Guidelines on stepping up the authentication component in AAIs implementing the AARC BPA

Guidelines: AARC-G029

Published Date:	30-03-2018
Revision:	1.0
Document Code:	AARC-G029
Work Package	JRA1

Authors:	Mischa Salle (NIKHEF), Nicolas Liampotis (GRNET), Davide Vaghetti (GARR), Christos Kanellopoulos, GEANT), Mikael Linden (CSC), Shiraz Memon (FZJ), David Hübner (DAASI), Alessandro Paolini (EGI), Nils van Dijk (SURFnet), Uros Stevanovic (KIT), Marcus Hardt (KIT), Peter Solagna (EGI)

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

Abstract

This document provides guidelines on step-up of the authentication component. It covers requirements and implementation recommendations, describes a proposed authentication step-up model, and outlines related work and documentation.

Table of Contents

Table of Figures

1 Introduction

1.1 Background

These Guidelines are part of a suite of recommendations that jointly support the AARC Blueprint Architecture (BPA) and the Policy Best Practices produced by the AARC project. These recommendations are meant to support the use of federated identities in research infrastructures and generic e-infrastructures and the interactions between IdPs/SPs and proxies deployed therein. They further enable research collaborations and e-infrastructures to offer services by providing a well-defined and aligned set of policies across research and e-infrastructures.

The *AARC Blueprint Architecture* [AARC-G012_BPA] is a main result of the AARC project towards to enable the deployment of interoperable AAIs for research collaborations and e-infrastructures. The BPA defines generalised architectural patterns found in existing AAI solutions. The cornerstone of the BPA is the SP-IdP-Proxy, which passes along authentication information about the user to services. This SP-IdP-Proxy component may trigger additional actions for a user to "step-up its authentication", i.e. provide a stronger level of authentication, should this be required by a relying SP. For this reason, the SP-IdP-Proxy plays a central role in the present document.

The driving requirements for this document stem from work in the AARC1 project, where the requirements of e-infrastructures, research infrastructures and research communities were analysed together with the respective AAI architects and implementers.

The engagement with the research communities, showed that authentication step-up (i.e. two-factor authentication) is more urgently needed than elevating other components of assurance (such as identity vetting or authentication freshness). This document therefore focuses on elevation of the "authentication" component (as defined in current assurance frameworks REFEDS Assurance Framework (RAF) [RAF], Vectors of Trust (VoT) [VoT], or NIST *Digital Identity Guidelines* [NIST_SP-800-63-3]); elevation of the identity vetting assurance is out of scope for this document.

1.2 In this Document

The body of this document covers requirements (Section 2) and implementation recommendations (Section 3); a proposed authentication step-up model is described in Appendix A, and related information is outlined in Appendix B.

1.3 Target Audience

The target audience includes implementers of SPs that require multi-factor authentication (MFA), implementers of MFA services and developers/operators of SP-IdP-Proxies.

1.4 Terminology

To be specific, and to avoid confusion, in the context of this document the term “step-up authentication” or “authentication step-up” refers to the elevation of the authentication component of an assurance framework.

1.5 Scope

As mentioned above, these guidelines focus on elevation of the authentication component, specifically, the technical aspects of its implementation. While step-up of the authentication component has implications for many related aspects, such as “How to ensure the second factor is delivered to the right entity?” or “How can I describe different levels of authentication assurance?”, discussion of these is outside the scope of this document.

1.6 Standards and Protocols

This document aims to encourage implementers of authentication step-up services to follow existing approaches and patterns, such as using standardised protocols, as closely as possible, to ensure that step-up services can be useful in multiple scenarios and that individual components can be replaced by others.

Even though SAML terminology is used extensively in the document, the recommendations are also valid for OIDC and the flows are protocol agnostic.

2 Requirements

Authentication step-up is a general requirement for multiple communities. The documents referenced in Appendix B include use cases from those communities; these often describe requirements very specific to their use case and some level of abstraction is required. The general use case is of users, such as citizen scientists, that try to authenticate to resources using credentials with low assurance. Whilst some resources are available to them, some others may require more secure authentication methods. Authentication step-up is then needed to improve the original authentication strength of those users. Unfortunately, many IdPs fall short of providing information about assurance components. Reasons for this include unavailability in general at the IdPs, the cost of delivering higher levels of authentication, the complexity of signalling authentication levels, and missing standards to do this in an internationally uniform way.

A related point is that some communities have users that do not have home institutions (or the home institutions do not have an identity provider that releases appropriate attributes); these users may authenticate initially using for instance social media or self-registered accounts, and may need step-up authentication when accessing more security sensitive resources. See also *Milestone MJRA1.2: Design for Deploying Solutions for "Guest Identities"* [AARC1-MJRA1-2].

As there is a trend among service providers towards using OpenID Connect (OIDC), a sensible approach is required to make sure step-up works for both SAML and OIDC. From a high-level point of view, services need to meet only a few criteria to ensure this.

First of all, service providers need to be able to express the requirement for the user to be authenticated with a second factor. Typically a service will redirect a user to the IdP the user came from with the request to authenticate the user with a second factor. In the context of the AARC BPA, this IdP is the SP-Idp-Proxy. In return, the SP needs to be provided with information on how a user was authenticated (e.g. whether a second factor was used or not).

3 Implementation Recommendations

This section summarises implementation recommendations based on the lessons learned – from work and implementations such as those described in Appendix B – regarding authentication step-up services, and on the results of many discussions on the matter. The recommendations address both SAML and OIDC for implementing the step-up flows.

The recommendations are as follows:

1. The SPs and the SP-IdP-Proxy may agree via a policy that only users that authenticated with multi-factor authentication (MFA) be passed onwards to those SPs. In this case, SPs may rely on the SP-IdP-Proxy to ensure that multi-factor authentication has taken place as it is presented in the flow described in Appendix A, without further communication.

2. When there is no policy configuration in the SP-IdP-Proxy for a given SP, then the SP should be able to signal the requirement for multi-factor authentication (MFA) towards the SP-IdP-Proxy.
   - For SAML: use `AuthnContextClassRef` to require `https://refeds.org/profile/mfa`, as defined in the REFEDS Assurance Framework [RAF] Section 5.1.
   - For OIDC: using a claims request, request the `acr` claim as an essential claim, with the value `https://refeds.org/profile/mfa`. (See REFEDS Assurance Framework [RAF] Section 5.2 and its Appendix B for details and examples.)
3. To convey the information regarding MFA from the SP-IdP-Proxy to the SP, the proxy should, according to RAF:
   - For SAML: use the `AuthnContextClassRef`.
   - For OIDC: use the `acr` claim.

4. If an IdP declares to support MFA, it should be preferred instead of reverting to a third-party service for the following reasons:
    - Home-IdPs are close to the users, which makes ID vetting and hardware-token issuance more efficient, cheaper and more secure.
    - Users benefit from using the Home-IdP-MFA because they only need one hardware token, not one each for potentially several MFA services.
    - Home-IdPs should use one standard to convey the assurance information, if possible. The REFEDS Assurance Framework references the REFEDS SFA and MFA profiles (https://refeds.org/profile/mfa) [REFEDS-MFA].
    - Services should support either OIDC or SAML in the way recommended in this document.
    - Users benefit from using the Home-IdP-MFA, because they only need one hardware token, not one for potentially several MFA services.
5. Once an SP obtains MFA to strengthen the authentication assurance component it should use reasonable session lifetimes based on its security requirements.
6. Proxies should communicate the freshness of authentication (e.g. SAML `AuthenticationInstant`) to their SPs. Where there are multiple authentication factors, different authentication times can be communicated. It is recommended that the oldest of these be used.
7. Implement the step-up process in as few steps as possible, to keep the process user-friendly.
8. The GDPR requires minimal data storage and high transparency of processes to the user. Therefore, step-up services should make it clear to the user what personal data is required and why.

4 Conclusions

Step-up of the authentication component is a complex task. This document has given guidance on how a straightforward approach may be implemented. It has focused on the technical aspects, giving recommendations for the implementation. A model for authentication step-up, defining the flows in which a user is involved, is described in Appendix A; a summary of related work and key documents is provided in Appendix B.

Open questions include whether the SPs can and should query their IdP (i.e. the SP-IdP-Proxy) for capabilities supported, and whether they can communicate the need for MFA in their metadata, so that additional redirects can be avoided. Potentially, policies can be installed at the SP-IdP-Proxy that require MFA for users before they are sent to an SP. This would probably be done only in cases where the SP cannot be modified to support requesting MFA.

Furthermore, the number of redirects could be reduced if IdPs were announcing their capability to support MFA in their metadata. This would allow the IdP-SP-Proxy to determine whether to use a dedicated MFA service or to contact the IdP to provide MFA.

Finally, it should be noted that both SAML and OpenID Connect provide standard mechanisms for representing the certification status of an IdP regarding its conformance with the requirements of an identity assurance framework (see SAML V2.0 Identity Assurance Profiles Version 1.0 [SAML-AP-V1] and OpenID Connect Discovery Specification Version 1.0 [OIDC-CDS-v1]. However, this cannot be expected at the moment. These open issues will be addressed in future iterations of the guidelines.

Appendix A Authentication Step-Up Model

This appendix describes a model for authentication step-up to support communities that require multi-factor authentication (MFA). The model is based on an analysis of several approaches referred to in Appendix B. However, none of these approaches has taken into account the AARC Blueprint Architecture (BPA). The model described here therefore extends one approach slightly, so that it works well with, and properly integrates MFA into, the BPA.

A.1 Proposed Flows

To realise the step-up setup, two separate flows are defined:

- One for registering a user that does not yet have a second factor (which is not strictly part of the authentication step-up service).
- One for the actual step-up, to use this second factor.

The two flows were originally designed for the AARC – Life Science AAI pilot [AARC-LSAAI]. However, they were designed to be generic, so that they can be adapted by future AARC pilots. For more information about the context in which they were developed, please see *Second factor authentication component for the Life Science AAI* [SFA-LifeScAAI].

A.1.1 Registration Flow

In a proxied architecture, such as the Life Science AAI being piloted in the AARC project, the authentication step-up service is connected to the SP-IdP-Proxy. Figure A.1 below shows an example flow for registering a user to such a community step-up service.

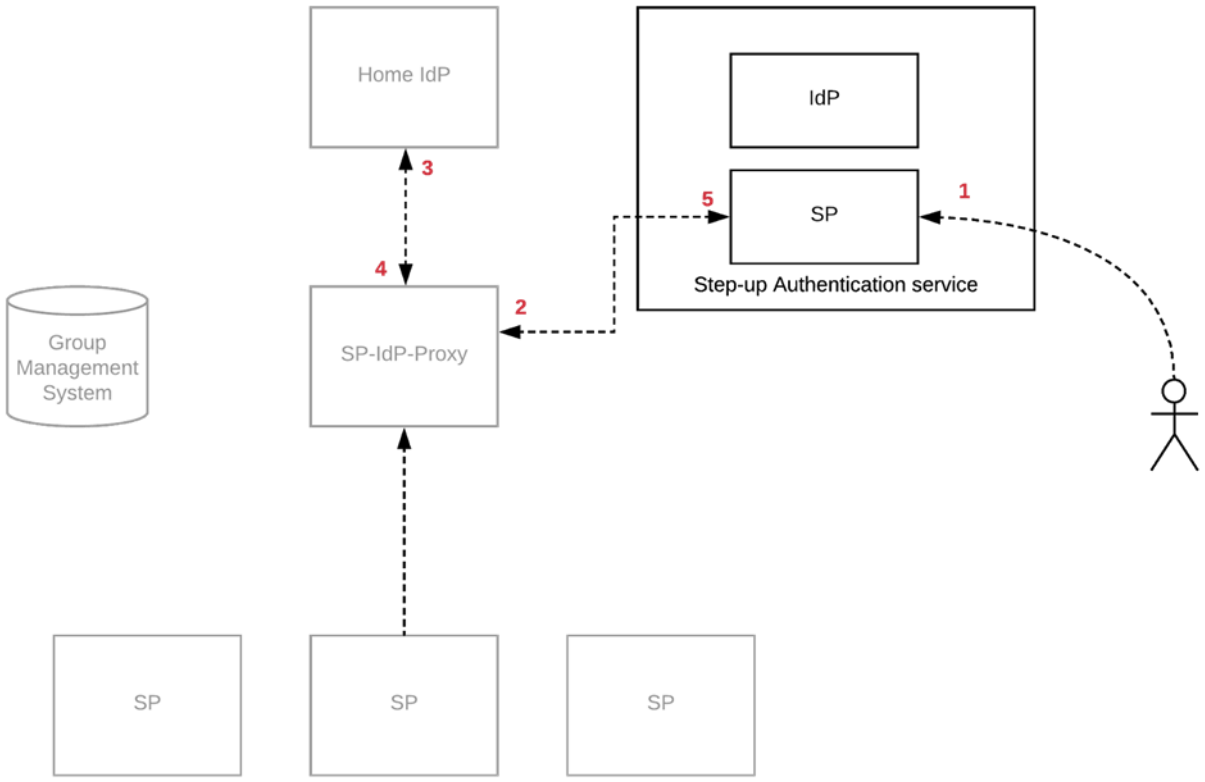

Figure A.1: Registration flow for authentication step-up service connected to an SP-IdP-Proxy

Mandatory Steps

1. The user visits the authentication step-up service and starts the registration process.
2. Assuming the step-up service is a community-run service, the user is then redirected to the community SP-IdP-Proxy.
3. The SP-IdP-Proxy checks to see if there is an active authenticated session for that user. If not it redirects the user to their IdP where the user is authenticated.
4. The user comes back to the SP-IdP-Proxy with the attributes released from their IdP.
5. The SP-IdP-Proxy bundles the relevant attributes and redirects the user back to the authentication step-up service. Apart from the common user attributes, the community identifier is also provided so the step-up service can link second-factor information to that identifier.
6. The user is authenticated and can now register and manage the devices that they want to use for step-up authentication.
7. For all successive authentications, the step-up service can now issue a Level of Assurance statement towards the SP-IdP-Proxy (see Section A.1.2).

Optional Steps

8. The collaborative organisation (CO) wants to vet the just-registered second factor of the user in the context of the CO.
9. The user starts the token vetting in the context of the CO by making a request to a specific URL of the step-up service, where the user authenticates using the token they want to get vetted.
10. A vetting workflow is started which allows the step-up-service to validate the user's token and identity.
11. The user is registered with a specific token.
12. For all successive authentications, the step-up service issues a Level of Assurance statement (different from that in Step 7) towards the SP-IdP-Proxy.

Please note that the task of linking a second factor to a user that is already registered at the SP-IdP-Proxy is a complex one and is outside the scope of this document. Please refer to the documentation referred to in Appendix B (specifically, the analysis of MFA registration alternatives in [ELIXIR-MFARegAlt]) for more extensive discussion on that topic.

A.1.2 Authentication Flow

As already mentioned in Section A.1.1, in a proxied architecture such as the Life Science AAI the authentication step-up service is connected to the SP-IdP-Proxy. Figure A.2 below shows an example flow for the authentication step-up process using MFA.

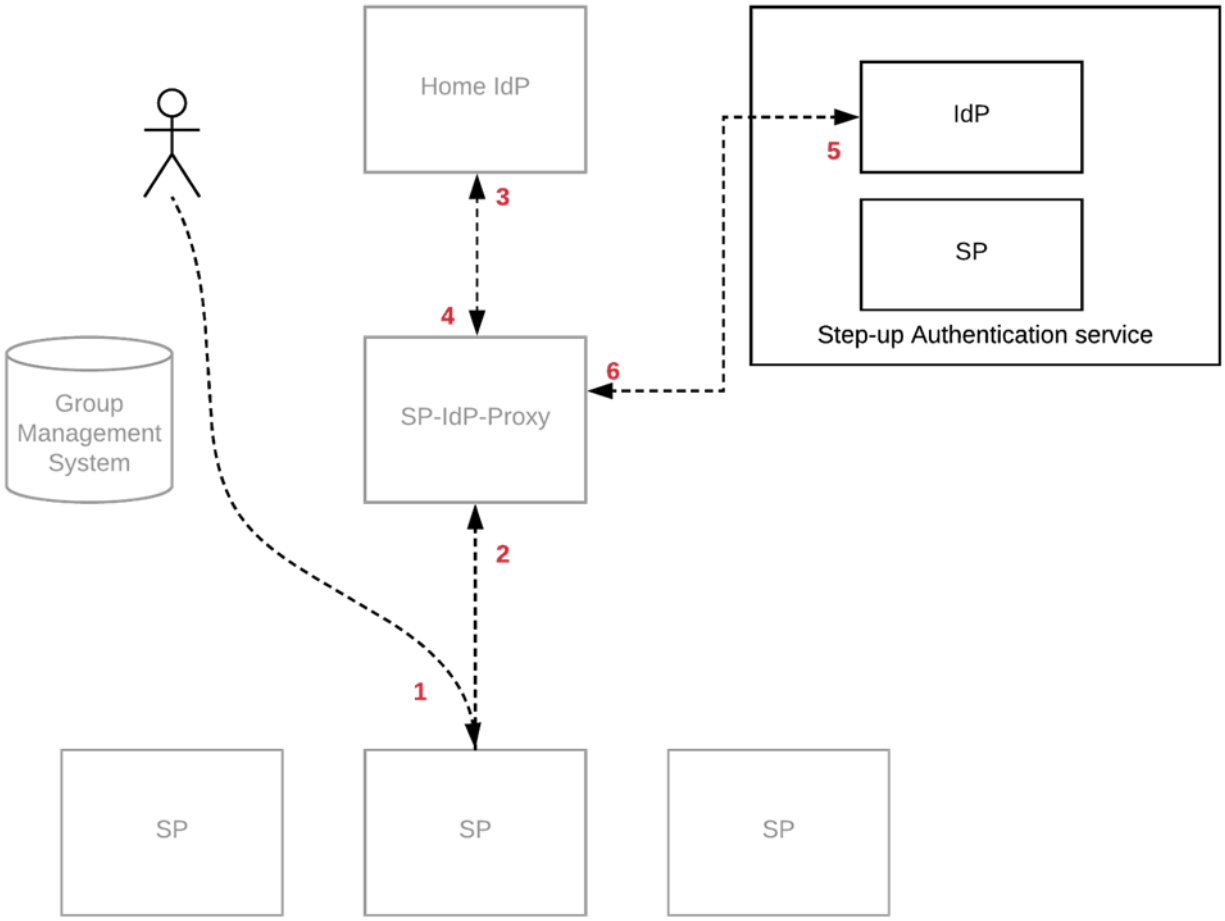

Figure A.2: Authentication step-up process using MFA

Mandatory Steps

1. The user accesses a service provider (SP) that requires second-factor authentication.
2. The SP redirects the user back to the SP-IdP-Proxy. The SP can either signal this requirement to the proxy, or the proxy can have a predefined configuration indicating that the service requires a second factor.
3. If there is no active session for the user, the SP-IdP-Proxy authenticates the user at their IdP.
4. The user is redirected to the SP-IdP-Proxy and now has an active session.
5. The SP-IdP-Proxy requests authentication of the user with a second factor, and sends the unique identifier for the user to the step-up service.
6. The user authenticates using one of their available second factors and is then redirected back to the SP-IdP-Proxy, with information about which factor has been used.
7. The SP-IdP-Proxy redirects the user back to the service provider and signals (e.g. in accordance with the REFEDS Assurance Framework) [RAF] that the user has used MFA.

Alternative Flow

An infrastructure or community may prefer to use Home-IdP-MFA attributes. This requires an alternative flow, outlined below. In this flow, the SP-IdP-Proxy uses MFA from the IdP, if the IdP can provide it; alternatively, it uses a step-up service such as the one described above. The description of the steps is intentionally high level, because discussions in this field are still ongoing.

1. The user accesses a service provider (SP) that requires second-factor authentication.
2. The SP redirects the user back to the SP-IdP-Proxy. The SP can either signal this requirement to the proxy, or the proxy can have a predefined configuration indicating that the service requires a second factor.
3. If there is no active session for the user, the SP-IdP-Proxy authenticates the user at their IdP. The SP-IdP-Proxy requests MFA from the IdP, but signals that a single factor would also be sufficient.
4. If the user is authenticated with multiple factors at the IdP, the SP-IdP-Proxy can redirect the user back to the service, signalling that the user has used MFA (=> Step 7).
5. If the user is not yet authenticated with two factors, the SP-IdP-Proxy requests, using a unique identifier for the user, authentication of the user with a second factor (from the step-up service, of course).
6. The user authenticates using one of the available second factors and is then redirected back to the SP-IdP-Proxy, with information about which factor has been used.
7. The SP-IdP-Proxy redirects the user back to the service provider and signals that the user has used MFA.

Appendix B Related Information

Several groups in different contexts either are or have been working on topics related to those presented in this document, i.e. assurance itself, evaluation of assurance components and various aspects of an assurance component. Their work, and key documents, are listed below.

- The *AARC architecture team has defined a terms and definitions document* that captures and defines terms used in the context of AARC [AARC-JRA1-Terms].

- The GÉANT group analysed the *Technical Architecture Options for Providing Step-Up Authentication (and Assurance Levels)* [GN-ArchiOptions], which are:

  - "Proxy Approach" (this should not be confused with the SP-IdP-Proxy of the AARC Blueprint Architecture, though it might be combined with it). This approach assumes that the MFA service itself is a dedicated proxy that directs the user to their home IdP for the initial authentication and handles the second factor itself. This proxy may be used as an additional IdP by SPs, in cases where multi factor authentication (MFA) is required.

    Two implementations exist:

    — Haka MFA [Haka-MFA], which describes two flows:

      - SP-initiated flow: SP -> MFA -> IdP ("Proxy Approach").
      - IdP-initiated flow: SP -> IdP -> MFA.

    — SURFconext Strong Authentication Service [SURFconext], which also describes two flows, of which the first is a "Proxy Approach".

  - "SAML Attribute Authority Approach", in which a SAML attribute authority (AA) is employed to provide MFA information about a user to SPs that require it.

  - "Dedicated Two-Factor IdP Approach", which defines a dedicated IdP to which users are sent to provide their second factor, after they have first secured the standard SAML authentication with their home IdP. This equates to the IdP-initiated flow in the Haka implementation [Haka-MFA] and to the second flow in the SURFconext Strong Authentication Service [SURFconext]. In contrast to the "Proxy Approach" above, this requires SPs to be modified, so they can support the dedicated step-up service (such as an additional IdP).

- AARC and the GN4 project have prepared a concise document on *Second factor authentication component for the Life Science AAI* [SFA-LifeScAAI], which lists requirements collected from the Life Sciences community and describes two example flows for authentication assurance elevation.

- The AARC2 Architecture Team works on account linking and has produced *Guidelines for evaluating the combined assurance of linked identities* [AARC-JRA1-3a-Link].

- Close collaboration with the ELIXIR project (which is one of projects in the Life Sciences community) has yielded deeper insight. ELIXIR provided a set of requirements as well as their *Roadmap for Step-up Authentication* [ELIXIR-Roadmap] which is based on their analysis of MFA registration alternatives

[ELIXIR-MFARegAlt]. The user flow for subscribing to the MFA is described in their *User Instructions for Multi-Factor Authentication* [ELIXIR-UserMFA].

- Assurance frameworks categorise the field and define multiple profiles, each specifying values for (some of the) different assurance components, to define precisely how well a user is known. One example is the authentication component. Authentication may indicate a single factor [REFEDS-SFA] or multiple factors [REFEDS-MFA]. This is important in scenarios where general assurance elevation is addressed. For this document, the authors only considered work that defines the overall assurance to be composed by individual components. These are:
    - REFEDS Assurance Framework. An updated version is currently being worked on [RAF]. See also the REFEDS Assurance Working Group page [REFEDS-AssuranceWG].
    - Vectors of Trust IETF draft [VoT-IETF].
    - The third version of the NIST *Digital Identity Guidelines* document [NIST_SP-800-63-3].

Future work will include the definition of a more general flow for raising assurance levels of several assurance components (such as identity vetting). Work-in-progress is being documented in the working draft document *A holistic view on Assurance elevation* [AARC-Holistic]. As mentioned above, these other aspects are covered in *Guidelines for evaluating the combined assurance of linked identities* [AARC-JRA1-3a-Link] (identity vetting) and *Guidelines for combining group membership and role information in multi-AA environments* [AARC-JRA1-4b-Comb] (freshness), albeit not specifically targeting “elevation.”

References

NB URLs featuring the hash character may return an error message when clicked from a Word document. If so, copy and paste the URL into the browser address field.

[AARC-G012_BPA] *AARC Blueprint Architecture*
https://aarc-project.eu/wp-content/uploads/2017/04/AARC-BPA-2017.pdf

[AARC-Holistic] *A holistic view on Assurance elevation*
https://docs.google.com/document/d/1R24xKC-cC7sLyb13Gr2jxKtlA83_qESrkCorT4PTb74

[AARC-JRA1-Terms] *AARC JRA1 Terms and definitions*
https://docs.google.com/document/d/18AllfUKLi90f1odm6hINkQvRljbFhy9lfkY1M447uBQ/edit

[AARC-JRA1-3a-Link] *Guidelines for evaluating the combined assurance of linked identities*
https://docs.google.com/document/d/15gdUGuAMiDVQIC_eEDfA1vy35NKKh47K_Ak5NdBUzcI/edit#heading=h.yk3xnw2c7w37

[AARC-JRA1-4b-Comb] *Guidelines for combining group membership and role information in multi-AA environments*
https://docs.google.com/document/d/1Ysjb0UN9SM5oVQOy7MMNve6A1I7AmkFprdA2Bor5n2Q/edit#heading=h.resxjp3e424c

[**AARC-LS-AAI**] https://wiki.geant.org/display/AARC/CORBEL+LifeSciences+AAI

[AARC1-MJRA1-2] *Milestone MJRA1.2: Design for Deploying Solutions for "Guest Identities"*
https://aarc-project.eu/wp-content/uploads/2016/06/MJRA1.2-Design-for-Deploying-Solutions-for-Guest-Identities.pdf

[ELIXIR-MFARegAlt] *The Multi-Factor Authentication registration alternatives*
https://docs.google.com/document/d/1pq4Emu4NYYc3tUEogV7iPlS1puBy2CP3t_JoeFrNhmM/edit#heading=h.nuioklf1z834

[ELIXIR-Roadmap] *Roadmap for Step-up Authentication*
https://docs.google.com/document/d/1VHVY45WvzxIIcWBf290h-N2OOmgBnZqDcgRJnqksBI0/edit

[ELIXIR-UserMFA] *User Instructions for Multi-Factor Authentication*
https://docs.google.com/document/d/16ObOsMhPTMBVfIKJzbBZvJMhtRI2ZKTf_1gSoCMQXAM/edit#heading=h.efsca0d179cp

[GN-ArchiOptions] *Technical Architecture Options for Providing Step-Up Authentication (and Assurance Levels)*
https://docs.google.com/document/d/1WxF6Ls4svLfUjCTePa6u4DAlR8fTPNU5Gw9KZTnSemE/edit#heading=h.nz193xn90yun

[Haka-MFA] *HAKA Multifactor Assurance*
https://wiki.eduuni.fi/display/CSCHAKA/Haka+MFA

[NIST_SP-800-63-3] NIST Special Publication 800-63, Revision 3, *Digital Identity Guidelines*
https://pages.nist.gov/800-63-3/sp800-63-3.html

[OIDC-CDS-v1] *OpenID Connect Discovery Specification Version 1.0*
https://openid.net/specs/openid-connect-discovery-1_0.html#ProviderMetadata

[RAF] *REFEDS Assurance Framework (working in progress)*

https://docs.google.com/document/d/15v65wJvRwTSQKViep_gGuEvxLl3UJbaOX5o9eLtsyBI/edit#heading=h.s47mvmy5r944

[REFEDS-AssuranceWG] *REFEDS Assurance Working Group*
https://wiki.refeds.org/display/GROUPS/Assurance+Working+Group

[REFEDS-MFA] *REFEDS Multi-factor Authentication*
https://refeds.org/profile/mfa

[REFEDS-SFA] *REFEDS Single Factor (draft document)*
https://docs.google.com/document/d/1ZjpzyYWZhqjbTeIzxX9Vug9Whqb9YEkK29e1FBjL5VM/edit

[SAML-AP-v1] *SAML V2.0 Identity Assurance Profiles Version 1.0*
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.html

[SFA-LifeScAAI] *Second factor authentication component for the Life Science AAI*
https://docs.google.com/document/d/18OfWMXLx88zw6eqgPIyG3zIuyIoWGXc0LMMS57dgyOE/edit#

[SURFconext] https://www.surf.nl/en/services-and-products/surfconext/what-is-surfconext/surfconext-strong-authentication/index.html

[VoT-IETF] *IETF Vector of Trust*
https://tools.ietf.org/html/draft-richer-vectors-of-trust

Glossary

AAI	Authentication and Authorisation Infrastructure
BPA	Blueprint Architecture
AA	Attribute Authority
CO	Collaborative Organisation
IdP	Identity Provider
IETF	Internet Engineering Task Force
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OIDC	OpenID Connect
RAF	REFEDS Assurance Framework
REFEDS	Research and Education Federations
SAML	Security Assertion Markup Language
SFA	Single-Factor Authentication
SP	Service Provider
VoT	Vectors of Trust