Consultation: REFEDS Assurance Framework round 2

THIS CONSULTATION IS NOW CLOSED. EDITS MADE AFTER 22/06/2018 WILL NOT BE CONSIDERED AS PART OF THE CONSULTATION.

Background

The AARC project and the REFEDS Assurance Working Group have developed a proposed REFEDS Assurance Framework (including two assurance profiles Cappuccino and Espresso) to be used by research and education federations in order to support a variety of assurance needs from service providers. The framework and the profiles specifically avoid the concept of "levels" - recognising on the one hand that the required assurance needs of any given scenario, group, or service do not necessarily map neatly on to a static hierarchy and on the other that home organisations can often meet some sets of requirements in different "levels" in traditional structures but can struggle to meet the complete requirements at any given level. The REFEDS Assurance Framework and assurance profiles intend to meet known use-cases in a pragmatic and tailored way.

The REFEDS Assurance Framework is complemented by the REFEDS Single-factor authentication profile that is exposed to a parallel consultation.

With thanks to AARC for supporting man-power to create this proposal.

Mikael Linden has written a useful background blog on the consultation.

Overview

**** The consultation CLOSED at 5pm CEST on Friday 22nd June 2018 ****

Participants are invited to:

- Review and comment on the proposed Assurance Framework.

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.

This Assurance Framework is now available for a second round of consultation. Details from the first consultation can be found at: Consultation: REFEDS Assurance Framework.

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 Assurance Framework 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	74	The idea that asserting values on the eppn reassign also implies that eppn is unique seems unintuitive and liable for misinterpretation. I also find the statements at line 74 and at 94 to be conflicting. 74 = "if the Home organisation asserts unique and no-eppn-reassign, then the ePPN attribute value also shares the same uniqueness properties as eduPersonUniqueID (ePUID)." 94="Finally, the reader is reminded that they should not assume any uniqueness property that goes beyond the specification of the attribute." Unique and not-reassigned do not necessarily mean the same thing, which is implied by line 74 somehow.	Hannah Short (CERN)	Reworded the section to express clearly what is required on ePPN uniqueness and reassignment.
2	114	It would be helpful to see examples brief examples of each Identity proofing level, without having to go through 5 clicks and a download form to get to Kantara.	Hannah Short (CERN)	Added an example to each ID proofing level.
3	156	I feel like a broken record and am sure there's a reason why you have decided to be generic here, but might it be useful to reference Sirtfi?	Hannah Short (CERN)	The working group didn't change the resolution of comments #10 and #19 in the first consultation. The Assurance framework and Sirtfi are parallel and orthogonal frameworks.

4	62	Which are the pairwise identifiers recommended by REFEDS? persistent-id is mentioned in the footnote. What about the (proposed) SAML2 pairwise-id? Speaking about this: why does it have to be pairwise (i.e. why would subject-id not qualify, considering it fulfills all three requirements)? Is the reason to keep it rather vague to allow for additional identifiers in the future? If so, I still think you need some reference to these "recommended identifiers". If it's just supposed to be persistent-id, why not just name it in the table directly?	David Hübner (DAASI /DARIAH)	Reformatted the list of identifiers and included a reference to the latest SAML2 Subject Identifier Attribute specification draft.
5	218-234	Shouldn't this be profile/espresso (in addition to profile/cappuccino)? According to the table (line 176) and with the authentication strength gone, the only difference between the profiles is IAP /high, which is asserted here.	David Hübner (DAASI /DARIAH)	Adopted proposal.
6	237	There is no real conjunction anymore, though, is there? While I realize, that there is no document, that really connects RAF and the authentication profiles, I still feel that Appendix C is a bit out of scope for this documents and might be better placed in the MFA and SFA profile documents.	David Hübner (DAASI /DARIAH)	Dropped Appendix C.
7	5	I'm missing something of an explicit problem description or goals that this standard seeks to accomplish. Current text is rather vague ("need to make decisions" - why, to what end, how are they going to use this info?).	Thijs Kinkhorst (SURFnet)	Reformatted the sentence in the beginning of the abstract.
8	114	Hard to read and understand table, because it's constituted only of references to external documents. Propose to add concrete indications of the meaning, common denominators of the choices, or examples of expectations.	Thijs Kinkhorst (SURFnet)	Added an example to each ID proofing level.
9	114	References Kantara spec which is only available should one feel inclined to fill out a form asking for all kinds of personal information and even a "reason" why one would want to read the doc. Propose to only reference open standards only.	Thijs Kinkhorst (SURFnet)	Kantara has changed its policy and made IAF-1420 publicly available.
10	134	The options 1d and 1m are likely too short to allow the majority of our IdPs to assert them. The "grace period" after someone departs before their account is impacted is commonly at least a month (note that a month is >30d) and often more in the order of about 60 or 90 days. The text itself mentions "in some organisations the student status remains effective until the end of the semester" (which hence can be up to 6m), but the standard does not provide a way to express this case; is it provided as an example of something undesirable? (maybe make that explicit then that the spec does intend to exclude these persons) Either there need to be longer timeframe options (order of multiple months) or it's likely that hardly any of our IdPs will be able to assert it (so to enjoy either of the coffee sensations). At the very least it would be helpful to define the 1m flavour as up to 32 days to be able to assert it by those who use a month's time.	Thijs Kinkhorst (SURFnet)	Clarified the difference between "business decision" (when a person departs) and "IT practice" (how long it then takes that the person's affiliation attribute is updated). Prolonged 1m to mean maximum 31 days.