Comparison Guide to Identity Assurance Mappings for Infrastructures

Publication Date	2019-03-14
Authors:	Ian Neilson (STFC); David L. Groep (Nikhef)
Document Code:	AARC-I050
DOI:	10.5281/zenodo.3627594
Status:	PUBLISHED
Grant Agreement No.:	730941
Lead Partner:	Nikhef, STFC

© GÉANT on behalf of the AARC project.
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.

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 missing '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 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 they are evaluated is implicitly assumed, to a greater or lesser extent. This assumption allows these frameworks to be more compact, and hence more easily adoptable within their target constituency.

Recent frameworks have predominantly moved to separating identity assurance into *constituent components*, of which the separation of managerial and organisational elements is one example. 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 into 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 appropriate 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 of the Interoperable Global Trust Federation [IGTF] are not formally separated into distinct components. Instead, they present a more direct reflection of the risk management model and assurance use cases of the stakeholders in the research and collaboration e-Infrastructures, in particular driven by the global consortia of RPs 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 profit from their implicit organisational background and the evolutionary development of trust within their constituencies. Both arise from 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 (for example, it is 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 presents a significant burden to adoption within those communities where partial implicit trust already exists. For example, the 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 as 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 which would not be tolerable in a peer-reviewed transparent community, but that might remain undetected for a long time 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 trail of breadcrumbs' – the many decisionsthat lead them from their initial state to their current state of partially implicit trust -, or else their work on identity assurance framework 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 of addressing identified 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' looking for 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 of that domain without a full understanding of the risks incurred.

As a basis for the assurance profile comparison presented here, we selected the identity proofing elements of the REFEDS RAF profiles. 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 indicates that RAF, more than the other frameworks, has to be considered within its proper and more elaborate ecosystem.

More generalised comparisons and a gap analysis of 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

The charts presented below provide high-level representations of the structure and relative complexity of the 4 identity assurance frameworks discussed in the preceding chapters. Each framework describes a set of requirements each of which must be fulfilled by the issuing body for the assured identity to comply with a specific assurance level within the particular framework. The diagrams do not indicate *what* the requirements mean, only that there is a specification that must be applied within the component category, indicated by the title of the text box element. Similarly, a large number of requirements does not necessarily imply the difficulty or otherwise of fulfilling the specification for the component in question. Rather, the diagrams aim to provide a common representational framework with which to better understand and compare the assurance frameworks.

4.1. Description of representational elements used

Dashed lines link common requirements for a specified assurance level. These generally run vertically within diagram crossing horizontal grey bars which represent requirement statements. The size and position of the bars indicate to which assurance levels a particular statement applies. Requirements bars are grouped together in boxes, each of which is annotated with the title of the component of assurance, taken from the framework text.

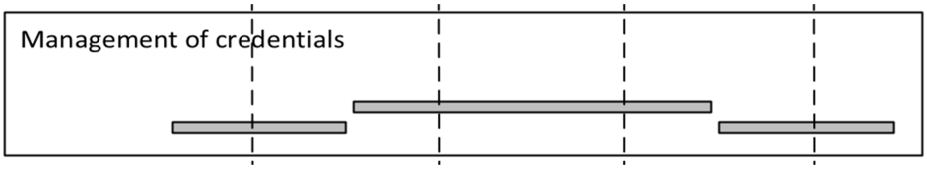

Figure 4-1: Representation of assurance requirement statements

For example, Figure 4-1 (taken from **Error! Reference source not found.**) represents 2 separate requirement statements applied across assurance profiles, within the component of “Management of credentials”. The first statement, represented as two grey bars on the same horizontal level, applies to the leftmost and rightmost assurance profiles, represented by the vertical dashed lines. The second requirement applies only to the 2 central assurance profiles.

Where a common set, comprising more than two requirements statements, is to be applied, they are represented as a single, broader rectangle with the appropriate number shown at the left edge. Figure 4-2 below shows where 3 common requirements must be met on all 3 intersecting assurance profiles.

Figure 4-2: Representation of multiple common requirement statements

Diagrams such as these are always going to be an approximate representation of the complexity of separation of requirements across more complex profile levels. Three further representations are used to indicate that the diagram is attempting to concisely represent what is, in fact, a complex set of statements. These are illustrated in the examples below.

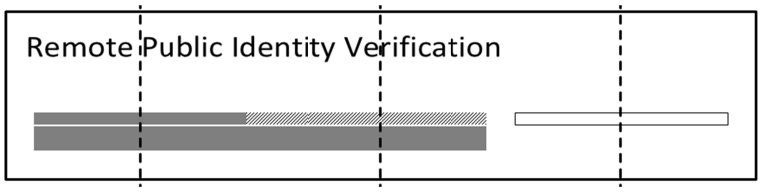

Figure 4-3: Variations of requirement representation

In Figure 4-3 (taken from Figure 4-7), the first (thin bar) requirement statement is applied to the leftmost profile. However, in addition, the presence of a hashed bar, on the same horizontal level, applied to the central profile, indicates that a requirement statement, controlling the same assurance component, but with additional restrictions, is to be applied in this category.

Finally, the presence of an open, unfilled bar, on the rightmost profile in Figure 4-3 indicates that this requirement must *not* be applied to this profile. In general, there is variation as to how these hashed 'modifier' bars are applied and the reader should refer to the assurance texts for clarification in these areas.

Finally, Figure 4-4 represents 2 assurance profiles (the vertical dashed lines) for *both* of which alternate paths of *either* 4 or 2 requirement statements must be fulfilled for the component specification Subject Key Pair Generation.

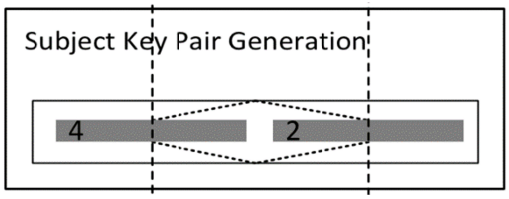

Figure 4-4: Alternate requirement choices

4.2. IGTF Levels of Authentication Assurance

The Interoperable Global Trust Federation (https://www.igtf.net/) publishes an assurance framework specifying requirements for 4 assurance levels: ASPEN, BIRCH, CEDAR and DOGWOOD. The IGTF website introduces these profiles as describing -

> *"… a technology-agnostic assurance level that represent the IGTF consensus on achievable trustworthy authentication seen from both the relying party point of view as well as being a feasible level for identity service providers to achieve for a variety of scenarios."*

In the diagram below, each of the 4 profiles is associated, by the vertical dashed-lines with a set of requirements under the given headings, taken from the framework text. At the lower end of the dashed lines the corresponding 4 PKI Implementation Names are given –

> *"… In terms of a single linear scale, relying parties have often considered authorities compliant with ASPEN (PKI implementation: SLCS), BIRCH (PKI implementation: MICS), or CEDAR (PKI implementation: Classic Secured) to be similar in terms of assurance level, and authorities compliant with DOGWOOD (PKI implementation: IOTA) to be different. In this document, several aspects are separated and relying parties may find more fine-grained controls."*

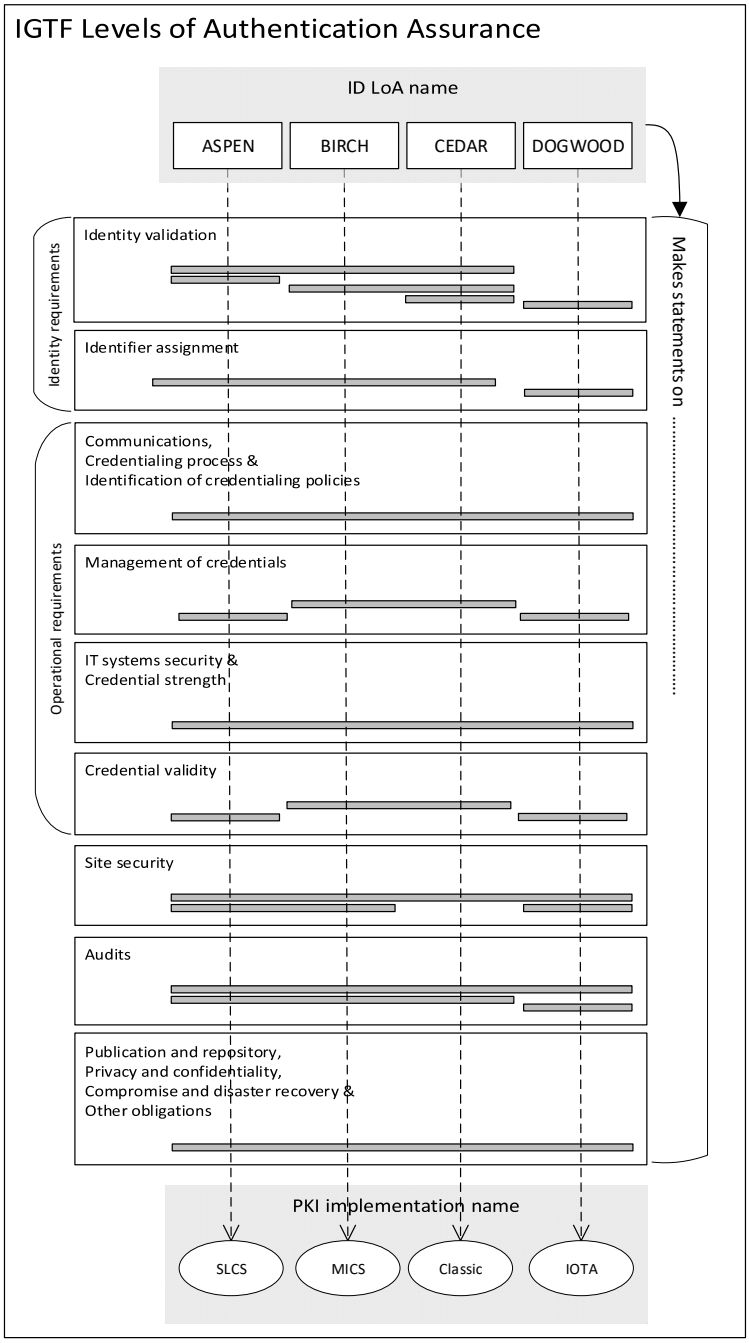

Figure 4-5 IGTF Levels of authentication assurance

4.3. REFEDS Assurance Framework

As discussed in the preceding chapters, the REFEDS Assurance Framework adopts a different approach to assurance specification, and this is reflected in the resulting diagram (**Error! Reference source not found.**). Three component attibutes of identifier uniqueness, id-proofing and attribute quality and freshness are combined with an external specification for authentication strength (REFEDS Authentication Profile being one of https://refeds.org/profile/sfa or https://refeds.org/profile/mfa).

In order to "*serve the RPs seeking for simplicity*" (as stated in section 4 of the REFEDS Assurance Framework Wiki page[1]), these components can be combined to form named profiles Cappuccino and Espresso.

The RAF specification, in itself, makes no statements to requirements which must be fulfilled for Id-proofing 'levels' – Low, Medium and High. Rather, the specification explicitly references relevant component sections in the IGTF, eIDAS and Kantara frameworks. This relationship is shown in Figure 5-1.

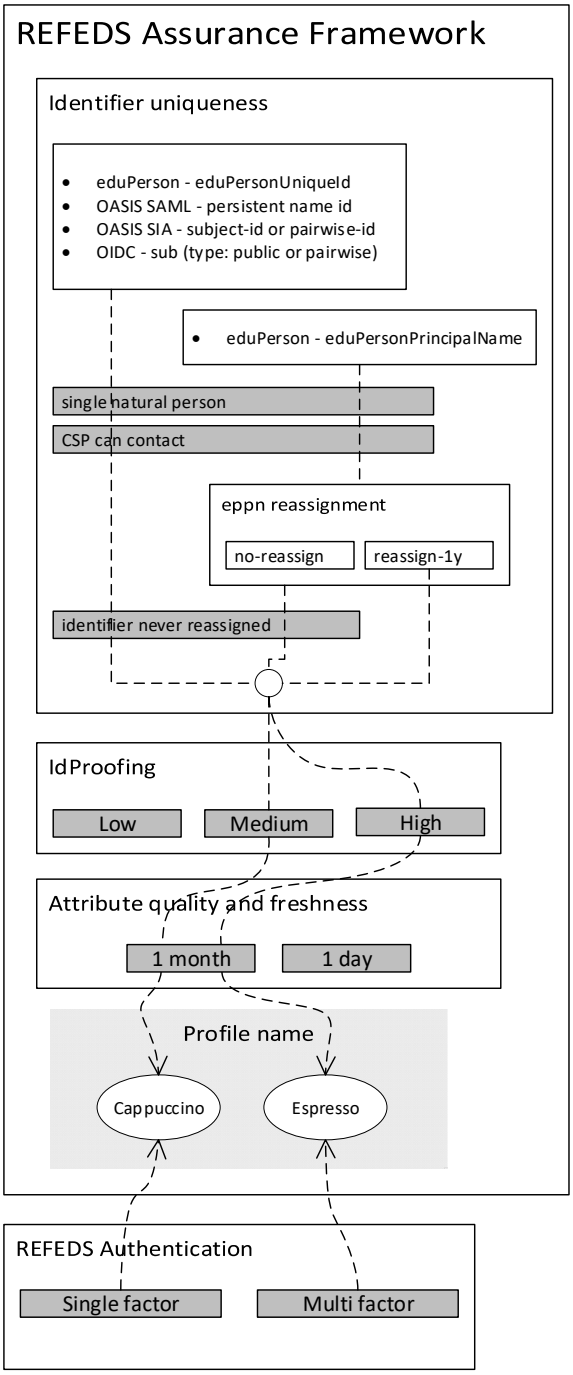

Figure 4-6 REFEDS assurance framework

4.4. Kantara Identity Assurance Framework

The diagram of the Kantara Identity Assurance Framework (shown below in figure 4-8) represents just one part – the Operational Service Assessment Criteria (KIAF-1420) – of the Kantara Initiative's (https://kantarainitiative.org) comprehensive Identity Assurance Framework. Detailed specifications governing assessment and assessor qualifications for other, substantial elements.

[1] https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0)

The diagram Figure 4-7 shows how the four defined Kantara assurance levels (labelled 1 to 4) are specified.

Figure 4-7: Kantara Assurance framework

4.5. eIDAS assurance framework

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (http://data.europa.eu/eli/reg/2014/910/oj), requires (Art 8.3) that "*minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified*". These technical specifications are defined in Regulation 2015/1502 (https://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj) and this has been used to generate the diagram below.

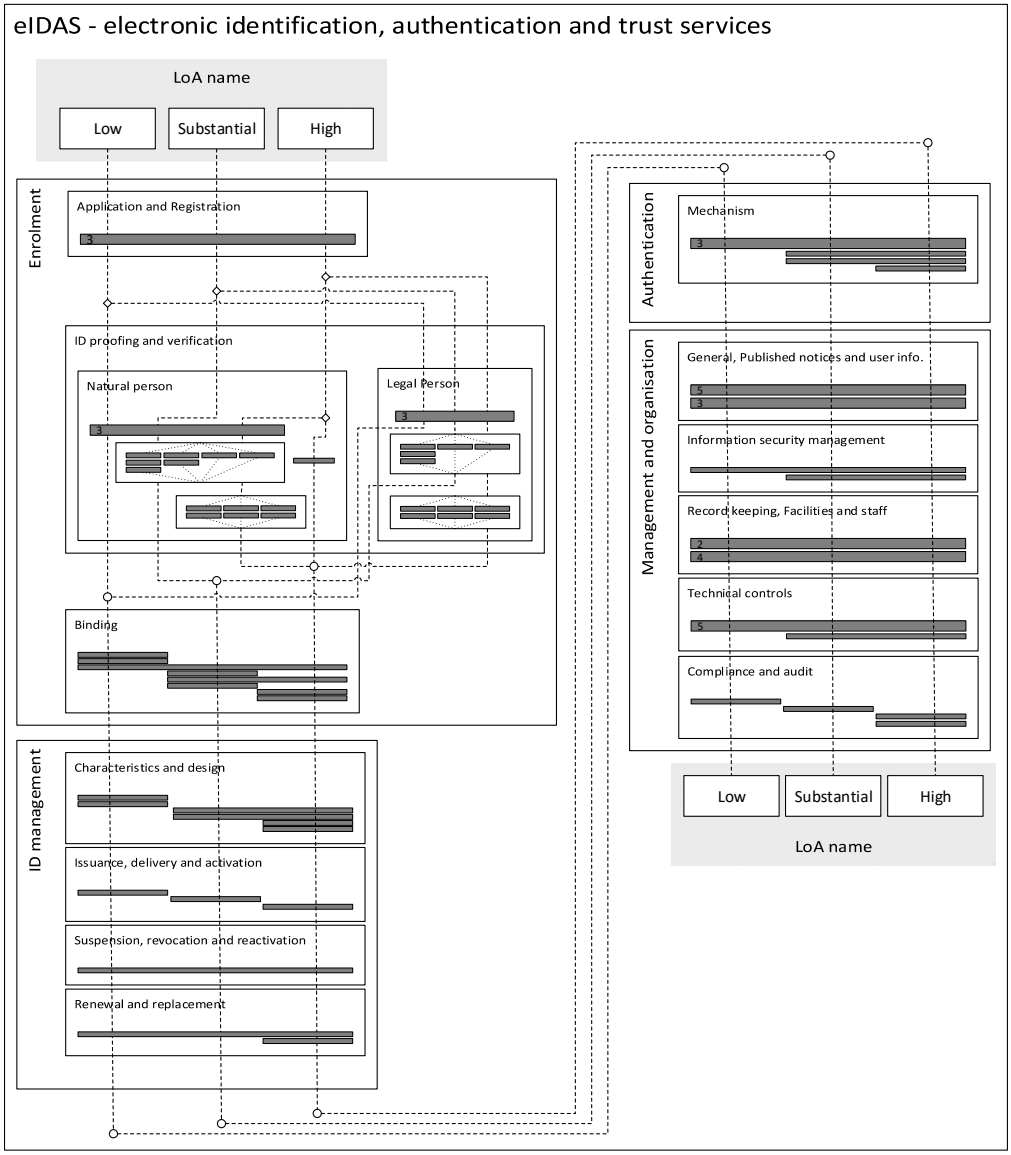

Figure 4-8: eIDAS assurance framework

5. Comparing assurance frameworks

As described in chapters 2 and 3 above the assurance frameworks described in this document display differences related to their origins, target audience and applicability within an audiences' domain of implementation. The diagrams in chapter 4 provide a reference against which both the overall structure and the relative complexity of the individual frameworks might be judged. Again, as described above, it is clear that Kantara KIAF-1420 provides the most 'comprehensive' framework – at least in terms of numbers of component requirements. eIDAS technical specifications, with narrower scope and foundation on the regulatory framework, appears, in complexity of implementation, between Kantara and the 'simpler' IGTF. The latter being able to leverage assumptions about the risk profiles of the relying parties and credential provider organisations by which the framework is implemented. The RAF appears, by this analysis, somewhat of a 'hybrid' framework, this being explicit in its use of the other frameworks' Id-proofing components. This relationship is shown in Figure 4-1 where the RAF Id-proofing specifications of Low, Medium and High form the centre of a 'spaghetti' overlay linking the RAF specification to the relevant, external, KIAF, eIDAS and IGTF framework elements.

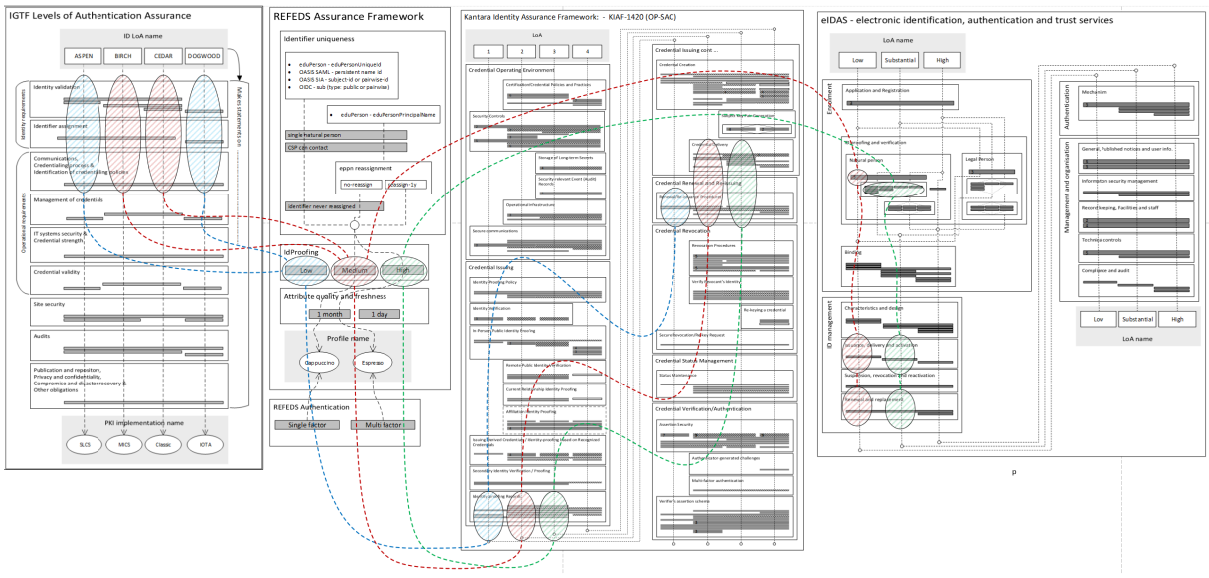

Figure 5-1: Comparing assurance frameworks

For example, the RAF Medium Id-Proofing specification could be fulfilled by compliance to any of

- *either* of the highlighted IGTF BIRCH or CEDAR profile elements under 'Identity and Operational Requirements' or
- KIAF LoA 2 'Identity-proofing Requirements' *and* 'Credential Delivery and Renewal/Re-issuance Procedures' or
- eIDAS LoA Low 'ID Proofing and Verification for a Natural Person' *and* 'Issuance, delivery and activiation' *and* 'Renewal and replacement'

The RAF framework thus provides an explicit ‘equivalence’ between the Id-proofing requirements of the 3 profiles, as shown in the diagram, and at least as far as the RAF authors’ analysis. This is a single component of what can be seen is a much larger, complex landscape. As mentioned above more generalised comparison and gap analysis must be left for future investigation.

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.