Comparison Guide to Identity Assurance Mappings for Infrastructures

Publication Date	2019-02-28
Authors:	Ian Neilson;David Groep
Document Code:	AARC-I050
DOI:	
Status:	DRAFT
Grant Agreement No.:	730941
Lead Partner:	Nikhef, STFC

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract

With a wide range of identity assurance frameworks to choose from, the most appropriate choice of assurance profile for a use case (one that meets both the risk assessment and the social and community context in which the assurance is needed) may be viewed as confusing. The choice of Cappuccino or Espresso from the REFEDS Assurance Framework, Assam from the AARC social media assurance, Birch and Dogwood from the Interoperable Global Trust Federation, Silver and Bronze from InCommon, and Levels 1 through 4 from both Kantara and NIST SP800-63 – all of these merit a policy mapping and comparison framework. In this whitepaper, we identify the implicit trust assumptions (in research and collaboration frameworks, the R&E identity federations, general private sector frameworks and e-government schemes) and present a way of comparing these frameworks.

This whitepaper is a response to the request for a matrix showing the different assurance levels in the context of the AARC Guidelines and deliverables.

Table of Contents

1. Introduction

A wide variety of identity assurance frameworks ("IAFs") has emerged over the past decades from a range of different backgrounds: e-government, commerce, banking, academia in general, or research and collaboration in particular. These frameworks have subsequently evolved, in both convergent and complementary directions – reflecting choices in identity risk management, intended breadth or reach of the specifications, intended audience, and the implicit coherency (or lack thereof) within these target audiences.

The result after a few decades is a multitude of assurance frameworks, and many assurance profiles (also often called assurance *levels*) within them. For the uncommitted, it has become a complex and daunting space with which to engage. And for those looking for interoperation between services and infrastructures relying on different frameworks, the requisite policy mapping exercises are complex.

In this whitepaper we compare the two main IAFs from the federated research collaboration domain (the REFEDS Assurance Framework, RAF, and the Interoperable Global Trust Federation, IGTF) – both of which have formed the basis for the AARC *Guideline on the exchange of specific assurance information between Infrastructures (AARC-G021)*, with the Kantara Identity Assurance Framework (KIAF-1420, which most closely related to version 2 of NIST SP800-63) and with the eIDAS assurance levels.

This paper should be considered as a non-normative, explanatory document, providing context to the AARC-G021 guideline. The work here does neither replace nor augment the G021 guideline, but is meant to elucidate the concepts of assurance and identity vetting in the context of the risk appreciation of the federated research and collaboration infrastructures.

2. On context and breadcrumbs

The suite of assurance frameworks reviewed reveals two basic variants. On the one hand, frameworks such as NIST SP800-63, Kantara IAF 1420, and eIDAS aim to include all potentially relevant aspects of identity assurance, including the management and organisation of the credential issuing authorities. On the other hand, we find frameworks whose focus includes all components of assurance, but where the organisational context in which these are evaluated is implicitly assumed, to a greater or lesser extent. It allows these frameworks to be more compact, and be more easily adoptable within the target constituency of these frameworks.

Recent frameworks have predominantly moved to separating identity assurance in *constituent components*, of which the separation of managerial and organisational elements is just one exponent. The pioneering IETF Vectors of Trust work [RFC8485] by Richer and Johansson proposes the same for the identity assertions elements (presenting these as

Identity Proofing, *Primary Credential Usage*, *Primary Credential Management*, and *Assertion Presentation*). NIST SP800-63rev3 achieves the same with a broader set of components, and the REFEDS RAF framework follows the same model.

The separation of assurance in individual components distinct from organisational context has been taken to its ultimate conclusion in a framework such as REFEDS RAF, where technology choices within the R&E federations, in particular the use of SAML2, lead to completely separating off the authentication assurance from all other assurance components ("The assurance of authentication is not covered by this specification") [RAF], instead opting to place these in independent specifications ("REFEDS SFA" and "MFA"). As such, the REFEDS RAF reflects specific community choices to enable trust in the "assertions made by the Identity Providers and their back-end Credential Service Providers". The *assurance profiles* that group commonly feasible elements together are then provided to serve relying parties (RPs) seeking for simplicity (although these profiles do not extend to the authentication assurance elements that had been separated out).

The Assurance Profiles by the Interoperable Global Trust Federation [IGTF] are not formally separated in distinct components, but instead are a more direct reflection of the risk management model and assurance use cases by the stakeholders in the research and collaboration e-Infrastructures, in particular driven by the global consortia of relying parties more than by identity providers. The result is twofold: a focus on matching the risk profile(s) of the RPs, addressing those elements of assurance that must be taken care of by the identity providers (the push coming here from the RPs to which identity providers have to comply); and on exclusively using profiles to express assurance (putting the onus on the identity provider to construct self-consistent bundles of assurance components as a prerequisite for participation).

Both REFEDS RAF and the IGTF can however profit from their implicit organisational background and the evolutionary development of trust within their constituencies. Both form communities whose (human) core of trust providers and assessors is relatively small (75-125 people each, i.e., well below Dunbar's number), and both have evolved gradually from within a constituency where organisational and managerial controls have been externally provided (e.g. through joint endeavours with a level of semi-hierarchical coordination in the case of REFEDS, and in a context of global research and infrastructure consortia bound together through agreements broader than identity management in the case of the IGTF).

In addition, because of its direct engagement with the majority of its credential service providers and their internal coherency, the IGTF can leverage the peer-review methodology to facilitate compliance assessments. The assurance assessment process [IGTF-SA, GFD.169] and its peer-review and scrutiny process providing transparency towards RPs, are adequate safeguards within the RP risk envelope.

Both REFEDS and IGTF also benefit both from being frameworks targeted mainly at public sector participants. Many assumptions underlie 'being a public sector body', including matters related to liability or insurance (it is e.g. more common to have the ability to be self-insured), and for bodies to self-accommodate residual risk coming from third-party

interactions - as a result such elements do not feature at all in the REFEDS and IGTF frameworks.

Frameworks such as Kantara IAF-1420 and eIDAS cannot leverage such implicit trust. By necessity, their frameworks have to include all pertinent organisational and managerial controls, and provide them in a way that permits external auditors to make definite statements of compliance. They are thus far more elaborate, to the extent that this present a significant burden to adoption within those communities where partial implicit trust already exists – the observed level of adoption of the InCommon Silver assurance profile [INC-Silver] defined in terms of NIST SP800-63rev1 LoA 2, to which initially one, then zero federated identity providers signed up, provides a case in point. Yet in less homogeneous and larger communities, auditable completeness, complemented by enforcement processes, is customarily seen at the only mechanism for 'scalable' trust. Thus, these frameworks have to be complete and self-consistent: omitting requisite elements would leave the door open for unpredictable behaviour whose shortcuts would not be tolerable in a peer-reviewed transparent community, but that can remain undetected for long in a community that leverages auditable compliance statements.

The distinction between these two approaches can be viewed in two ways: either the stakeholder community frameworks (IGTF, REFEDS RAF) have 'lost the breadcrumbs' that brought them to their current state of partially implicit trust, or else their work on identity assurance framework has emerged late (later) in their collaboration life time, at a point in which partial implicit trust had already been established through different mechanisms.

Having performed an (implicit) risk assessment once, there is a further risk of divergence as assumptions regarding the assurance framework and its domain of applicability are internalised by the community. This is apparent in e.g. the multitude of assurance frameworks in national R&E federations, on which REFEDS RAF now attempts to impose a more coherent global approach.

3. Selecting Assurance Frameworks

Having an approach to identity assurance that partially leverages implicit understandings within a stakeholder community may be an appropriate way to addressing the trust and risk management issues. Both REFEDS RAF and the IGTF infrastructure assurance profiles have the great benefit of simplicity, and are more easily understood and adopted by participants in the (federated) research and academic community. Each should be used within its proper scope: REFEDS RAF (and the complementary REFEDS SFA and MFA authentication assurance specifications that conceptually form a bundle) for identity providers whose scope and purpose value broad adoption and feasibility from an institutional standpoint. The IGTF profiles, and the infrastructure interoperability profiles of AARC-G021, for meeting the risk profile of (global) research and collaboration Infrastructures.

The Kantara IAF1420 is by far the most comprehensive of schemes, extending NIST SP800-63 to both a more multinational character and broader domain of applicability, and as such provides the best basis for performing a 'gap analysis' of the 'lost breadcrumbs' in other frameworks. A scheme like eIDAS, focussing on a subset of countries (EU only) and a more restricted domain (e-government applications and citizen interaction) falls somewhere in between.

Regardless of the approach chosen, the assurance 'landscape' is now dotted with many frameworks, and those presented with this rather wide range of options are often daunted by the choice facing them. Within the scope of research and collaboration, the continued preference is for concise frameworks that focus on simplicity, since in the majority of cases that facilitates wide adoption, and the risk incurred by relying on implicit trust and assumptions is minor. Yet it is important to realise that the resulting trust, whilst acceptable within a 'non-profit', public sector academic and research environment, is circumscribed by the limits of its constituency, and should not be applied outside that domain without at least a proper gap analysis.

As a basis for the assurance profile comparison presented here, we selected the identity proofing elements of the REFEDS RAF profiles as the basis. The reasons for choosing RAF are its concise representation, and the use of the assurance 'vectors': ID uniqueness, ID proofing and vetting, and attribute freshness.

The comparison with the IGTF Authentication Assurance readily indicates that for research and collaboration infrastructures the basic RAF framework is not sufficient, as elements regarding operational security and credential management are lacking. We have thus discretionarily recombined the RAF profiles "Cappuccino" and "Espresso" with the most appropriate authentication assurance profiles, REFEDS SFA and MFA, respectively.

Still, the elements on site security, assessment ("audit"), and transparency that feature prominently in the IGTF framework (and are emphasises via different mechanisms in Kantara IAF1420 and eIDAS) are absent from the REFEDS RAF framework. This reflects the context of REFEDS RAF (it is to be used primarily within the context of the eduGAIN R&E federation service) and the current lack of transparency down to the credential service provider level within R&E federations. Yet this does not mean that RAF would be inappropriate to serve as the basis for the assurance model comparison – it only indicated that RAF, more than the other frameworks, has to be considered within its proper and more elaborate ecosystem..

A generalised comparison and gap analysis for assurance frameworks (potentially including visualisations and interactive tools to facilitate a comparison) are more properly left to a future investigation.

4. Graphical representations of assurance

Describe the graphics methodology here.

Lorem Ipsum …

4.1. IGTF Levels of Authentication Assurance

On ASPEN, BIRCH, CEDAR, and DOGWOOD.

Lorem Ipsum …

4.2. REFEDS Assurance Framework

Including SFA and MFA.

Lorem Ipsum …

4.3. Kantara Identity Assurance Framework

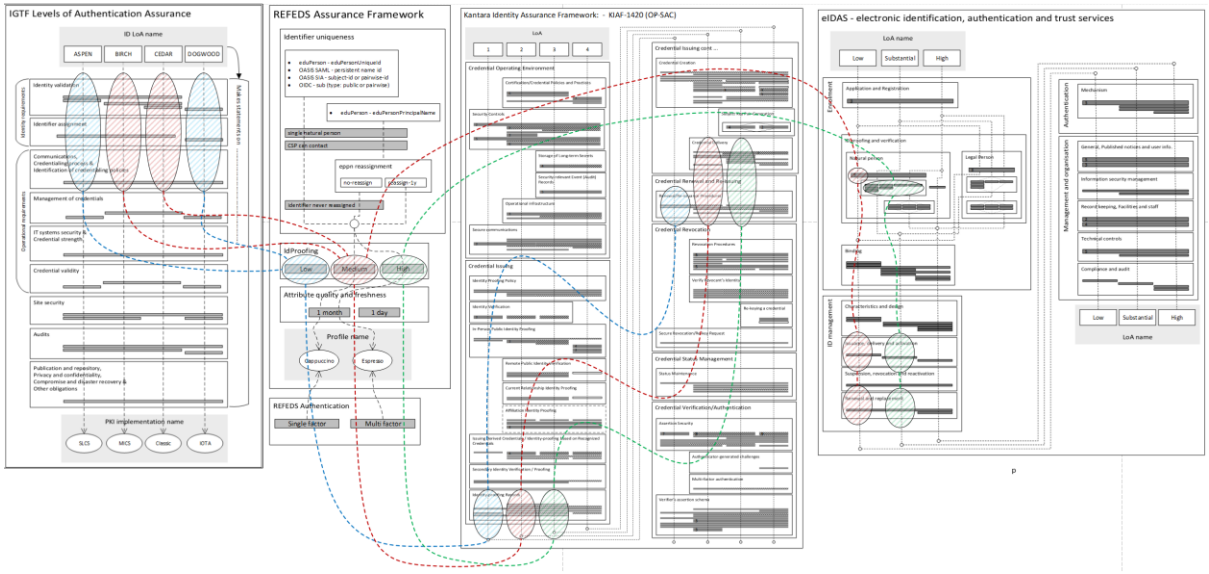
Lorem Ipsum …

4.4. eIDAS

Lorem Ipsum …

5. Comparing assurance frameworks

Lorem Ipsum …



Lorem Ipsum …

References

GFD.169 Y. Tanaka, M. Viljoen, S. Rea; *Guidelines for auditing version 1.0*; OGF GFD.169; https://www.ogf.org/documents/GFD.169.pdf

IGTF *IGTF Profiles of Authentication Assurance;* Interoperable Global Trust Federation IGTF; https://www.igtf.net/ap/loa/

IGTF-SA *IGTF Assurance Assessment;* Interoperable Global Trust Federation IGTF; http://wiki.eugridpma.org/Main/AssuranceAssessment

INC-Silver *InCommon Identity Assurance Profiles Bronze and Silver version 1.2*; InCommon LLC, 2013; http://www.incommon.org/docs/assurance/IAP.pdf

RAF *REFEDS Assurance Framework ver 1.0*; REFEDS Assurance WG; https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0

RFC8485 J. Richer (ed.), L. Johansson; *Vectors of Trust*; IETF October 2018; https://tools.ietf.org/html/rfc8485

Acknowledgements

The authors acknowledge the valuable contributions by the participants of the TIIME Vienna 2019 “Untangling Assurance Spaghetti” unconference session (http://tiimeworkshop.eu/), in particular Leif Johansson (SUNET) and Colin Wallis (Kantara Initiative). The views in this document are those of the authors and do not necessarily represent the view of the TIIME meeting participants.

Appendix A.1

Do you have appendicitis?