Consultation: REFEDS Assurance Framework

This consultation is now closed, thank you for all the inputs.

Background

The AARC project and the REFEDS Assurance Working Group have developed a proposed REFEDS Assurance Framework and two assurance profiles 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.

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

Note

The Assurance Framework has placeholders for authentication profiles for which REFEDS is carrying out separate consultations. These will be resolved into the framework before publication.

Overview

The consultation opened on Friday 21st April 2017 and closed at 5pm CEST on Friday 9th June 2017. This consultation is now closed.

Participants are invited to:

- Review and comment on the proposed Assurance Framework.
- Review and comment on the proposed assurance profiles proposed by the 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.

Change Log

Change Log for the REFEDS Assurance Framework Consultation. Actions from these proposals can be found in an attachment.

<table>
<thead>
<tr>
<th>Number</th>
<th>Line / Reference</th>
<th>Proposed Change or Query</th>
<th>Proposer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Section 2.2</td>
<td>What about the other IGTF APs? Presumably CEDAR is also here if CEDAR&gt;BIRCH. What about ASPEN? (suggestion for Appendix)</td>
<td>Jens Jensen</td>
</tr>
<tr>
<td>2</td>
<td>Section 2.1</td>
<td>There is active discussion around the major shortcomings of SAML persistent IDs because of their case-sensitivity requirements, so I worry this is going to be obsolete on day one. Perhaps the reference to specific identifiers can be left to implementation guidance and not baked in.</td>
<td>Scott Cantor</td>
</tr>
<tr>
<td>3</td>
<td>Section 2.1</td>
<td>In light of recent concerns raised about the relationship between EPPN and mail attributes, it may be wise to be explicit about any assumptions that one is intended to make (or not) about that. For example, if it's meant to be assumed that a given EPPN value if found in a mail attribute refers to the same person, that isn't mandated by eduPerson, and should be called out here.</td>
<td>Scott Cantor</td>
</tr>
<tr>
<td>4</td>
<td>Line 166</td>
<td>s/securitybcontacts/security contacts/</td>
<td>Scott Cantor</td>
</tr>
<tr>
<td>5</td>
<td>Section 4</td>
<td>I'm really surprised that there's still no profile defined for &quot;strong authentication, no verification&quot; given the very consistent feedback I think IdPs have always gotten that that's the dominant requirement of a lot of projects. I think, as with InCommon Silver before, the verification requirements will prove impractical for most IdPs to meet whereas MFA is becoming very common, at least in the US.</td>
<td>Scott Cantor</td>
</tr>
<tr>
<td>6</td>
<td>Section 5.1</td>
<td>The overall assurance profiles really need to be handled via AuthnContextClassRef if you intend for RPs to be able to request their use.</td>
<td>Scott Cantor</td>
</tr>
<tr>
<td>7</td>
<td>Section 5.1</td>
<td>The text around the use of the EntityAttribute(s) needs to clarify whether there's an intended &quot;authorization&quot; semantic such that CSPs are not meant to assert the profile(s) if they don't carry the attribute. That tends to be inferred by people and that's one reason the InCommon MFA profile elected not to suggest that approach. If the profile is self-asserted by the CSP or at least if this document doesn't purport to suggest otherwise, I would reconsider that mechanism.</td>
<td>Scott Cantor</td>
</tr>
</tbody>
</table>
The inclusion of SAML metadata entity attributes in the framework makes me nervous that the entire framework will stall due to unresolved questions around handling of metadata entry attributes by federation operators. However, as far as I can tell, the metadata entity attributes are only a hint for IdP discovery, and I understand the recommended practice is to list all eduGAIN IdPs in our discovery interface then gracefully handle errors rather than preemptively restricting the list of IdPs to only those with certain entity attributes.

Jim Basney

Section 3.2

"The Identity Provider is trusted enough to be used to access the organization’s own systems." This cannot never be fulfilled by some organisations in Italy because they don't use SAML internally, so their IdP is used only to access external systems. At the same time all the identities managed at the IdP are trusted at the same level of the identities used to access internal systems.

Lalla Mantovani

Section 2.4

Attribute freshness is also determined by the operational security of the IdP, which can have an impact on the LoA of the asserted attributes. We were wondering whether this should be added as a 5th point determining the overall LoA (i.e. as a 2.5). Section 3 point 4 mentions that "Generally-accepted security practices are applied to the Identity Provider." but this is too vague and still does not take operational security into account in the determination of the overall LoA. We feel that this could be made explicit by e.g. requiring SIRTFI for this baseline LoA.

Mischa Sallé & the rest of AARC-JRA1

17, Sec 4, etc

The profile name "espresso" duplicates the name NISO ESPRESSO report, which is directly mentioned in the REFEDS discovery guide. This runs the risk of confusing service providers who might be referred to both the ESPRESSO report for discovery best practices and the espresso profile for assurance, and will be looking for both of these on URLs within refeds.org namespace. I know profile names were voted on (and indeed, I stupidly voted for espresso). However, I believe avoiding this confusion is a compelling reason to choose another coffee beverage.

Guy Halse

Line 44

Proof-reading s/has/have/

Andrew Cormack

Line 88

Or the SP could invoke some strong out-of-band process to verify whether the user is still the same? I'm thinking of courses that involve a student having a year in industry/another country, or academics taking sabbaticals. Either of those could result in a year of non-use of a service. Or, indeed, there might be some services (e.g. enrollment) that are naturally only used once a year!

Andrew Cormack

Line 57-ish

Maybe worth stating explicitly that none of the following applies to the identifiers actually listed under "unique"? "In addition to the three identifiers mentioned in the definition of "unique", within the REFEDS community..." and "... two additional values that a CSP declaring uniqueness can use to indicate the extent to which this applies to ePPN"

Andrew Cormack

Lines 177 & 186

It bothers me that line 177 implies that Espresso is a superset of Cappucino, but the table in 186 says they aren't. The implication is that anything qualifying as "mfa" also satisfies "good-entropy", but I'd much prefer that (if it's true, which depends on what replaces the placeholders s2.3) to be handled explicitly by making good-entropy a requirement of Espresso as well (in the same way as you've done for the ranked IAP values)

Andrew Cormack

Line 51

"authenticated sessions can qualify to different values." This possibility is not expanded on in the SAML representation section, only the entity level assertions are included.

Hannah Short

Line 65 - 78

Should this be linked somehow to the Research and Scholarship entity category? R&S makes almost the same requirements on ePPN. Likewise, the fact that no ePPN reassignment properties are included in the capuccino and espresso profiles imply that ePPN should not be used (to my mind). I can imagine this being confusing when it comes to adoption by entities already using R&S.

Hannah Short

Lines 110 - 114

The wording here is potentially misleading. Does "assert" mean comply with, or broadcast compliance with (e.g. in SAML metadata)? If they are incremental, is it really necessary to broadcast both?

Hannah Short

Line 164

Given the lack of other "Generally-accepted security practices" in this domain, could we tie the framework to Sirtfi? +1 to Mischa's comment above

Hannah Short