Draft: REFEDS Assurance Recommendations

Authors: Jule Ziegler, Tom Barton, Pål Axelsson, Jon Miner, Alan Buxey, [add your name]

Introduction

The REFEDS Assurance WG was established in 2016 to address the needs in Research & Education (R&E) of defining a minimal degree of identity and authentication assurance. After successful community consultations, the first full version of the REFEDS Assurance Suite was published in 2018, being comprised of the REFEDS Assurance Framework (RAF), the REFEDS Single Factor Authentication Profile (SFA) and the REFEDS Multi Factor Authentication Profile (MFA). While RAF specifies requirements on identities and allows them to be individually assertable, REFEDS SFA and MFA cover criteria on authentications using a single factor or multiple factors, respectively.

Although the REFEDS Assurance Suite specification is, in itself, considered as complete, there are various aspects, e.g. related to signaling, interoperability, awareness, which still remain unaddressed. This fact also appears to correlate with the low adoption rate that has been observed in the R&E community so far. As part of this document we capture these assurance related aspects we feel need to be addressed and identify potential ways how these aspects can be tackled. The recommendations which are derived in this document do not exclusively contain action items assigned to the REFEDS Assurance WG but do also cover general recommendations and ones which could be addressed in collaboration with other Working Groups. Finally, a conclusion on the plans for 2021 of the REFEDS Assurance WG is given.

Overall Level of Awareness

It was noted that although outreach activities for promoting the REFEDS Assurance Suite are continuously being performed at various occasions in the R&E space, both nationally and internationally, the adoption rate is still fairly low. It appears that the significance of assurance information has not yet become clear within the community and that its meaning might not yet be fully understood. It must be clearly communicated that assurance information is not about releasing another set of personal data, but is instead focusing on processes and practices related to identities and authentications performed within an organization. When it comes to adoption, the WG also recognizes the challenge that as long as Service Providers are not starting to request assurance information, Identity Providers probably won't start releasing such information. This is why representative use cases will help to trigger a forward movement within the community. With the National Institute of Health (NIH) starting to request RAF, MFA, and R&S in 2021 such a use case was obtained but additional ones are still desired.

The WG concluded that:

- Continuous outreach should be kept alive

- The WG agrees that promoting activities cannot be carried out by themselves in the long run. Especially in the case of national identity federations and NRENs, the WG recommends to set up national assurance awareness programmes to reach as many institutions as possible. It is to investigate whether material for such programmes could be provided by the WG. Also, t

- The activity of designing logos should be further pursued. These logos can in turn be used for outreach purposes and REFEDS brand recognition, similar to what was done by InCommon when distributing logo badges at Internet2 TechEx conferences. Vector-graphic versions of any logos are needed.

Assurance Certification in Metadata for REFEDS Assurance Suite

The question of whether REFEDS Entity Categories (ECs)[1] would be needed for RAF, SFA and MFA arose several times. Entity categories provide some technical means to enable both filtering capabilities and also to collect statistics about entities implementing assurance specifications which was on the one hand considered as useful but on the other hand raising the question if introducing ECs would impede adoption. For example in the case of R&S, it was observed that even though entities could technically release R&S ECs the challenge of supporting ECs is rather policy wise than technical. When asking for feedback about assurance ECs within the community the poll yielded no clear consensus. While discussing this topic further within our regular Assurance WG calls two potential alternatives to ECs have been identified by the WG:

1. Instead of following a technical approach for collecting statistics about assurance adoption, assurance components could be added to the currently developed REFEDS baseline expectation work.

2. Instead of creating assurance specific ECs the eduPersonAssurance attribute which is used for expressing RAF components could be added (as an optional attribute) to the R&S specification.

The WG concluded the following:

- The WG considers the baseline approach as the preferred option over the EC approach at the moment. The WG also agrees that this might change in the future and thus needs periodic reinvestigation.

- R&S: making eduPersonAssurance mandatory will probably not work as this is a lot of work The WG proposes to add eduPersonAssurance="https://refeds.org/assurance" as a required attribute-value pair to R&S. The rationale is that this value merely states compliance to the Conformance Criteria of RAF while additional assurance info (e.g. attribute freshness) remains optional and can be released by the IdP, if desired and the respective criteria being met, as additional value of eduPersonAssurance.

[1] https://wiki.refeds.org/display/ENT/Entity-Categories+Home

Releasing RAF Attributes

It was noted that some potential implementers have asked *when* RAF attributes should be sent, i.e., to which SPs they should release RAF identity information.

The WG concluded, that a three-fold strategy should be followed:

1. Add a best practice recommendation to RAF that RAF attributes should always be sent. The rationale for this is that RAF attributes are not personal information, they are metadata about IdP policies and practices that pertain to a class of IdP users to which the Subject belongs. And of course always sending them is far simpler than any alternative means in which some sort of request-response processing is required to get RAF attributes. KISS. The WG recognized that, of course, not all IdPs would observe this best practice, and so also recommend the following.

2. Add another best practice recommendation to RAF that SPs wishing to receive one or more RAF attributes list those attributes in their entity metadata's requested-attributes statement. This would further broaden the circumstances under which RAF attributes actually help address needs among federation participants.

3. To further expand the circumstances under which RAF attributes help address needs, the WG recommends to the REFEDS WG to be convened to review the R&S Entity Category to add RAF attributes as optional attributes under a revised R&S specification.

- best practice

RAF ID Proofing Component

The WG also noted that the RAF IAP/Low, IAP/Moderate, and IAP/High values are currently defined in terms of comparable IGTF profiles, Kantara Classic Assurance Levels, and eIDAS assurance levels. This work was done prior to the release of NIST 800-63 v3, which split identity assurance and authentication assurance apart from the v2's monolithic assurance levels.

The WG concluded that:

- To keep the RAF specification up to date and useful to many relying parties who are obliged to reference the identity assurance specification NIST 800-63A from v3, the WG should undertake the work of adding 800-63A v3 equivalents to IAP/Low IAP/Moderate, and IAP/High.

Assurance Testing Toolss, as well as on the range and the methodology of writing tests.
ORCID MFA Support

Conclusion

In regard to the first objective, especially the section on the ID Proofing Component identifies work which is important and might lead to a new version of RAF. Whether and when new versions of the RAF, SFA and MFA specifications would be published has not yet been agreed on and underlies the community-driven processes of REFEDS.