AARC2-JRA1.1A -- Guideline on the exchange of specific assurance information between Infrastructures

Guideline on the exchange of specific assurance information between Infrastructures (AARC-G021)

Summary

Increasingly Research Infrastructures and generic e-Infrastructures compose an 'effective' assurance profile derived from several sources. The assurance elements may come from an institutional identity provider (IdP), from community-provided information sources, from step-up authentication services, and from controls placed upon the user, the community, or the Infrastructure Proxy through either policy or technical enforcement. Knowledge about the upstream source of either identity or authenticator can also influence the risk perception of the Infrastructure and result in a modification of the assurance level, e.g. because it has involved a social identity provider or perhaps a government e-ID. The granularity of this composite assurance profile is attuned to the risk assessment specific to the Infrastructure or Infrastructures, and is often both more fine-grained and more specific than what can reasonably be expressed by generic IdPs or consumed by generic service providers.

Yet it is desirable to exchange as complete as possible the assurance assertion obtained between Infrastructures, so that assurance elements need not be re-asserted or re-computed by a recipient Infrastructure or Infrastructure service provider.

This document describes the assurance profiles that are recommended to be used by the e-Infrastructures and research infrastructures AAI platforms to exchange user authentication information between infrastructures.

Status

This document is now in **final public comment**

Assigned DOI: https://doi.org/10.5281/zenodo.1173558 (this one was a bit challenging as we do not have a formal author list - too many undefined contribuants from AARC and AppInt)

Documents

Recasted document with specific scoping, rationale - and tightening the association with the REFEDS RAF framework - is now available:

- AARC-G021 Final Call document
- MS docx version

public-commentable versions:

- https://docs.google.com/document/d/1Fi07J9lpUbqYTlPMINkbHl7xvA5tJ98L4jai6XNKbDM

And a snapshot of the REFEDS RAF document (2018-02-15) for reference.

Discussion

Specific Open Questions (Feb 1st) Addressed:

- the 'attribute freshness' (ePA-1m) as coming out of an Infrastructure Proxy is now normatively defined in this document as
  "The ATP assurance component (attribute freshness) SHALL reflect the affiliation of the identity with the CSP, i.e. the Infrastructure Proxy."
  It's the interpretation that makes most sense in case the resulting assertions from the proxy would (acidentally or on purpose) be re-inserted in eduGAIN, and also it better reflects the fact that for linked and composite identities the change of affiliation in an upstream IdP does not necessarily reflect any change in the Infrastructure. The Community is always authoritative ...

IF this has already been stated in another JRA.* document, please put the ref here* 👒
RESOLVED: included in this guideline as rough consensus shows there is no better place for now

- the "Darjeeling" profile is very, very close to Espresso, the only thing it adds is that it adds to MFA support *also* a quality requirement on the first factor. Is that profile really useful? Could we drop it (please)?
  RESOLVED: rough consensus indicates this can be dropped
- On output, if the combination of assurance component values meets a REFEDS RAF profile, you must now *also* assert the REFEDS RAF profile values - so that if the assertion 'escapes', it still makes sense to generic service providers
  RESOLVED: no negative comments received
- The flagging of 'social identity providers' was considered quite important, so Assam does that for you. However, if the identity provider is a homeless IdP with known qualities, you SHOULD also assert those properties if you know about them (like IAP/low and maybe even SFA).
  RESOLVED: if one can reasonably know that IAP/low is met, this should be added as well

Other comments addressed

Q	Addressed by

References to other (potentially future) guidelines	`add to each of the guideline documents:`
	`  "This Guidelines should be used and interpreted in the context of the`
	`  AARC Blueprint Architecture (https://aarc-project.eu/architecture/) and`
	`  the AARC Policy recommendations (https://aarc-project.eu/policies/)."`
	
	`so that we don't have to re-iterate the references every time?`

On the subject of Darjeeling, if we are asserting both Espresso and MFA, then you would assert Darjeeling, Espresso (as per the "superset" rule), *and* MFA *and* components (as per the components rule), so this kind of suggests Darjeeling is mostly redundant even if some infrastructure had a use case for it.	Dropped as by rough consensus
if you have, say, BIRCH plus MFA, then you can't assert BIRCH? ... because the BIRCH profile says SFA, so your values are no longer a superset. This actually links to a long-standing discussion in the REFEDS RAF WG, which concluded that - however strange it may seem - SFA is not a subset of MFA.	In the MFA profile it puts nowhere any quality requirements on any of the factors. It is unlikely that thsi will change, since MFA has been recently adopted by REFEDS and they do not want to change it. As a result, we conclude here that we need some additional specs on the MFA to make this happen. Under implementation notes in the document there is now a specific paragraph addressing this: "If the authentication assurance component meets the REFEDS-MFA criteria and the CSP can determine that at least one of the factors also meets the good practice requirements for REFEDS-SFA..."
Auditability and tracability of decisions in the proxy, or the business logic inside the proxy should be considered	Although very true, this is out of scope of this specific guideline document.

Meetings schedule and Minutes

Mailing list discussion only