Making Identity Assurance and Authentication Strength Work for Federated Infrastructures

Jule Anna Ziegler[1], Uros Stevanovic[2], David L. Groep[3], Ian Neilson[4], David P. Kelsey[4], and Maarten Kremers[5]

[1]Leibniz Supercomputing Centre, Garching near Munich, Germany
[2] Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany
[3]Nikhef, Amsterdam, the Netherlands
[4]UKRI STFC Rutherford Appleton Laboratory, Didcot, UK
[5]SURF, Utrecht, the Netherlands

Abstract

In both higher Research and Education (R&E) as well as in research-/ e-infrastructures (in short: infrastructures), federated access and single sign-on by way of national federations, operated in most cases by NRENs, are used as a means to provide users with access to a variety of services. Whereas in national federations institutional accounts, e.g. provided by a university, are typically used to access services, many infrastructures also accept other sources of identity: provided by "community identity providers", social identity providers, or governmental IDs. In order to assess and communicate the quality of identities being used and authentications being performed, so called Level of Assurance (LoA) frameworks are used. Because sophisticated LoA frameworks like NIST 800-63-3, Kantara IAF 1420 or eIDAS regulation are often considered too complex to be used in R&E scenarios, the REFEDS Assurance Suite, a more lightweight approach, has been developed. To select an appropriate assurance level, Service Providers need to weigh risks and potential harms in relation to the kind of service they offer. However, the management of risks is often implicitly assumed and little or no guidance to determine the appropriate assurance level is given. In this paper, first, common LoA frameworks and their relation to risk management are investigated. Following that, their components are compared against the REFEDS Assurance Suite using a graphical representation. The focus of this paper lies in providing guidance and best practices based on example scenarios for both Service Providers to request the appropriate REFEDS assurance level, as well as for Identity Provider operators on how to implement REFEDS assurance components.

1 Introduction

The world is getting increasingly interconnected. More and more of people's lives are becoming virtual, sometimes unexpectedly more so [1]. At the cornerstone of the interaction with social web services, e-commerce, corporate governance, research and education [2], among others, stand digital identities. Identities and thus identity management (IdM) play a crucial role in many applications [3], and the move to the online world brings new risks [4]. Therefore, the question of *who* is using, accessing or managing resources or services is critical and relies on the ability to securely and reliably use digital identities. In this paper we focus mostly on authentication, or *who* is accessing services, and not on authorization, which is concerned with *if* and *what* kind of access should be granted. The distinction between both terms is important in Federated Identity Management (FIM) - they are not interchangeable, and they do denote different concepts.

There are many definitions of identity, and while social scientists are mainly interested in the qualities that make a person (and the question of what is identity and what constitutes identity) [3], here we consider digital representation of identities including their usage and elements. There are two important components of an identity, namely *sameness*, i.e. the person today is the same as the person yesterday, and *uniqueness*, every person is distinguishable from another [4]. As will be elaborated later, these two concepts are interlinked. The International Telecommunication Union Standardization Sector (ITU-T) defines identity as "*representation of an entity in the form of one or more information elements which allow the entity(s) to be sufficiently distinguished within contex*" [5]. Additionally, ITU-T states that "*for IdM purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts*" [5]. This definition is a general one, and it may extend to objects or entities, i.e. not people. In this paper, we focus on personal identities, and information relating to people, not objects.

Identity Management involves managing users' identity attributes [6]. It consists of "*processes, policies and technologies to manage the complete lifecycle of user identities across the system and to control the user access to the system resources by associating user rights and restrictions*" [7]. ITU-T NGN identity management framework (Y.2720) [8] states that these processes and procedures are used for:

- assurance of identity information, e.g., identifiers, credentials, attributes;
- assurance of the identity of an entity, e.g., users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects;
- enabling business and security applications.

In the above, the concepts of *identifier*, *attribute*, and *credential* have been introduced. An *identifier* is a text string used to, typically uniquely, identify a person or a subject. An *attribute*, or an *attribute assertion*, is a claim made by someone, e.g. an Identity Provider (IdP), that a particular identity, e.g. a person, possesses a specified quality [6]. A *credential* is an "*identifiable object that can be used to authenticate the claimant is what it claims to be*" [9]. For example, a digitally signed attribute assertion can be considered to be an authentication credential [6].

As stated, the assurance and the reliability of the information is paramount. In Federated Identity Management (FIM), an "*arrangement can be made between multiple organizations that lets subscribers use the same identification data to obtain access to the secured resources of all organisations in the group*" [9]. The benefits are [6]:

- Single-Sign-On (SSO) capabilities, providing ease-of-use for the users across multiple services
- scalability by enabling the Service Providers (SPs) to offload management of user attributes and credentials to Identity Providers (IdPs)
- security by moving the checking and management of identity closer to the authoritative source

However, as science is becoming ever more collaborational, crossing institutional and geographical boundaries, the challenges of identity, authentication and authorization are also

growing. Whereas in Research & Education (R&E) users expect the ability to use their institutional accounts, in research/ e- infrastructures (short: infrastructure), other identities provided by social or governmental IdPs may also be used. Each of these may have different requirements for the management of information of their users. They may require different authentication methods, e.g. passwords versus tokens, or have different security requirements while using the same methods (e.g. different password strengths). Accuracy requirements about the users' information may vary, or for the timely updates of the users' information. Hence, the quality of such information is central to FIM concepts and to the establishment of trust between participating entities. For these reasons, the *Level of Assurance (LoA)*, or the expression of the level of confidence about the users' information is necessary [6].

LoAs vary in their meaning and definition, for example NIST [11], eIDAS [12] introduce their own definitions and procedures. What will be demonstrated as part of this paper, however, is that they are all related, since the focus of their considerations is the same, i.e. the quality of users' information. Chadwick [6] states two main points in expressing LoA, a *registration* LoA, or what was the procedure of registering a user and the accuracy of the user's information, and an *authentication* LoA, or how *secure* is the corresponding authentication credential, which will both be considered and expanded in this paper. One of the challenges of today's LoA concepts, however, is that little guidance is given to the service provider to self assess, what kinds of risks and harms their service is exposed to through reliance on federated identities, and therefore, decide how can they be treated by selecting the appropriate assurance level. This is why our main objective in this paper is to present genuine use cases and provide guidance on how to weigh risks, harms and their impact in relation to which services are being offered and how they are used. Furthermore, guidance on how to implement REFEDS Assurance components is given. Hence, the intended target audience of this paper is less the end user but rather operators, such as IdP operators, SP operators and proxy or infrastructure operators. The reference framework, i.e. the assurance components and values, being used for these purposes, is the REFEDS Assurance Suite, which will be presented in Section 3. The structure of the paper is as follows:

- An introduction to relevant assurance frameworks and how they relate to risk management will be given (Section 2)
- The REFEDS Assurance Suite covering both identity and authentication assurance will be presented (Section 3)
- A Graphical Comparison of identity assurance components for various assurance frameworks will be shown (Section 4)
- Guidance, examples and current best practices for both Identity Providers as well as Service Providers will be given (Sections 5 and 6)
  - Section 5 provides guidance for Identity Providers by means of a campus use case to implement REFEDS Assurance components
  - Section 6 provides guidance for Service Providers to select the appropriate assurance level by considering assets and risks associated with accessing services and resources
- A conclusion and outlook to required research will be given (Section 7)

2 Assurance Frameworks and Risk Management

"*The nice thing about standards is that you have so many to choose from.*"[1]

Risk management is commonly used as the basis for having authentication controls and assurance requirements for services, even if the form in which risk management is introduced and its recognisability as a formal process may differ. In its explicit form a risk management framework is integrated into an existing and mature overall management system, as discussed in e.g. ISO 31000, addresses specific information security risk management in an actionable way (NIST SP800-30), or is adopted as-is from external sources, e.g. due to regulatory requirements, contractual requirements, or because of participation in consortiums and federations. In other organisations, the risk management may be either intuitive or ad-hoc, based on implicit contextual factors such as personal trust, or reflect the personal risk perception of the people involved. In either case, the mitigation of risk will involve adopting controls that

[1] Andrew S. Tanenbaum [Computer Networks, 2nd ed., p. 254.#]

address risk treatment, where "*selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived*" [10].

There are many ways in which the risk assessment may be translated into a set of information security controls. Information security management systems, such as ISO27000, by taking the information assets as central elements, tend to describe identity assurance, identity vetting, and authentication assurance as implementation measures to address user access management. For example, ISO27002 puts identity verification predominantly in the context of "management of secret authentication information of users" while targeted frameworks for identity, credential, and access management may provide more in-depth discussion of the balance between risk and the elements of identity assurance and authentication strength. A multitude of such frameworks exists, with NIST SP 800-63, the Kantara Identity Assurance Framework (IAF), and the eIDAS regulation being the most well known in the public sector. The research and academic sector are familiar with frameworks such as the REFEDS Assurance Suite, presented in Section 3, and the IGTF assurance profiles.

Assurance frameworks tend to reflect the organisational context from which they originate. The initial two versions of **NIST Special Publication 800-63**, issued in 2006 and 2011 respectively, strongly reflect the US Federal government memorandum **OMB M-04-04**, which introduced four assurance levels as the basis to which risk management should refer when determining the appropriate assurance and authentication controls. Although some guidance is provided in the memorandum by way of examples, the actual risk assessment is very much implicit, and reflects the then-perceived requirements of the US Federal government. Given the relative dominance and early publication, it was OMB M-04-04, via NIST SP 800-63 versions 1 and 2, which drove much of the subsequent frameworks, including the initial versions of Kantara IAF Assurance Levels. The eIDAS framework emerging from the EU Regulation on electronic identification and trust services for electronic transactions in the internal market similarly reflects e-government needs and defines three comprehensive assurance levels [12]: low, substantial, high, albeit adapted to the European context.

The **Kantara IAF (KIAF)**, an industry-recognized identity assurance standard, is based on the previously described NIST standards with the initial KIAF-1200 version reflecting NIST SP 800-63 ver. 1 requirements (four LoA) and the latest version (KIAF-1430 and -1440, Dec. 2019) reflecting NIST SP 800-63 ver. 3 requirements respectively. The requirements derived from NIST are encapsulated in so-called Operational Service Assessment Criteria (SAC) being used for different Trust Marks. For general organizational conformity Kantara added additional requirements derived from different sources and best practices to establish, amongst others, a "*risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community.*" [13]. However, no further guidance on how to map these risks to appropriate assurance levels (part of SAC) is given.

eIDAS (Electronic Identification, Authentication and Trust Services) is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. The regulation allows European Member states to integrate their electronic identification schemes. The regulation marks three levels of assurance: Low, Substantial and High. The minimum technical specifications and procedures for assurance levels are noted down in an implementation regulation [14]. Guidance for risk assessment is provided by the member states, such as the guide from the Dutch government [15].

The **IGTF assurance profiles** [19] evolved from a single-level assurance model defined during the initial establishment of federated IT infrastructures for research from 2001 onwards. They thus assumed as a basis the implicit risk assessment associated with distributed computing and storage services spanning multiple administrative domains, such as the WLCG, EGI, and PRACE federated infrastructures. Distinct assurance profiles were added in response to changes in service portfolio, risk exposure, as well as risk appetite of the federated infrastructures that leverage the IGTF assurance profiles for authentication and identity assurance, to encompass four non-hierarchical "profiles" combining technology-agnostic identity and authentication assurance elements.

Recognising that, fundamentally, two models exist for measuring trust - either the level-based approach discussed before, or a local "calculation" of the effective assurance within the application itself - Johansson and Richer in 2015 proposed the decomposition of the levels of assurance into the components "identity proofing" and "primary credential usage", "primary credential management", and "assertion presentation" [16]. Instead of a scalar assurance level, a "**Vector of Trust**" (VoT) would be conveyed, with each element of the

vector qualified either in terms of hierarchical strength, or in descriptive categories with ambiguous ordering. A similar approach, although with less flexibility, was adopted by NIST in 2017 in the 3rd version of the SP800-63 "Digital Identity Guidelines", which decomposes assurance into Identity Assurance Levels (IAL), Authentication Assurance Levels (AAL) and Federation Assurance Levels (FAL), wherein FAL defines technical and procedural guidelines for federated identity systems and the assertions used therein.

The component-based approach, by providing more expressiveness, permits better matching of assurance elements to information security controls derived from a specific risk assessment. In particular, the presence of additional and compensatory controls in the system may permit some elements to be addressed outside of the identity assurance and authentication strength requirements. Specifically, the unbundling of identity proofing and authentication credential management allows the selection of different sources of authenticator and identity attributes, as long as a unique binding link between the two can be provided. Also, research use cases, as a minimum, often require a unique, non-reassigned identifier, but do not necessarily need actual identity data [17].

Granularity and decomposition of assurance into various components does, however, increase the complexity of trust processing by a relying party or service provider, thereby potentially adding a measure of risk (e.g. because of mistakes in either implementation or processing logic of access control). As a result, the component-based frameworks frequently define "profiles" that target either a baseline or a commonly-occurring set of controls, or are working towards such profiles. Frameworks that do not explicitly define such profiles, e.g. NIST SP 800-63-3, need an additional specification to enforce either a per-service or a per-organisation risk assessment, such as set for the US Federal government in memorandum M-1917, or to provide such in other ancillary documents.

It is interesting to note that, regardless of the complexity of the underlying components of assurance, the number of assurance profiles in any framework tends to be between two and four. The IGTF assurance profiles define, effectively, two (its profiles ASPEN, BIRCH, and CEDAR differ only in underlying technology, and only DOGWOOD is materially distinct), eIDAS provides three (low, substantial, and high), OMB M-04-04 four (1-4, providing little, some, high, or very high confidence) and REFEDS - which is described more precisely in the following section, uses three levels. In line with what is seen in other sectors where choices between alternatives have to be made, e.g. in marketing, offering a limited set of options, e.g. three, appears optimal [18].

3 REFEDS Assurance Suite

Most of the frameworks, including RFC 8485 and NIST SP 800-63-3, retain a single component for identity assurance. These are "identity proofing" and "identity assurance level", respectively, with RFC 8485 allowing for non-hierarchical definition of this component. The REFEDS community, considering federated research and academic use cases in the broad sense, similarly split identity assurance and authentication strength, into the **REFEDS Assurance Framework (RAF)**, the **Single Factor Authentication (SFA)** and the **Multi Factor Authentication (MFA) profiles**, respectively [20, 21]. Yet, by also considering the individual, orthogonal RAF identity assurance components, i.e. Identifier uniqueness, ID proofing, Attribute freshness, and allowing them to be individually assertable, it extends conventional frameworks by adding granularity that federated service providers can use as risk mitigation control. In response to general organizational uniformity and security posture, some baseline expectations for identity providers were also defined.

In the following, the three individual identity assurance components of RAF will be described in more detail:

- **Identifier uniqueness** (ID unique) permanently binds a digital identifier to a single person. The identifier must not be shared with, or re-assigned to, any other person or entity at any time. Therefore, uniqueness properties are defined which require, amongst others, that a "user" must be a single natural person and can also be contacted (Uniqueness property 1 and 2). Given these properties, shared or functional accounts and automated bots or robots are not within the scope of RAF. This criteria may also be seen as a core criteria, as reliance on the remaining two components would be questionable if the identifier uniqueness was not fulfilled.

- **ID proofing and credential issuance, renewal and replacement** (in short: ID proofing) relies on the presence of a unique identifier and defines three ascending levels (low, medium, high) to "prove" the identity of a real world user, while also addressing credential lifecycle management: the initial association of a credential with a user and subsequent renewal and replacement practices. Instead of defining new criteria, the ID proofing part references existing practices such as Kantara, eIDAS or IGTF.
- **Attribute quality and freshness** controls the continued validity of a user's affiliation with their home organization. Therefore, it differentiates between two values where the value of the component will accurately reflect the status of the affiliation within one day or within 31 days of a user's departure. This requirement, however, does not define the organizational procedure for the departure of employees, but is the maximum allowed latency before which technical systems must be updated.

Considering the component-based, orthogonal character as highlighted above, and the possibility to process individual assurance components, different combinations of the components and their values are reflected within two identity assurance profiles. Besides no assurance at all, the **REFEDS Cappuccino profile** represents moderate assurance, i.e. unique identifier, with medium ID proofing and attribute freshness of one month, whereas the **Espresso profile** constitutes a stronger assurance profile by upgrading to high identity proofing (see Figure 1). However, further profiles, which may be needed to satisfy use cases requiring more stringent freshness of attributes, e.g. 1 day, may be added, if needed.

The authentication assurance components, i.e. REFEDS SFA and MFA, are deliberately decoupled from the identity assurance profiles, making the whole Assurance Suite flexible and customizable in order to qualify for different use cases and to satisfy different risk mitigation strategies. In terms of combining the authentication assurance components with REFEDS Cappuccino and Espresso, a simple recommendation to use a similar strength of identity and authentication assurance is provided, i.e. Cappuccino in conjunction with SFA and Espresso with MFA respectively. But, always depending on the use case and the risks involved, one has to evaluate whether other combinations of identity and authentication assurance would be more meaningful.

Regarding the authentication assurance, the SFA profile defines criteria for both authentication factors, as well as for associated processes when using a single factor. For the former, it defines quantitative thresholds regarding the minimum authentication secret length and the maximum secret life span for different authentication factor types, together with high level requirements to ensure threat protection through cryptographic protection of secrets and protection against online guessing attacks. The latter main criteria, that of processes when using SFA, defines rather high level, organizational requirements for dealing with lost authentication factors taking into account human-based or knowledge-based procedures but also requirements for backup authenticators.

The overall requirements of REFEDS SFA define a security baseline and thus are seen as minimal requirements which can be exceeded, if necessary, for example, by existing federation specific or institutional policies. To achieve this, the SFA profile uses a mixture of state-of-the-art technical requirements, e.g. minimum secret length, and high-level, risk-based requirements. By referencing risks and threats, and not defining strict requirements, identity providers are enabled to decide on their own whether, for example, online guessing attacks are mitigated by rate limiting or by using any other means.

As already stated, all components of the REFEDS Assurance Suite are decoupled, which implies that REFEDS MFA is *not* built on top of REFEDS SFA but is rather seen as an interoperability profile. In particular, this means that compliance to REFEDS MFA can be asserted independently from the SFA profile, so that each factor used for a multi factor authentication does not necessarily have to qualify to the requirements defined in the REFEDS SFA profile.

The MFA profile uses a similar, high-level, approach to determining three main criteria, requiring that the authentication factors being used must be of different types and independent of each other to prevent mutual access in order to mitigate single factor only risks like phishing or offline cracking.

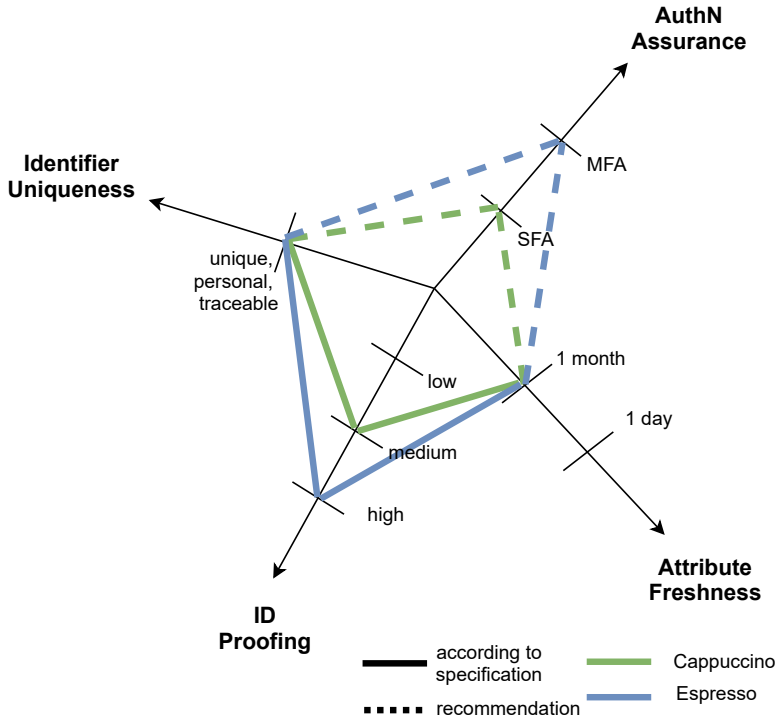


Figure 1: REFEDS Assurance Suite Components and Profiles

4 Graphical Comparison of Assurance Frameworks

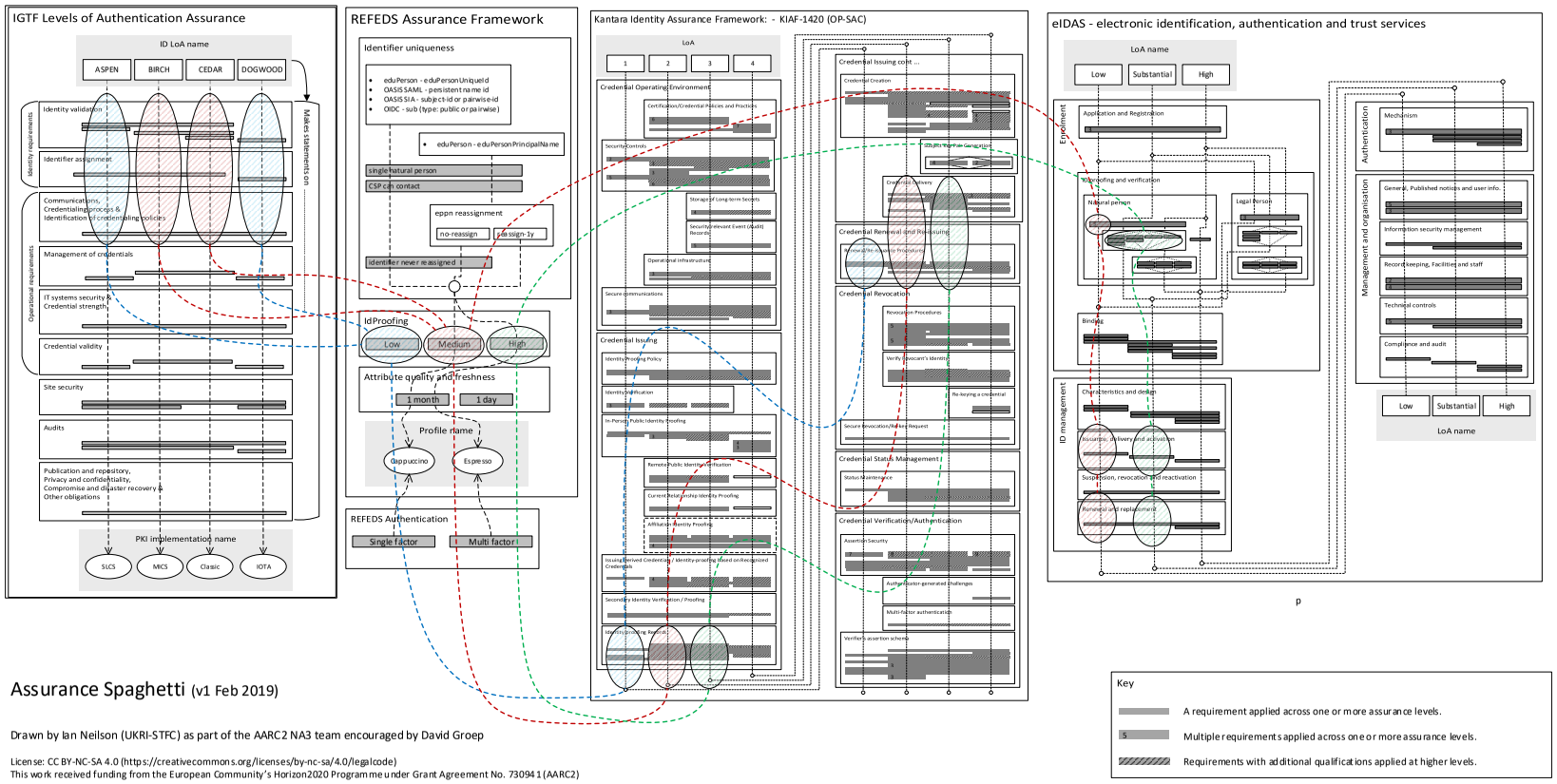
In this section four common assurance frameworks are presented in a graphical format with the aim of assisting the reader in understanding the relationships, similarities and differences between the frameworks, at a high level, which may otherwise be difficult to evaluate from the texts themselves. Such an understanding forms a crucial part of the decision service managers take as to which frameworks may be appropriate to use in mitigation of the risks arising from user authentication and authorization.

Similarly, service providers, in performing the risk assessment for their service, must understand the context in which identities issued under a particular framework were intended to be used. Their decision to allow, or bar, identity assertions from a specific framework, which may be presented at the service's authentication interface, should be influenced by this understanding.

In 2019 the AARC Policy Development Team published its guideline *AARC-I050 - Comparison Guide to Identity Assurance Mappings for Infrastructures* [22]. This document identified differences in the implicit assumptions about trust present in the Kantara, eIDAS, IGTF and REFEDS assurance frameworks described in previous chapters. It illustrated some of these differences using a graphical representation of the frameworks with an overlay showing the way in which the REFEDS Assurance Framework leverages the ID proofing components of the other frameworks.

The assumptions identified in AARC-I050 generally arise from historical evolution of the framework and the context within which the identities, and hence the frameworks, are used. For example, AARC-I050 states that "*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*" [22]. Hence, it identified that the issuer of an IGTF identity may not have been subjected to the same external, 3rd party audit process of, say, a Kantara-based identity. However, use of such an identity in the context of a research environment, where the service provider does have a relationship with IGTF via their own national representative on the peer network of IGTF authorities or through their project's relying party representation, may be appropriate.

Figure 2 below is the summary diagram from the final chapter of AARC-I050 which presents the four assurance frameworks considered in the document together with the ID



Assurance Spaghetti (v1 Feb 2019)

Drawn by Ian Neilson (UKRI-STFC) as part of the AARC2 NA3 team encouraged by David Groep

This work received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2)

Figure 2: Graphical Comparison of Assurance Frameworks [22]

proofing overlay. Readers are referred to AARC-I050 for a detailed description of the graphic method employed. However, in a general sense, each framework is divided vertically into a number of assurance "levels" and horizontally by groupings of component requirements placed upon an identity arising from a given "level". For instance, eIDAS "levels", Low, Medium, and High, represented by vertical dotted lines, pass through varying requirements such as "ID management – Issuance, Delivery and Activation", represented by horizontal bars within an open box. What, exactly, the component requirements are is not addressed in this representation beyond their title, but the resulting "bird's eye" view does give an overview of the complexity and breadth of the frameworks presented as a whole.

Consideration of exactly which aspects of identity assurance are important to a service provider when approaching their service risk assessment, and which of those aspects can be adequately addressed by a framework - such as REFEDS RAF, leveraging parts of alternative frameworks used in an appropriate context - is necessary for a proper understanding of, and control of, risk arising from identities used for authentication.

5 Identity Providers: Implementation of REFEDS Assurance Components and Profiles

In this section we will have a closer look at the bases on which an Identity Provider may provision the REFEDS assurance components. On purpose, the requirements do not specify how they are to be implemented, allowing flexibility and variety in processes between institutions and countries. Yet many institutions in R&E share common characteristics, so some different ways are considered here, showcased by means of the campus scenario in subsection 5.1.

5.1 Campus Use Case

Adding the capability to assert identity and authentication assurance is likely to require a change in processes and procedures, many of which in the R&E environment are the result of a slow organic evolution of both processes and systems. The potential need to review, or even change, such processes and systems understandably triggers a reluctance on the side of the entities affected to participate in any assurance scheme. However, when it comes to assurance, it is worth noting that the underlying aim of the REFEDS Assurance Suite is not to request new attributes or new processes, but is rather about expressing an assurance level based on identity and authentication related processes that are *typically already in place*. Thus, any existing process can be employed as a basis to define the per-user assurance level and assert it publicly towards relying parties. But as the REFEDS Assurance Suite does, on purpose, not define any audit process of assigning specific responsibilities, a challenge of the specification is that every IdP is advised to self-assess their compliance against the specification.

Within this subsection, campus IdPs will be assessed, in a high-level way, by addressing the components defined within Cappuccino and SFA. This high-level assessment can then be used as a reference for an IdP considering asserting assurance attributes, and thereby increase their confidence in any self-assessment.

To structure any self-assessment we recommend to start with considering the different roles, e.g. affiliations, and assess each of them individually. Generally, when it comes to campus IdPs the most common roles used in a federated context are *student* and *staff/employee*. Due to space constraints, we only further elaborate these two roles here, although other roles, such as guest researchers or contractors, should not be neglected during self-assessment. Roles and accounts, such as group accounts, not being able to use federated services at all can be excluded here. So the primary task constitutes the discovery of roles and whether or not there are differences in their processes and practices, e.g. if the identifiers of students are handled differently from those of employees or not.

The "ID/unique" component of RAF may be considered the most important one since it binds the identifier to the unique human user and acts as the anchor both for the other assurance elements and for the relying parties to associate roles, groups, or capabilities to their users. ID/unique decomposes into four uniqueness requirements, with the first two of them stating that the user is a single natural person and can be contacted by the IdP. In on-campus scenarios a user identifier is, by its nature, undoubtedly bound to a single natural person, typically combined with some kind of in-person checks and provisioning of

address or mobile number. While fulfilling these requirements, this might not necessarily be the case in scenarios where users are able to register remotely. In off-site enrolment of users, satisfying these requirements will require some additional controls, which could include solving Captcha, behavioural interaction analysis, e.g. interacting with a web page which could show the Acceptable Use Policy and require scrolling and confirmation, and verification of contact information such as verifying the existence of an e-mailbox and the ability to respond to a challenge e-mail. However, special care needs to be taken with the reassignment practices, requirements numbered 3 and 4, as some campuses may reuse existing identifiers after a certain period of inactivity or a cool-down period. This is common practice for e-mail addresses. For the identifiers to be considered of sufficient quality to satisfy uniqueness, they need to be non-reassignable, or provided and considered with additional information that would then satisfy the uniqueness requirement[2].

In addition to having unique identifiers for users, the Cappuccino profile imposes some requirements to verify the identity of users (ID Proofing). While ID Proofing is often perceived as difficult to implement, especially when higher controls such as liveness checking or even in-person verification are needed, existing procedures for vetting the identity of students, and especially of employees, frequently already meet or even exceed the medium ID proofing requirements of Cappuccino. For example, in European countries, students are typically enrolled in-person and show their official ID document, or are enrolled based on strong authentication through governmental e-ID schemes. In comparison, the Cappuccino, medium level identity proofing, profile does not necessarily require in-person identity proofing to happen on enrolment as it also allows for remote vetting based on liveness checking. This checking is combined with a choice of compensatory controls that could include validation of government-issued photo-ID documents, verification of address-of-record, or an ongoing relationship during which any of these have been previously validated and that has been protected by strong credentials [13, 19].

If special cases exist, such as foreign student enrollment, these need to be taken into account which could lead to different assurance levels being asserted for users in the same role, depending on the initial vetting level, or some class of users being excluded from assurance assertions. However, this will usually affect only a small fraction of the user population, and should not be considered an obstacle in providing assurance for the user population at large.

The requirement on "Affiliation Freshness" originates from the fact that some SPs may want to link access rights with roles and hence, this defines a maximum latency by which IdP internal systems must reflect affiliation changes. The internal delisting procedures may provide hints here. It is also advisable to check the existence of top level policies, which of course also applies to the other REFEDS criteria, as participating in federated infrastructures, such as national identity federations or research infrastructures, is commonly coupled with similar requirements, some of which may be even more stringent. For example, to obtain the member status "Advanced" in the German identity federation, IdPs are "*obliged to keep user data correct and bring it up-to-date within 2 weeks*" [25]. So those members automatically qualify to assert Affiliation Freshness of Cappuccino which requires one month.

Besides the three core criteria on identity assurance, RAF also specifies basic requirements for operating an IdP. These requirements are derived from the InCommon Baseline Expectations for Identity Providers [26] where further guidance can be obtained.

For moderate assurance, SFA is the recommended authentication profile to combine with the Cappuccino profile. Given that recent standards, such as NIST SP800-63B rev.3 (2017), do not recommend to enforce periodic change of passwords in the presence of other compensatory controls since overly frequent changes have a negative effect on the password quality chosen by the user, REFEDS SFA also omits regular password changes and instead imposes minimum requirements on the secret length, and this is not limited to passwords. However, this is now generally considered as standard practice, and can usually be configured in directory services out-of-the-box; other compensatory controls listed may require specific tooling. To comply with SFA, IdPs are advised to carefully check the quantitative values on minimum secret lengths and the life span of transmitted secrets, especially if backup authenticators and initial secrets are issued as well. In regard to threat protection, IdPs are free to decide how to cryptographically protect authentication secrets at rest and in transit, and how to

[2]To satisfy and assert R&S [20] requirements ePPN [23] value must be non-reassignable, or sent together with ePTID [23]. There are other attributes that satisfy uniqueness, like eduPersonUniqueId [23] or subject-id [24].

protect against online guessing/brute-force attacks. In case of the latter, measures such as to limit the number of attempts or to slow down re-entering of secrets are highly effective. In scenarios where campus IdPs do not involve a service desk to handle the replacement process of lost secrets, they should make sure not to use outdated mechanisms such as only answering a secret question.

To conclude, many IdPs run by universities will already fulfil the core requirements of the Cappuccino profile. When it comes to authentication assurance, attention should be paid to whether the exact values, e.g. quantitative values such as secret length, and the restrictions imposed on the replacement process match. Also, special cases for both identity and authentication assurance need to be considered here. Since performing self-assessments requires allocation of sufficient manpower and time, organizations are advised to follow a role based approach and to start introducing assurance components gradually.

6 Service Providers: From Assets and Risks to an Appropriate Assurance Level

In an ideal world, service providers match the need for identity and authentication assurance with the risk and value of the assets to which access is being granted. It has been convincingly stated that "*Identity assurance is concerned with the proper management of risks associated with identity management*" [27], and Open Science Cyber Risk Profile (OSCRP) [28] differentiates six common science asset categories to assist research projects in identifying their assets and the associated risks to these. Yet, a consistent and integral risk assessment of services is complicated, and often ignored when considering assurance requirements, which are consequently seen as a cost or burden on the service resulting in loss of user base. Therefore, this section will refer to a number of representative use cases in order to guide service providers when selecting appropriate assurance components or profiles.

While, from the perspective of identity providers described in section 5, processes and controls matching the REFEDS Assurance Suite should be assessed to *properly mitigate risks related to the management of identities and authentications*, these processes and controls in turn need to be *understood and carefully chosen by SPs* to ensure they sufficiently mitigate the risks arising from the usage of their services or resources. Also, the interaction between IdP and SP is exclusively reflected by individual REFEDS assurance components and profiles as requested through the authentication mechanism.

Selection of an appropriate assurance level based on assessing risks would typically follow a three-fold approach:

1. Identification of assets and creation of asset inventory
2. Risk assessment for each of the assets
3. Treatment of risks by selecting appropriate assurance components and profiles, as part of a range of security controls, together with acceptance of remaining residual risks

This more formal approach, while potentially resulting in a self-consistent assessment of assurance requirements, is not feasible to implement for service providers who do not have formal asset and risk management processes in place. In lieu of an identification of all organizational assets and an inventory of assets based thereon, it may be sufficient to start self-assessing only those services that rely on external assurance information, and catalogue the purpose and the value of the respective services, their users, and the data contained therein. For example: does the service provide access to data, including adding or modifying data, access to ephemeral resources, such as computing power, or access to equipment, such as microscopes or telescopes? The previously-mentioned Open Science Cyber Risk Profile (OSCRP) assists scientific research projects by differentiating six common science asset categories, namely: Data Assets, Facilities Assets, System and Hardware Assets, Software Assets, Instruments, Intangible and Human Assets.These assets are then further defined in subcategories.

A subsequent choice is whether to assess the service provider as a whole, resulting in a single assurance level for all its services, or whether it would be advisable to assess each service individually, as the assets involved may be different even if, for instance, it is placed behind a common proxy. Alternatively, grouping of services that are sufficiently similar, e.g. a set of

services for ephemeral resources, a set for reproducible data, and a set for sensitive data, can simplify the self-assessment.

One might also assess services in production first, while the services in a development or testing phase can follow later on provided such pre-production services do not contain real data or can impact production systems or users.

To subsequently determine the appropriate assurance level, the result of assessment step 2, it is also important to take into account the service or part of service or transaction that is exposed through federation and not necessarily the whole business process it may support [11]. If a member of a national federation offers, for example, a voting system for students with federated access, only those data that can directly be viewed or modified by the federated users should be assessed, while the offline counting procedure and the backend, where the election results are stored, which of course should be protected too, but through potentially different mechanisms, are out of scope when selecting an appropriate assurance level for those users that will access the system through federated authentication. Depending on the self-assessed criticality of these data, compared with categories of harm listed below, one may require a higher authentication assurance level, e.g. MFA, to access such a voting system, whereas the identity proofing which has been carried out during student enrollment to access a range of other institutional services may be sufficient.

In terms of risk assessment or management (see step 2), we consider the following six core categories of harm from NIST [11] as important, which have been aligned with the purpose of and populated with examples from R&E:

1. Reputational damage and inconvenience
   e.g. loss of trust, whilst trust is of particular importance in federated AAIs
2. Financial loss and liability
   e.g. contractual responsibilities, recovery costs after an incident
3. Harm to assets and operations
   e.g. manipulation/abuse of soft-/hardware
4. Unauthorized release of sensitive information
   e.g. research data, personal or medical data
5. Legal violations
   e.g. due to disclosure of personal data in Europe, violating the EU General Data Protection Regulation, or violations of export control regulations and provisioning of services to entities on a UN proscribed list
6. Personal safety
   e.g. the ability to control research instrumentation outside of its allowed operating conditions, putting local operators at risk, or in tele-medicine in research hospitals

All of the above mentioned risks and harms can and should be considered, and their impact assessed depending on the research field and type of assets involved. In the following discussion, we give two examples that showcase how particular assets can be considered.

When assessing risks, harms and associated impacts of a service providing access to, for example, data assets, the kind of data needs to be further elaborated. OSCRP, for instance, divides Data Assets into Public Data, Non-Public Data, Internal Data, Documentation, Accounting Information, For Approved Access Only. Non-public data related to humans, such as medical, health, or biological data are, for example, subject to legal regulations (harm number 5). Furthermore, access to this data is to be strictly protected against unauthorized processing or alteration (harm numbers 3 and 4).

This is why ELIXIR, a distributed research infrastructure for life-science information and BBMRI-ERIC, a research infrastructure for biobanking, have strong requirements regarding who accesses and processes biological data, and for which purposes. These requirements are multifold and involve identity assurance, strong authentication, and information freshness. In the case of BBMRI-ERIC, access to data is mostly given on the project basis, and projects are tied to the institution. Therefore, for both BBMRI and ELIXIR, freshness of the institution information is paramount and both have strong requirements on the organizations to reflect changes in the affiliation immediately, i.e. when a person is leaving the organization. To minimize risks of unauthorized access, strong authentication is required, which may include MFA. ELIXIR uses a step-up service to address these challenges. The service provides MFA, and could be used to raise an ID proofing value, via an additional vetting procedure where the user must register a phone number on which to receive an OTP credential, with further TOTP

capabilities [30]. Furthermore, ELIXIR's Membership Management Service has additional capabilities to "enhance" assurance information about the user, such as "bona-fide" researcher, e.g. by vouching for one researcher by another, or by a specified group registration process. Currently, they are piloting a new capability for remote identity vetting using SiSuID[3].

The WLCG (Worldwide LHC Computing Grid project) has a stated purpose "*to provide global computing resources to store, distribute and analyse*" [29] the data generated by the Large Hadron Collider (LHC) at CERN. The volume of data during LHC Run2 was in the range of 50-80 PB/year. While the risks of unauthorized read access to data is small as data are mostly publicly available, thus minimizing harm numbers 4 and 5, further risks remain, especially harm numbers 1 and 3. The impact of unauthorized destruction or creation of data would be significant, and may lead to loss of valuable data, or the incorrect attribution of a scientific discovery. The potential impact of abusing the WLCG computing resources, such as for mounting a distributed denial of service attack or the storage of illegal or copyrighted material, is also potentially considerable as WLCG is world's largest computing grid [29]. Therefore, when examining the treatment of risks and derived assurance levels, we observed that WLCG opted for medium identity assurance combined with strong credentials[4], though typically without MFA, for most of its use cases. Since the early 2000's, WLCG has operated a X.509 based AAI, with the underlying trust fabric being based on policies controlled by the IGTF, including, amongst others, Authentication Assurance Profiles [19]. These profiles regulate all main components of REFEDS Assurance Suite, i.e. identity uniqueness, ID proofing and credential handling, and attribute quality and freshness, in addition to regulating the credential strength, where the assurance profile of choice is typically IGTF BIRCH. In the future, WLCG AAI infrastructure will switch from the X.509 based authentication and authorization to the OAuth2 [31] token based. In doing so, the requirements in terms of identity assurance and credential strength do remain the same [32].

After discussing representative use cases from R&E, including Life Science (ELIXIR, BBMRI-ERIC), High Energy Physics (WLCG) as well as national federations, we think it is a good practice, when determining the appropriate assurance level, to consider medium as the reference level for R&E services for both ID assurance and authentication assurance components, i.e. REFEDS Cappuccino and SFA. The rationale behind this recommendation is that, since most of the R&E services provide access to some sort of restricted assets, from an identity assurance perspective, a more reliable identity than a fully self-asserted one is typically needed, combined with moderate/medium user authentication, e.g. a combination of username and password.

To identify the assets to be protected, the classification of OSCRP serves as a good starting point. The identified assets can then be tested against the six core categories of harm derived from NIST. A potential outcome could be that a provider of high performance computing resources, System and Hardware Assets, does not identify exposure to any high impact risk in any of the categories and thus decides to require Cappuccino and SFA, whereas if, in addition, databases containing sensitive information would be connected to the system, a higher assurance level would be appropriate. Another example, when deciding to decrease from medium, based on a pragmatic assessment of risks, lowering the authentication assurance to lower-than-SFA would result in acknowledging no authentication assurance at all, i.e. users do not need to be authenticated to access the service. This might be appropriate for use cases where access to public data or documentation is provided. In all cases, it is strongly advised to document, and periodically review, all considerations and decisions being made.

7 Conclusion

In this paper, we have highlighted the increasing demand for identity and authentication assurance within the Research and Education (R&E) space. Several existing assurance frameworks have been investigated, including well-known standards such as NIST Special Publication 800-63, Kantara Identity Assurance Framework and the EU regulation eIDAS. Following that, their elements have been compared against the REFEDS Assurance Suite, which is the focus

[3] https://sisuid.com/

[4] With X.509 being called as "strong authentication" because of one or more aspects of the authentication protocol, e.g. stronger than username/password because proof of possession of the private key does not require the private key to be transmitted to the other entity.

of this paper and represents an assurance framework originating from R&E. The REFEDS Assurance Suite, by following a component- and profile-based approach, comprises three individual specifications, the REFEDS (Identity) Assurance Framework (RAF), the REFEDS Single Factor Authentication Profile (SFA) and the REFEDS Multi Factor Authentication Profile (MFA). As the main contribution of this paper, guidance has been provided for using the REFEDS Assurance Suite, both from the perspective of Identity Providers, when assessing internal processes and procedures against the REFEDS requirements, as well as from the Service Provider perspective on how to select appropriate assurance components or profiles. As the latter is closely linked with the identification of assets and the management of risks, we have proposed a lightweight approach by considering assets defined within the Open Science Cyber Risk Profile to test against six core categories of harm derived from NIST.

As an outlook to further work, R&E services of a similar nature can be grouped in to "families of related services" whose shared risk assessment can be met with a common assurance profile – a method used, for example, by the Dutch government to set the Assurance levels for authentication for electronic government services [15]. We plan to share first experiences and family groupings after sufficient uptake of the REFEDS Assurance Suite.

Acknowledgments

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2), 730941 (AARC2) and 856726 (GN4-3). The authors wish to thank the project members of GÉANT, AARC2 as well as the REFEDS community for helpful discussions and feedback to continuously improve the work presented in this paper.

References

[1] Wikipedia: *COVID-19 pandemic*.

[2] P. J. Windley, *Digital Identity: Unmasking identity management architecture (IMA)*, O'Reilly Media, Inc., Sebastopol 2005.

[3] U. Glässer, M. Vajihollahi M, *Identity Management Architecture*, in: Yang C., Chau M., Wang JH., Chen H. (eds) *Security Informatics. Annals of Information Systems*, vol 9. Springer, Boston, MA, 2010.

[4] G. B. Ayed, *Digital Identity Management*, in *Architecting User-Centric Privacy-as-a-Set-of-Services*, pp. 57-95, 2014.

[5] International Telecommunication Union, *X.1250: Baseline capabilities for enhanced global identity management and interoperability*, 2009.

[6] D. W. Chadwick, *Federated identity management*, in *Foundations of Security Analysis and Design V*, pp. 96-120, 2009.

[7] D. V. Thuan, *Identity Management Demystified*, in *Identity Management. telektronikk 3/4.07*, pp. 11-18, 2007.

[8] International Telecommunication Union, *NGN identity management framework. Recommendation ITU-T Y.2720*, 2009.

[9] Broeder Daan et al., *Federated identity management for research collaborations*, 2012.

[10] International Standards Organization (ISO), *ISO 31000 Risk Management*, lines 541-542

[11] NIST 800-63-3, *Digital Identity Guidelines*, 2017.

[12] European Parliament, Council of the European Union, *Regulation No 910/2014* (eIDAS), 2014.

[13] Kantara, *Kantara 1410 SAC*, 2020.

[14] European Commission, *Commission Implementing Regulation (EU) 2015/1502*, 2015.

[15] Forum Standaardisatie, *Assurance levels for digital service provision*, 2017.

[16] J. Richer, L. Johansson, *RFC8485 - Vectors of Trust*, IETF, 2018.

[17] M. Linden, D. Groep, D. Pöhn, T. Coulouarn, W. Pempe, H. Short, Recommendations on Minimal Assurance Level Relevant for Low-risk Research Use Cases (AARC-G013), 2015.

[18] D. Kuksov, J. M. Villas-Boas, *When more alternatives lead to less choice*, in *Marketing Science 29.3 507-524*, (2010)

[19] D. Groep, *IGTF Levels of Authentication Assurance*, 2016.

[20] REFEDS, *REFEDS Specifications*.

[21] J. A. Ziegler, M. Schmidt, M. Linden, *Improving Identity and Authentication Assurance in Research & Education Federations*, in *Security and Trust Management, 15th International Workshop*, 2019.

[22] I. Neilson, D. L. Groep, *Comparison Guide to Identity Assurance Mappings for Infrastructures (AARC-I050)*, 2019.

[23] Internet2/MACE, *eduPerson Object Class Specification*, 2016.

[24] S. Cantor, *SAML V2.0 Subject Identifier Attributes Profile Version 1.0*, OASIS, 2019.

[25] DFN, *Degrees of Reliance within the DFN-AAI*.

[26] InCommon, *Baseline Expectations for Trust in Federation*.

[27] Y. Beres, A. Baldwin, M. Mont, S. Shiu, *On Identity Assurance in the Presence of Federated Identity Management Systems*, in *Proceedings of the 2007 Workshop on Digital Identity Management*, 2007.

[28] Trusted CI, *Open Science Cyber Risk Profile*.

[29] WLCG, *Worldwide LHC Computing Grid Website*.

[30] M. Linden, *User Instructions for Multi-Factor Authentication*, 2019.

[31] D. Hardt, *RFC 6749 - The OAuth 2.0 Authorization Framework*, IETF, 2012.

[32] EGI, Policy on Acceptable Authentication Assurance, 2017.