Guideline on the exchange of specific assurance information between Infrastructures

Publication Date	2018-02-13
Authors:	AARC Consortium Partners;AppInt contributors;David Groep et al.
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	TNA3.3
Lead Partner:	Nikhef
Document Code:	AARC-G021 (Last Call v04)
DOI:	https://doi.org/10.5281/zenodo.1173558
License:	CC-BY-4.0

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

Abstract

Infrastructures and generic e-Infrastructures compose an 'effective' assurance profile derived from several sources, yet it is desirable to exchange the resulting assurance assertion obtained between Infrastructures so that it need not be re-computed by a recipient Infrastructure or Infrastructure service provider. This document describes the assurance profiles recommended to be used by the Infrastructure AAI Proxies between infrastructures: REFEDS RAF Cappuccino and Espresso, IGTF-BIRCH and IGTF-DOGWOOD, and a new specific profile addressing assurance partially derived from social-identity sources: AARC-Assam.

1. Introduction

Increasingly, Research Infrastructures and generic e-Infrastructures, referred to as Infrastructures henceforth, provide collective and 'meshed' services where a business process is composed of service elements from a variety of Infrastructures yet acts as a single coherent service towards the end-user. As part of the user interaction, Infrastructures compose an assurance profile derived from several sources. The assurance elements may come from an institutional identity provider (IdP), from community-provided information sources, from step-up authentication services, and from controls placed upon the user, the community, or the Infrastructure Proxy through either policy or technical enforcement. Knowledge about the upstream source of either identity or authenticator can also influence the risk perception of the Infrastructure and result in a modification of the assurance level, e.g. because it has involved a social identity provider or perhaps a government e-ID. The granularity of this composite assurance profile is attuned to the risk assessment specific to the Infrastructure or Infrastructures, and is often both more fine-grained and more specific than what can reasonably be expressed by generic IdPs or consumed by generic service providers.

Yet it is desirable to exchange as complete as possible the assurance assertion obtained between Infrastructures, so that assurance elements need not be re-asserted or re-computed by a recipient Infrastructure or Infrastructure service provider.

How an Infrastructure determines adherence to an assurance profile beyond the information given herein, or how the composition of assurance elements is to be performed is outside the scope of this document (it is dealt with in AARC-G031 "Account linking & LoA elevation in cross-sector AAIs") [AARC-G031].

2. Scope

These guidelines SHOULD be used when exchanging assurance information between "SP-IdP-Proxy" components of Infrastructures (Infrastructure Proxies as defined in the Blueprint Architecture [BPA]), and MAY be used when conveying assurance information between an SP-IdP-Proxy and service providers that are part of a coordinated set or consortium and bound to one or more Infrastructure Proxies.

These guidelines SHOULD NOT be used without further specific agreements to convey assurance information between identity providers (such as SAML IdPs or OIDC Providers) and Infrastructure Proxies. In such an exchange, incoming assurance information SHOULD be requested using the assurance profiles and assurance component values defined in the REFEDS Assurance Framework or using the IGTF Assurance Profiles. Which of these is appropriate depends on the use case and the technology, and the definition of such context is outside the scope of this document.

These guidelines SHOULD NOT be used to convey assurance information between Infrastructure Proxies and service providers that are not part of a coordinated consortium that has by itself adopted these guidelines. When assurance information is exchanged

between an Infrastructure Proxy and a general service provider, and where the component values are a superset of the values required for a REFEDS RAF assurance level, all corresponding REFEDS RAF assurance profiles MUST also be asserted.

This Guideline should be used and interpreted in the context of the AARC Blueprint Architecture (https://aarc-project.eu/architecture/) and the AARC Policy recommendations (https://aarc-project.eu/policies/).

3. Expression of assurance information

In line with the REFEDS Assurance Framework (RAF) [RAF], this guideline allows for both a composite assurance value and for assurance component values to be expressed. In the RAF, it is the component values that play the principle role in expressing assurance information, and the composite profiles ("Cappuccino" and "Espresso", for instance) are the result of a specific combination of assurance components that SHOULD be additionally asserted by the credential service provider (CSP) [CSP] if they qualify for such a profile.

While this requirement is of significant benefit to the recipient of assurance information, it places some of the burden on the CSP to keep track of the RAF process and change operational behaviour if the set of profiles changes. The component values therefore take precedence in the RAF specification.

This is less of a concern between the (limited) number of Infrastructures and Infrastructure Proxies. Here the simplicity of exchanging a few well-understood profiles carries significant benefit, and allows easier processing of assurance assertions by the participating Infrastructures. Therefore, in these guidelines the Profiles take precedence, and Profiles can be composed both of assurance components that have been previously standardised (e.g. by the RAF or NIST) as well as of other definitions of assurance components (e.g. through 1-statement policies or references to other documented profiles).

4. Rationale for the additional Profiles

This document defines one additional profile and imports two additional profiles from the IGTF [IGTF]. These profiles can be used as a supplement to - and where required in conjunction with - the RAF Assurance Profiles, and have been added to address some issues specific to the Infrastructure use cases

- the RAF authentication assurance relies on the definition of the REFEDS SFA and MFA profiles [SFA, MFA]. Whereas the MFA profile is well understood, the level of authentication certainty conveyed with the REFEDS SFA profile follows the minimum acceptable basis for the authentication factors of the subset it addresses of NIST SP800-63B. While appropriate to permit inclusion of as many R&E Home Organisation CSPs as reasonably possible, this is not usually considered sufficient for much of the Infrastructure use without specific compensatory controls, which are provided in the *IGTF-BIRCH* profile.

- The unique person identifier specification to be determined by the identifier components should be specified in accordance with AARC-G026 “Uniquely identifying users across infrastructures” [AARC-G026].
- Additional vetting can be provided by other sources (e.g. a community authority) to raise from incoming “IAP/low” ID proofing assurance identities [IAP] or other ‘lower-quality’ identities, making it meet the requirements of the *IGTF-DOGWOOD* profile. If an ID Proofing status is a result of additional information provided by identity linking in accordance with AARC-G031 “Account linking & LoA elevation in cross-sector AAIs” [AARC-G031], or based on data held by the community or the e-Infrastructure, this information SHALL be conveyed by adding the “IAP/medium” and/or “IAP/high” ID proofing status if it meets the requirements thereof.
- The attribute freshness requirement needs to take into account composite sources (such as Infrastructure registry, community sources, optionally other end-user technical and policy controls) as defined in the Section “*Attribute freshness assurance component*”, since the affiliation attribute for identities based on derived information or linked identities can no longer accurately reflect a status from an upstream identity provider.
- A mechanism is needed to flag at the Infrastructure Proxy identities that are based on social identities, or originate from sources outside the R&E community that are otherwise entirely self-managed, in whole or in part. Identity providers of last resort that connect to the R&E federation SHOULD qualify and assert “low” ID proofing and comply with the REFEDS RAF assurance values. Although in the general case such information might be flagged in entity metadata (e.g., using entity categories in SAML), within the current conveyance mechanism between Infrastructures, the challenge is that the proxy may process and can potentially address some of the issues with the social ID, such as ensuring uniqueness and adding ‘soft’ qualifies around reasonable association with a community or name form, making it meet sufficient criteria to satisfy the *AARC-Assam* profile.

Since it depends at least in part on the implementation of the proxy, its expression must therefore not only be via a profile but it also needs to be accompanied by an implementation specification or identifiable policy or technical controls.

These guidelines extend the REFEDS RAF profiles by adding specific profiles that – although not easily feasible for adoption by the IdPs of the R&E community at large - are currently established for Infrastructure risk profiles, and that can be composed by augmenting assurance data from sources available to the Infrastructures (since additional information on origin or on policy-enforced authentication strength) and are thus effective in addressing inter-Infrastructure use cases.

5. Profiles

The following profiles may be conveyed as entity assurance values within the scope of this Guideline, subject to the guidance given below. The “MUST”, “SHOULD”, and “MAY” entries indicate the value of the assurance attribute that are to be asserted.

5.1. REFEDS RAF Profiles

Name	**REFEDS RAF Assurance Profile Cappuccino**
SAML Identifier	https://refeds.org/assurance/profile/cappuccino
Other identifier(s)	-
Description	has a unique identifier, identity proofing and credential qualifies substantially to Kantara LoA 2, IGTF BIRCH or CEDAR, or eIDAS low, and can be attained with single-factor authentication according to REFEDS SFA without further constraints. Affiliation information is not older than one month.
MUST	https://refeds.org/assurance/profile/cappuccino *and comply fully with REFEDS RAF profile Cappuccino specification:* https://refeds.org/assurance/ID/unique https://refeds.org/assurance/IAP/low https://refeds.org/assurance/IAP/medium https://refeds.org/profile/sfa https://refeds.org/assurance/ATP/ePA-1m
SHOULD	
MAY	

Name	**REFEDS RAF Assurance Profile Espresso**
SAML Identifier	https://refeds.org/assurance/profile/espresso
Other identifier(s)	-
Description	has a unique identifier, identity proofing and credential qualifies substantially to Kantara LoA 3 or eIDAS substantial, and must be attained with multi-factor authentication according to REFEDS MFA, where the multi-factor credential cannot be derived solely from a single-factor. Affiliation information is not older than one month.
MUST	https://refeds.org/assurance/profile/espresso *and comply fully with REFEDS RAF profile Espresso specification:* https://refeds.org/assurance/ID/unique https://refeds.org/assurance/IAP/low https://refeds.org/assurance/IAP/medium https://refeds.org/assurance/IAP/high https://refeds.org/profile/mfa https://refeds.org/assurance/ATP/ePA-1m
SHOULD	
MAY	

5.2. Supplementary IGTF profiles for Infrastructures

Name	**IGTF BIRCH**
SAML Identifier	https://igtf.net/ap/authn-assurance/birch
Other identifier(s)	IGTF-BIRCH urn:oid:1.2.840.113612.5.2.5.2
Description	Persistent non-reassigned identifier, identity proofing based on in-person appearance (current or past), remote vetting with compensatory controls, or Kantara LoA 2 or better. Includes a reasonable verified representation of the real name of the entity, and is secure with a best common practice (27-bit entropy as per NIST SP800-63v2, 2004) single factor or multi-factor authenticator. Identity and authenticator are managed by the CSP.
MUST	https://igtf.net/ap/authn-assurance/birch
SHOULD	https://refeds.org/assurance/ID/unique *the unique identifier should be specified in compliance with AARC-G026 "Uniquely identifying users across infrastructures"* https://refeds.org/assurance/IAP/low https://refeds.org/assurance/IAP/medium https://refeds.org/profile/sfa *note: one cannot in all cases assert MFA here, since using two factors where one is (even with compensatory controls)derived from the other factor is not compliant with MFA, but permissible under the BIRCH profile provided specific compensatory controls are in place.* https://refeds.org/assurance/ATP/ePA-1m
MAY	urn:oid:1.2.840.113612.5.2.3.1.2.1 (1SCP IGTF file-protected soft keys) urn:oid:1.2.840.113612.5.4.1.1.1.5 (IGTF PKP Guidelines)

Name	**IGTF DOGWOOD**
SAML Identifier	https://igtf.net/ap/authn-assurance/dogwood
Other identifier(s)	IGTF-DOGWOOD urn:oid:1.2.840.113612.5.2.5.4
Description	Persistent non-reassigned identifier, identity proofing sufficient to ensure non-reassignment of the identifier for the lifetime of the CSP. May contain marginally-verified real name resemblance or identifiers clearly identifiable as pseudonyms. No anonymous credentials permitted and issuance is traceable at time of issuance. Authenticator is secured according to best common practice (27-bit entropy as per NIST SP800-63v2, 2004) single factor or multi-factor authenticator, or compensatory controls on credential validity period are in place. Identity and authenticator are managed by the CSP.
MUST	https://igtf.net/ap/authn-assurance/dogwood
SHOULD	https://refeds.org/assurance/ID/unique *the unique identifier should be specified in compliance with AARC-G026 "Uniquely identifying users across infrastructures"* https://refeds.org/assurance/IAP/low https://refeds.org/profile/sfa https://refeds.org/assurance/ATP/ePA-1m
MAY	urn:oid:1.2.840.113612.5.2.3.1.2.1 (1SCP IGTF file-protected soft keys) urn:oid:1.2.840.113612.5.4.1.1.1.5 (IGTF PKP Guidelines)

5.3. Supplementary specific profiles for Infrastructures

Name	**AARC Assam**
SAML Identifier	https://aarc-project.eu/policy/authn-assurance/assam
Other identifier(s)	AARC-Assam
Description	Identity substantially derived from social media or self-signup identity providers (outside the R&E community) on which no further policy controls or qualities are placed. Identity proofing and authenticator are substantially derived from upstream CSPs that are not under the control of the Infrastructure. The Infrastructure ensures uniqueness on the identifiers based on proprietary heuristics.
MUST	https://aarc-project.eu/policy/authn-assurance/assam
SHOULD	https://refeds.org/assurance/ID/unique *only provided the Infrastructure Proxy can comply with the requirements on this unique identifier as specified in the REFEDS RAF [RAF], including the single natural person and traceability requirements therein;* *the unique identifier should be specified in compliance with AARC-G026 "Uniquely identifying users across infrastructures"* https://refeds.org/assurance/IAP/low *provided the source complies with the REFEDS IAP low requirements*
MAY	

5.4. Attribute freshness assurance component

The semantics of *eduPerson(Scoped)Affiliation* changes for the Infrastructure Proxy .The ATP assurance component (attribute freshness) [ATP] SHALL reflect the affiliation of the identity with the Infrastructure (in compliance with guideline AARC-G025 “Exchange of affiliation information” [AARC-G025]) and not with the upstream identity provider. Since such Infrastructure affiliation may be based on several sources of upstream identity in case of account linking or when the account is composed based on information from multiple sources, the ATP freshness component value of the source attributes SHOULD NOT be simply copied to the freshness of the resulting attributes. It MAY reflect the freshness of source attributes for deriving attributes related to the infrastructure (information on the freshness of source attributes could be used in the logic of the Proxy in determining freshness).This behaviour also ensures that information communicated to service providers will be consistently related to the identifiers communicated by the Infrastructure Proxy as per the AARC-G026 “Uniquely identifying users across infrastructures” [AARC-G026] guidelines.

Meaning attached to the values of *eduPerson(Scoped)Affiliation* SHOULD comply with guideline AARC-G025 “Exchange of affiliation information”.

5.5. Implementation notes

All statements should be asserted in a SAML rendering in eduPersonAssurance. The authenticator contexts MFA and SFA values should also be presented in SAML in AuthenticationContextClassRef. See the REFEDS Assurance Framework for discussion.

If the authentication assurance component meets the REFEDS-MFA criteria *and* the Infrastructure Proxy can determine that at least one of the factors also meets the minimum requirements for REFEDS-SFA, *but* in order to assert a specific assurance profile REFEDS-SFA or another authentication that relies on a single factor is required, *then* the REFEDS-MFA authentication assurance MUST be interpreted to also satisfy this single factor authentication when determining the assurance profile value, but at the same time the assurance component value for authentication SHOULD continue to be expressed as REFEDS-MFA.

The ATP assurance component values (e.g. “https://refeds.org/assurance/ATP/ePA-1m”) should be interpreted as meaning that the Infrastructure Proxy that composes assurance and that processes the sources of information (external identity providers, community registries) will take action to correct a status change within one month after they became aware of the changes in the user’s status with the Infrastructure. The assurance originating at an Infrastructure Proxy will signify freshness within the originating Infrastructure according to its policies. Communities, but also institutions with long-term student enrolment typically re-evaluate eligibility only on a yearly basis or when changes of status are actively communicated to them.

Table of Contents

References

AARCGL	AARC Guidelines Series, https://aarc-project.eu/guidelines/
AARC-G025	Exchange of affiliation information https://aarc-project.eu/guidelines/aarc-g025/
AARC-G026	Uniquely identifying users across infrastructures https://aarc-project.eu/guidelines/aarc-g026/
AARC-G031	Account linking & LoA elevation in cross-sector AAIs, https://aarc-project.eu/guidelines/aarc-g031/
ATP	The 'freshness of the (eduPersonScopedAffiliation) attribute value' assurance aspect as per the REFEDS RAF assurance framework [RAF].
BPA	AARC Blueprint Architecture (AARC-G012), http://aarc-project.eu/blueprint-architecture/
CSP	Credential Service Provider, as used in the REFEDS Assurance Framework [RAF]: "*A trusted actor that issues and/or manages credentials. In the context of this specification, CSP refers to the Identity Provider and the associated Identity Management system that manages the user identities, attributes and authentication observed by the Relying Parties.*"
IAP	Identity vetting assurance aspect as per the REFEDS RAF assurance framework [RAF].
IGTF	https://igtf.net/ap/loa
MFA	REFEDS Multi-Factor Authentication (MFA) Profile https://refeds.org/profile/mfa
PROXY	Infrastructure Proxy as defined in the AARC Blueprint Architecture (AARC-G012), http://aarc-project.eu/blueprint-architecture/
RAF	https://wiki.refeds.org/display/GROUPS/Assurance+Working+Group
SFA	REFEDS Single-Factor Authentication (SFA) Profile (draft) https://refeds.org/profile/sfa; https://docs.google.com/document/d/1HOcM2o4N7Ly9elRd5OQH2dCmfjY83WBv7ZCPgFysNmE/