AARC-G031 - Guidelines for the evaluation and combination of the assurance of external identities

Summary

The Research Infrastructures (from now on just Infrastructures) that follow the AARC Blueprint Architecture [AARC-BPA] set up their own AAI to grant access to their services. The AAI is typically based on a central IdP-SP proxy that act as a gateway for the Infrastructure services and resources. In order to assign an identity to the users of the research collaboration or the community they serve, Infrastructures rely on external Identity Providers and employ identity linking strategies.

The Infrastructures also define one or more assurance profiles, or a combination of assurance components, tailored to a specific risk assessment [AARC-G021].

In order to assign an assurance profile to a user, the Infrastructure shall evaluate the assurance components of the linked identity, or identities, used to register to the Infrastructure's AAI or used during authentication at the infrastructure proxy. These guidelines provide a method to combine assurance information and to compensate for the lack of it.

Status

Final (18 May 2018), Endorsed by AEGIS (9 June 2018)

DOI: https://doi.org/10.5281/zenodo.1308682

Links

PDF

MS Word version

Working doc

https://docs.google.com/document/d/1ODfru_zjQHQp57MxE1PCZh7lafw57OCiM1fgejx4EbI/edit#

Discussion

AEGIS review comments 14 May 2018

What if there are user that use identity providers that do not support R&S?	R&S is just a way to assert the unique value for the ID component. When you do not have an assertion of the Id component, you can use R&S if you have it, if you do not you can use the **im_a_person** and **contacts** compensatory controls.
What if the external identity provider is a social media IdP? Is it still possible to achieve a minimal assurance profile?	One of the purpose of this document, along with AARC-G021 and AARC-G041, is exactly to allow Identity Providers outside of eduGAIN to be able to achieve at least level of low.
Affiliation can only mean that this identity has a meaning for this community. Do we really want to have the affiliation as part of the users' identity?	The document is agnostic toward the expression or not of affiliation information.
What if something like eIDAS is used in the future? We need to leave a window open for such identity sources, which might not signal the expected RAF values but we know they are good	Yes. While the current document is not making compulsory to use RAF or the suggested compensatory controls, we better highlighted the fact that others assurance frameworks might be used to convey assurance information: • **OLD** *A requirement for the assurance evaluation is that assurance components related to the same individual, but coming from different IdPs, are defined along the lines of the RAF, or can be translated into those definitions* • **NEW** *A requirement for the assurance evaluation is that assurance components related to the same individual, but coming from different IdPs, are defined along the lines of the RAF, or, when expressed through other assurance frameworks as for example eIDAS LoA [eIDAS LoA], can be translated into those definitions*.
Is the document aligned with the title which says “combined” (indicating there are at least two external IDs linked to the infrastructure ID) but the contents (compensatory controls) are applicable even if there is just one external identity	Yes, it is true. We changed the title to *Guidelines for the evaluation and combination of the assurance information of external identities*.

Meetings schedule and Minutes

Date	Location	Agenda	Minutes

21 Jul 2017 14:30 CEST	https://webconf.vc.dfn.de/aarc-jra1	First AARC2 JRA1.3 meeting	2017-07-21 Meeting notes
23 Aug 2017 14:00 CEST	https://webconf.vc.dfn.de/aarc-jra1	Discuss TOC and use cases	