at the bottom of the list. This may mean that the "listed in order of preference" comment may need to be removed, or extra guidance provided.	Eric Goodman / Scott Cantor	Agreed to delete section 5 and move to supporting documentation.
2	Section 5, lines 38-47	This profile defines two things: 1. It defines what it means when an IdP claims that an authentication event (assertion) was issued according to this profile and it defines how the IdP can express this in the assertion 2. In section 5 it defines how a SP COULD (SHOULD?) request authentication according to this profile. (1) Lines 1-36 clearly define the meaning of the identifier. No comment. (2) Lines 38-57 seem to me to be more like implementation guidance, and (security) advice. My suggestion would be to clearly mark this as such to differentiate it from (1) or leave it out of the profile altogether. It is valuable information, and it is a topic to continue to discuss. At this point I must conclude that there is not yet consensus on the way to use AuthnContextClassRef between SPs and IdP. A profile like SAML2Int will help to improve this situation as the less variance leads to better interoperability, but I don't think this profile is the way to achieve this.	Pieter van der Meulen (SURFnet)	Agreed to delete section 5 and move to supporting documentation.
3	Reference 2, lines 64-67	Is the URL for reference [2] a stable URL?	Pieter van der Meulen (SURFnet)	to check with I2.
4	Section 5, lines 38-47	Regarding Pieter's comment #2, the InCommon MFA Profile Working Group put guidance for this and a number of other topics into a separate, non-normative Usage Guidance For the InCommon “Base Level” and “MFA” Authentication Profiles. I would suggest doing the same here.	David Walker	Agreed to delete section 5 and move to supporting documentation.

5		As I understand it, the "base level" context class identifier was dropped, but I think that's a significant gap that should be addressed simply because it provides a technology neutral way of expressing "not MFA" for use with SAML and other protocols. We really want to get away from technically specific expressions like "password" and unfortunately it's required by SAML to include **something** in the assertion. So that's ultimately the main value of having it. It need not be part of this profile, but it wasn't really part of InCommon's either, it was simply included along with it.	Scott Cantor	it hasn't been dropped, just not circulated for consultation at this stage as consensus not reached.
6	Reference 1, lines 60-62	Minor detail for those who still click on links: The link behind the text https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf is incorrect (it contains the line number 62 in the url 🙂).	Ton Verschuren	Final version will be published as html not pdf
7	ITU reference	**Q1: LOA - how does this align (or NOT?) given that the ITU document specifically calls out LOAs that other like Vectors of Trust(VOT) initiatives and the latest 800-63 refresh have?** From my perspective: There is a possible mismatch of LOA assumptions going on implied in the MFA work. Sure, we don't dig into LOA, but how can you talk about MFA without LOA, especially since there's mechanisms in SAML for LOA to be expressed? Classic use of NIST 800-63 I believe has led people to assume federated ID 'starts around LOA0' in that yardstick. In the ITU definition, it appears to me that LOA2 is the initial level that federated ID has achieved by default PRIOR to elevation of the credential. This may lead to confusion and recommend REFEDS articulate a position on this difference or at least acknowledge they ARE different rather than have people make mismatched assumptions like: LOA1(NIST800-63)==LOA2(ITUx1254). Ref: see section 6.2 and maybe table 6.2 is useful in this regard? This will really confuse people. Additionally, VOT collapses into 1-4 LOAs which may not be the same fidelity that SPs want and this MFA statement appears silent on if I am reading it correctly. Recommendation: CLARIFY what LOAs are being expressed AND the relation to the ITU document and other community used documents (NIST, Vectors of Trust etc) will be immensely helpful. Additionally if the MFA work is *NOT* going to talk about LOA it should come right out and say that it will not use SAML2 LOA structures. (this is a provocative statement of course and think there needs to be some conversation around it at least.) Aside: Without talking about this, this could be another thing like 'isRequired=true/false' is ambiguous situation. I would rather be very clear on it as eduGAIN would be the filter on what is and isn't going to be expressed and we're going to need a crisp definition on entities and their decoration in my opinion.	Chris Phillips	Clarify in supporting documentation
8	ITU reference	**Q2. If the MFA work is meant to help 'move the needle' on what factors there are, should the group be concerned about some loophole like comments in the ITU work?** Observation: In the ITUx.1254 section 10.3.2, Table 10-6 it is worth noting that MFA is specifically called out that it is not resistant to general threats. I think this is the ITU document hedging on what they don't know and could be risky. Recommendation: Recommend REFEDS consider calling this out too or at least meet it head on and why. It's buried, but looks like the loophole 'don't blame us if 2fa doesn't defend against a threat'. I welcome to be challenged on this.	Chris Phillips	Clarify in supporting documentation