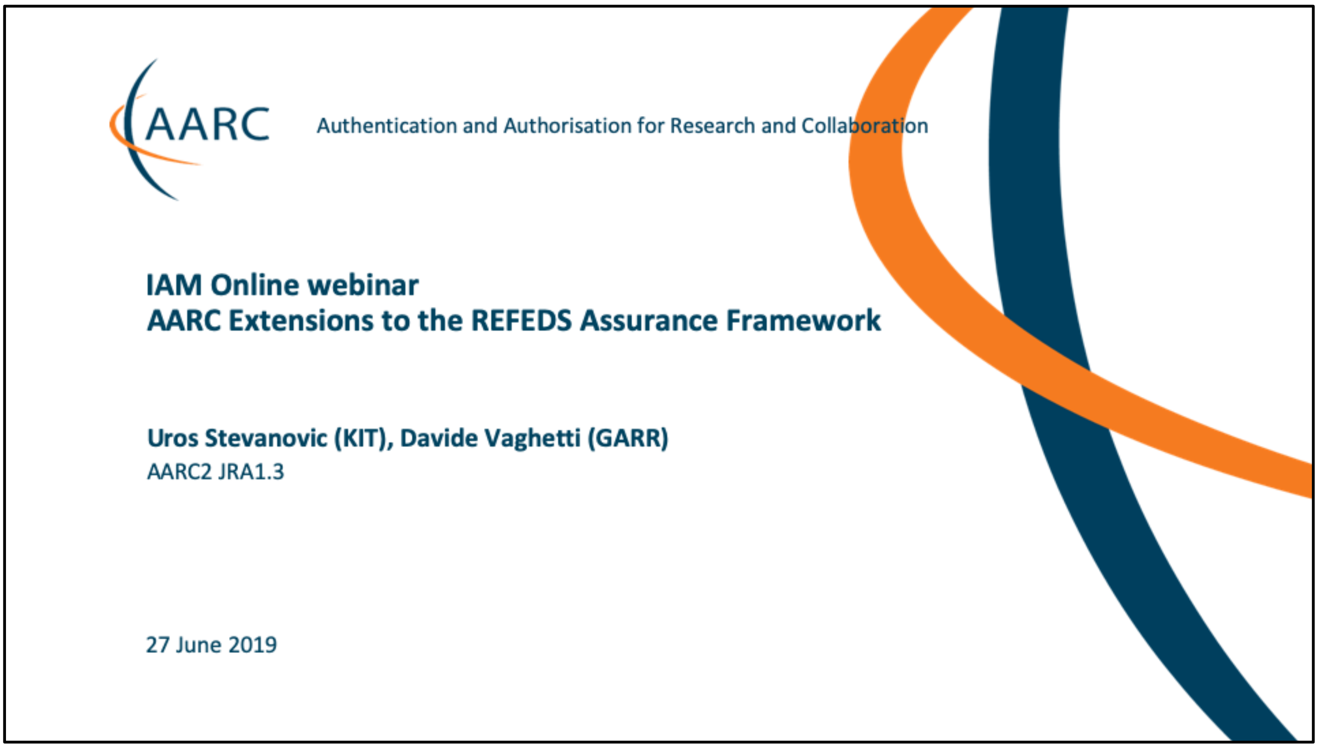


AARC Authentication and Authorisation for Research and Collaboration

IAM Online webinar
AARC Extensions to the REFEDS Assurance Framework

Uros Stevanovic (KIT), Davide Vaghetti (GARR)
AARC2 JRA1.3

27 June 2019

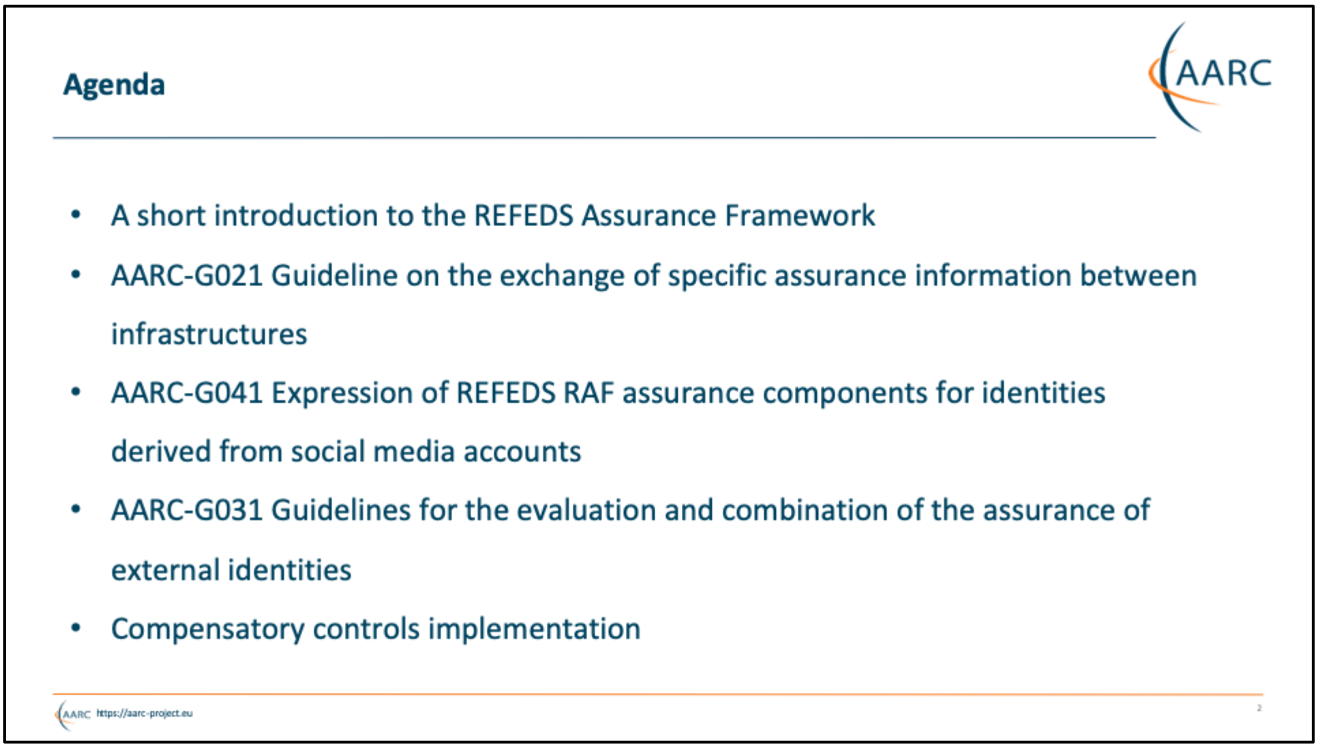
AARC-G031 provides guidelines for enabling the AAI of a research collaboration to evaluate the assurance of the identity of a researcher to which grants access to specific resources of the collaboration.

Why did AARC extend RAF?

The REFEDS Assurance Framework was explained in a previous webinar.

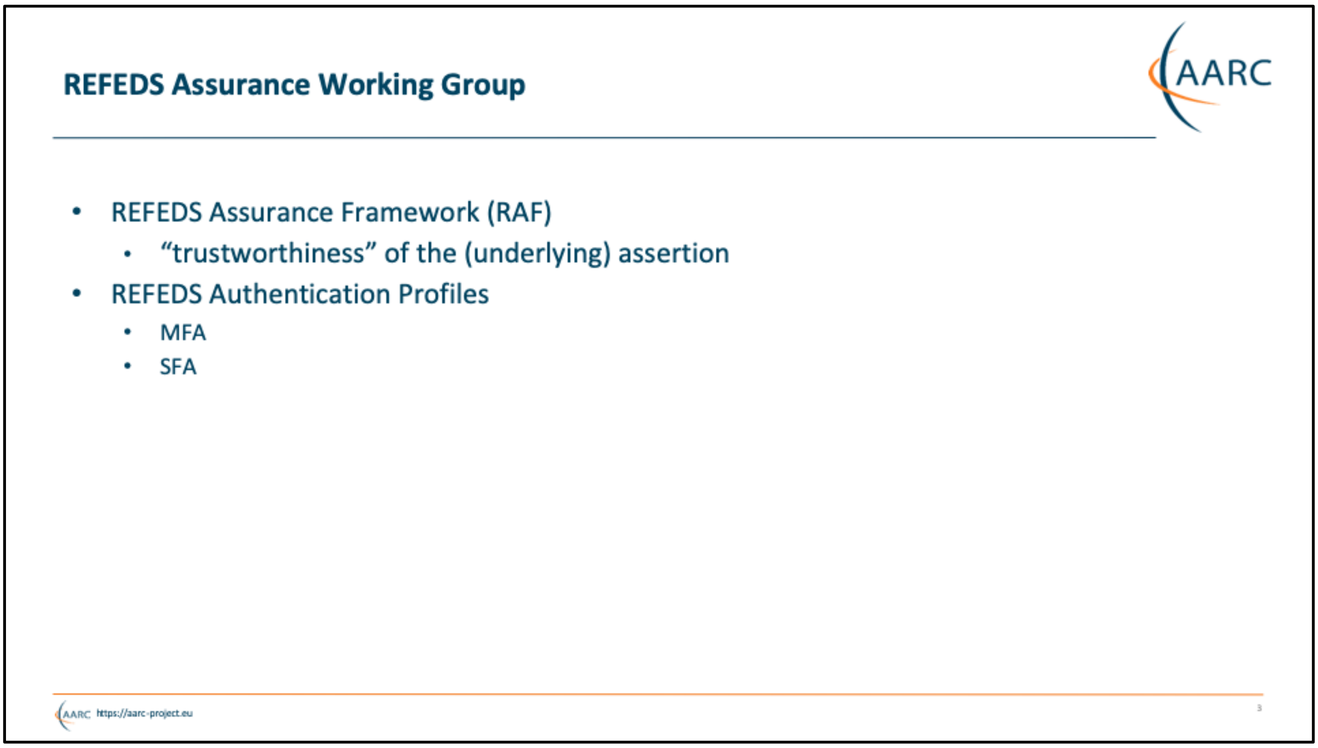
The AARC (Authentication and Authorisation for Research and Collaboration) project developed additional guidance to facilitate the exchange of assurance information across infrastructures (or between SP-IdP-Proxy components of infrastructures).

Supplementary AARC and IGTF assurance profiles targeting the specific research and infrastructures' needs in terms of risk profiles help out: shared assurance profiles inspired by the Service Provider and infrastructure requirements can be exchanged directly and help evaluate identity assurance information for the attributes and authenticator presented both by the user's home organisations via the R&E federations and from supplementary sources when enabling federated access-to-access services.



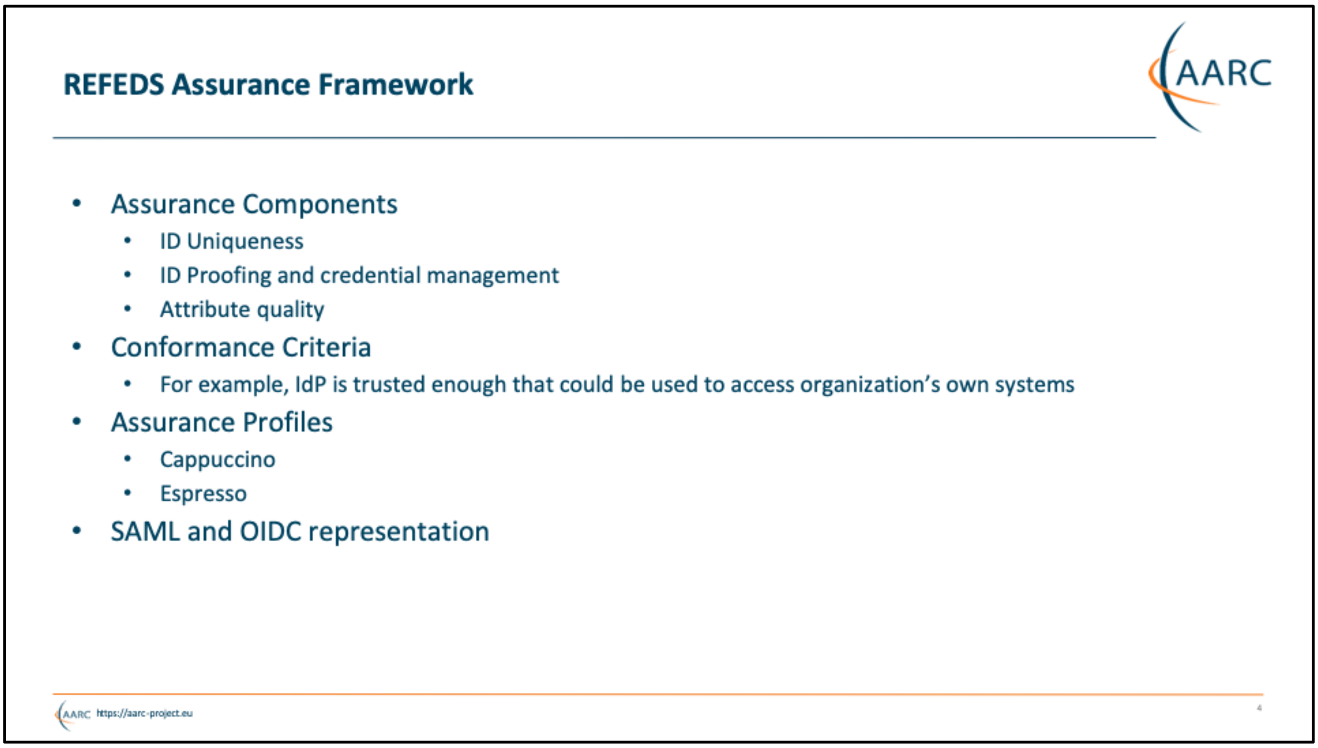
Agenda

- A short introduction to the REFEDS Assurance Framework
- AARC-G021 Guideline on the exchange of specific assurance information between infrastructures
- AARC-G041 Expression of REFEDS RAF assurance components for identities derived from social media accounts
- AARC-G031 Guidelines for the evaluation and combination of the assurance of external identities
- Compensatory controls implementation



REFEDS Assurance Working Group

- REFEDS Assurance Framework (RAF)
  - “trustworthiness” of the (underlying) assertion
- REFEDS Authentication Profiles
  - MFA
  - SFA

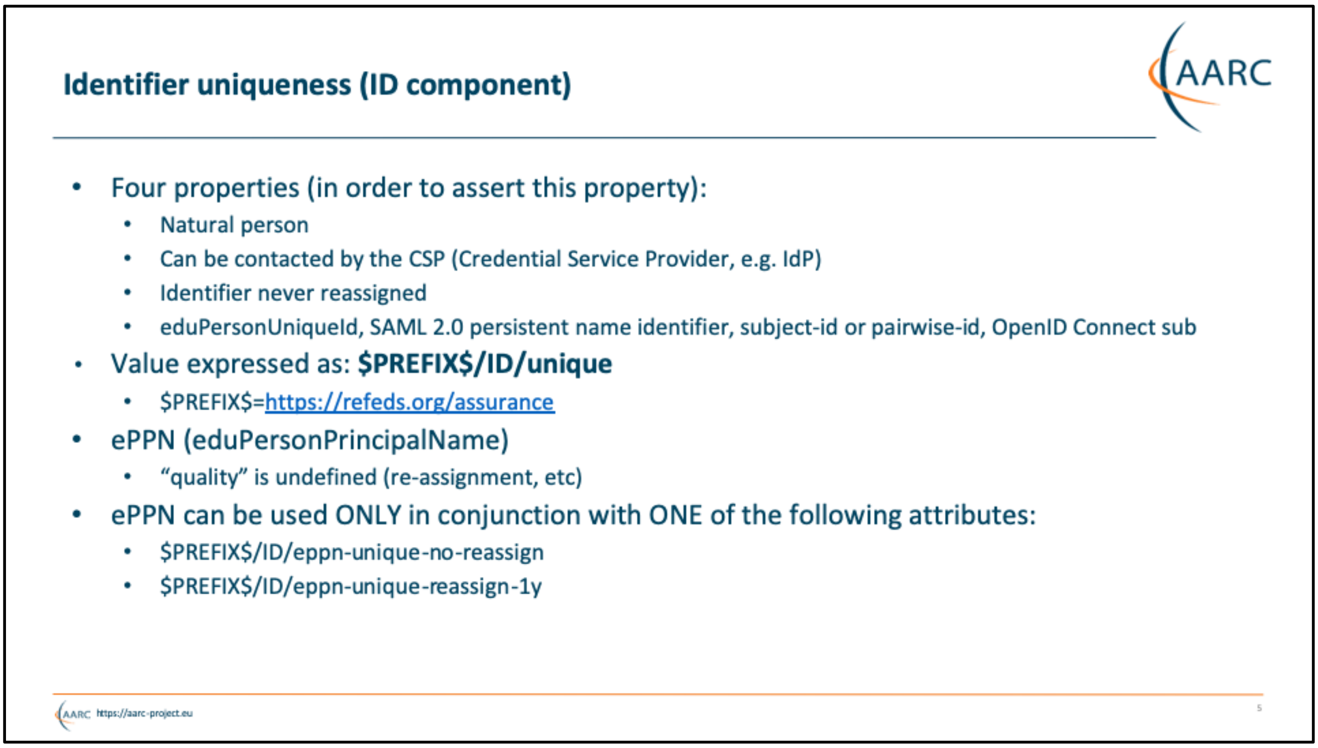


REFEDS Assurance Framework

- Assurance Components
  - ID Uniqueness
  - ID Proofing and credential management
  - Attribute quality
- Conformance Criteria
  - For example, IdP is trusted enough that could be used to access organization’s own systems
- Assurance Profiles
  - Cappuccino
  - Espresso
- SAML and OIDC representation

https://aarc-project.eu

4

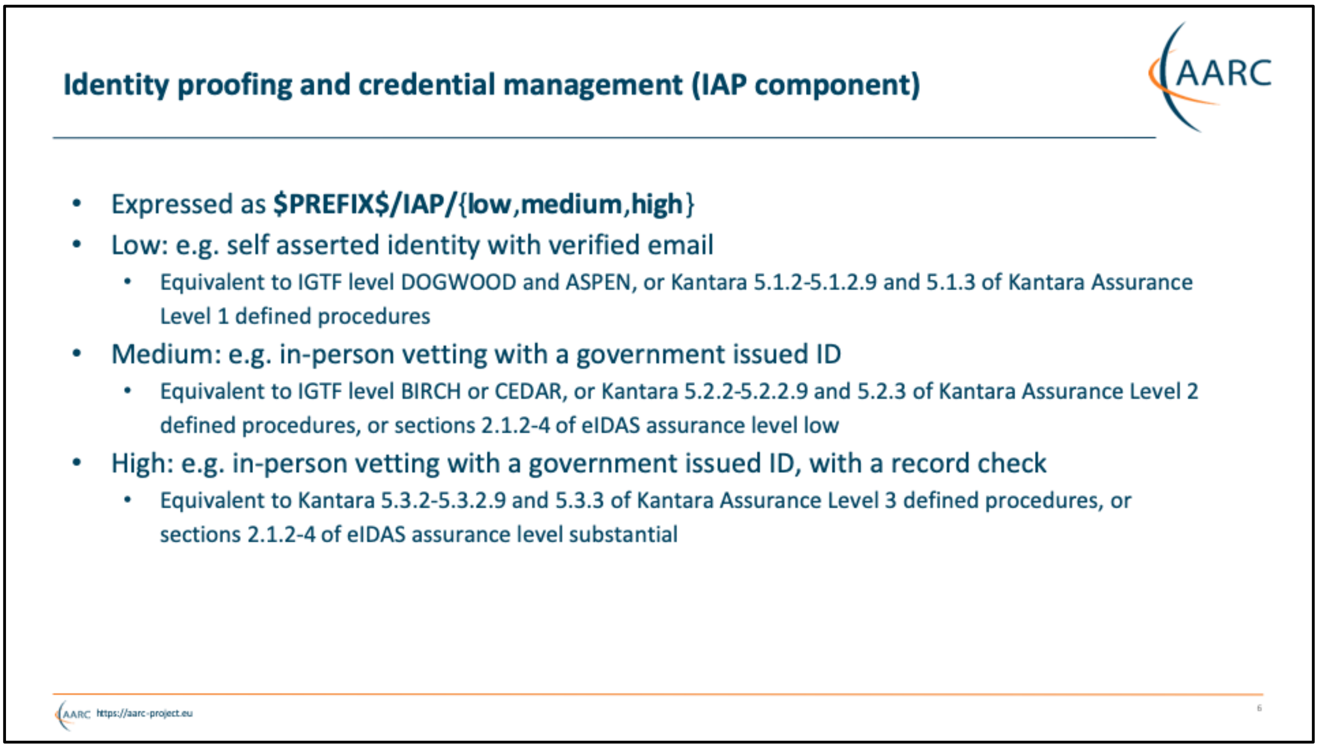


Identifier uniqueness (ID component)

- Four properties (in order to assert this property):
  - Natural person
  - Can be contacted by the CSP (Credential Service Provider, e.g. IdP)
  - Identifier never reassigned
  - eduPersonUniqueId, SAML 2.0 persistent name identifier, subject-id or pairwise-id, OpenID Connect sub
- Value expressed as: **$PREFIX$/ID/unique**
  - $PREFIX$=https://refeds.org/assurance
- ePPN (eduPersonPrincipalName)
  - “quality” is undefined (re-assignment, etc)
- ePPN can be used ONLY in conjunction with ONE of the following attributes:
  - $PREFIX$/ID/eppn-unique-no-reassign
  - $PREFIX$/ID/eppn-unique-reassign-1y

AARC https://aarc-project.eu

5

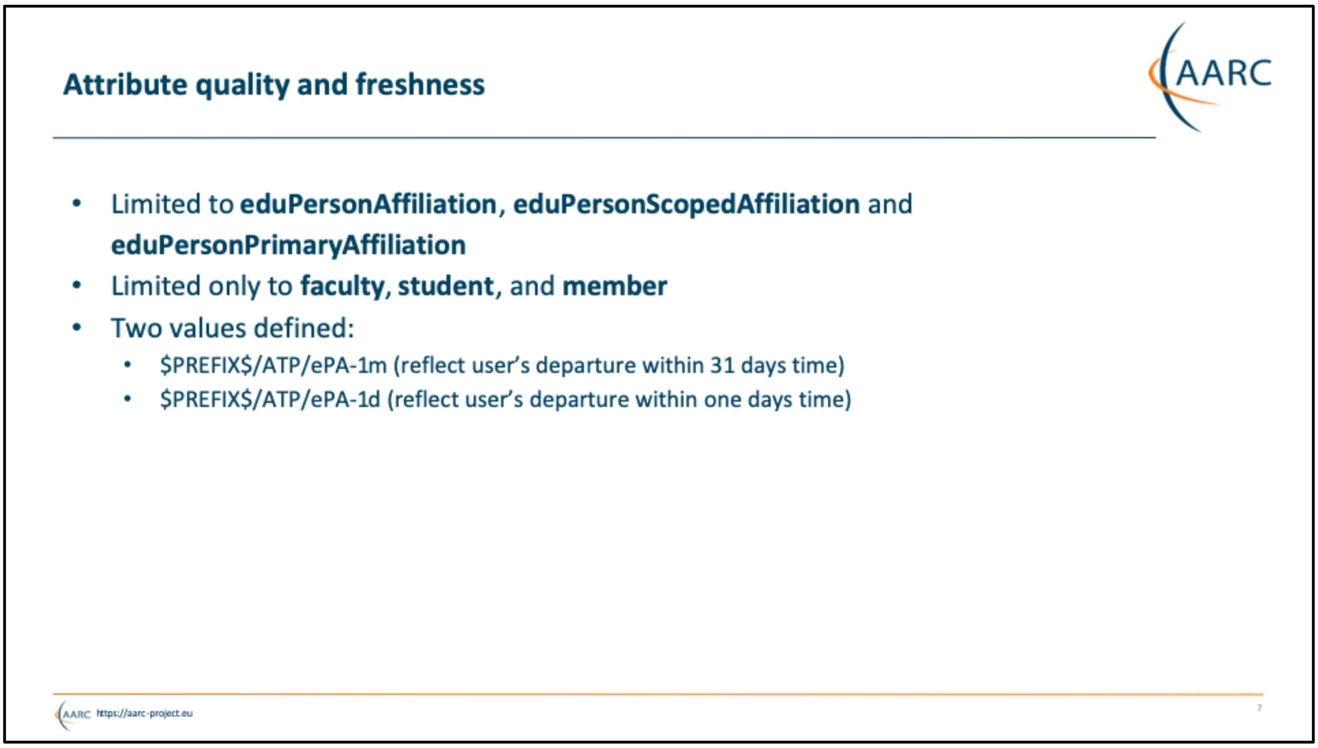


Identity proofing and credential management (IAP component)

- Expressed as **$PREFIX$/IAP/**{**low**,**medium**,**high**}
- Low: e.g. self asserted identity with verified email
  - Equivalent to IGTF level DOGWOOD and ASPEN, or Kantara 5.1.2-5.1.2.9 and 5.1.3 of Kantara Assurance Level 1 defined procedures
- Medium: e.g. in-person vetting with a government issued ID
  - Equivalent to IGTF level BIRCH or CEDAR, or Kantara 5.2.2-5.2.2.9 and 5.2.3 of Kantara Assurance Level 2 defined procedures, or sections 2.1.2-4 of eIDAS assurance level low
- High: e.g. in-person vetting with a government issued ID, with a record check
  - Equivalent to Kantara 5.3.2-5.3.2.9 and 5.3.3 of Kantara Assurance Level 3 defined procedures, or sections 2.1.2-4 of eIDAS assurance level substantial

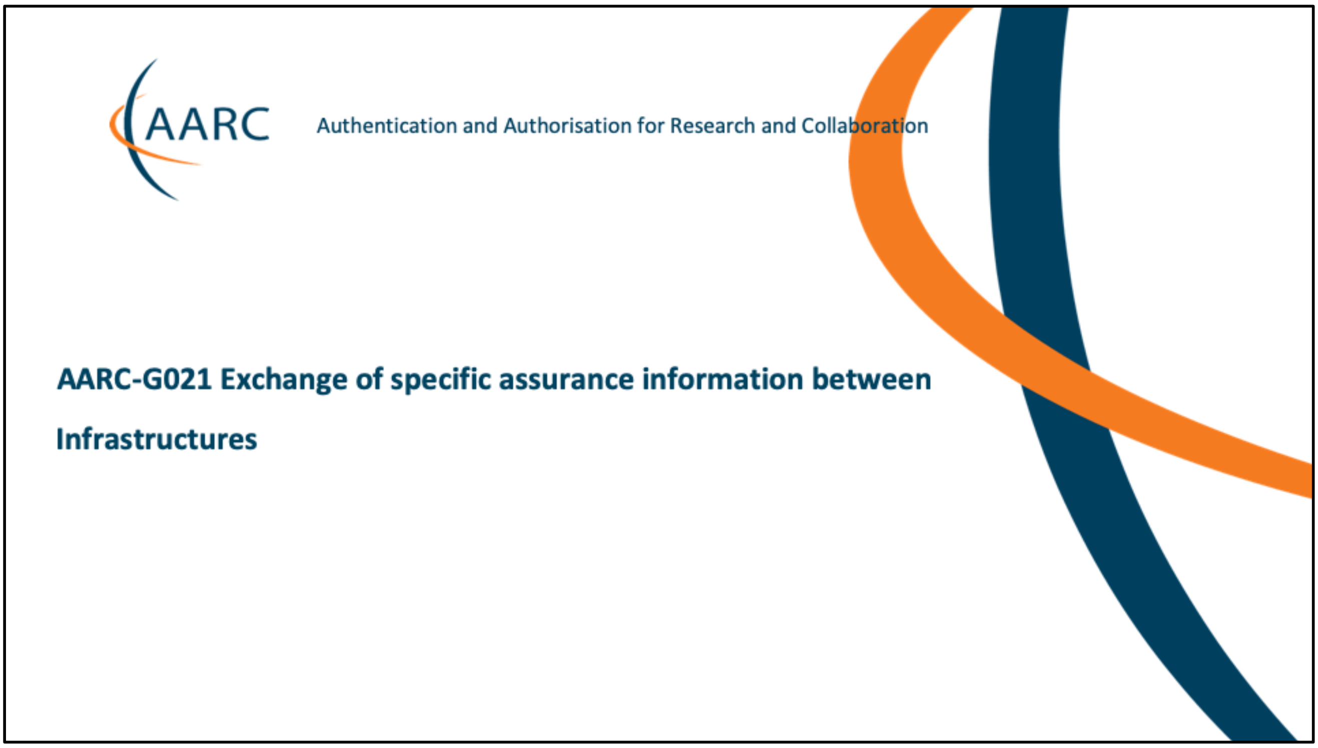
https://aarc-project.eu

6



Attribute quality and freshness

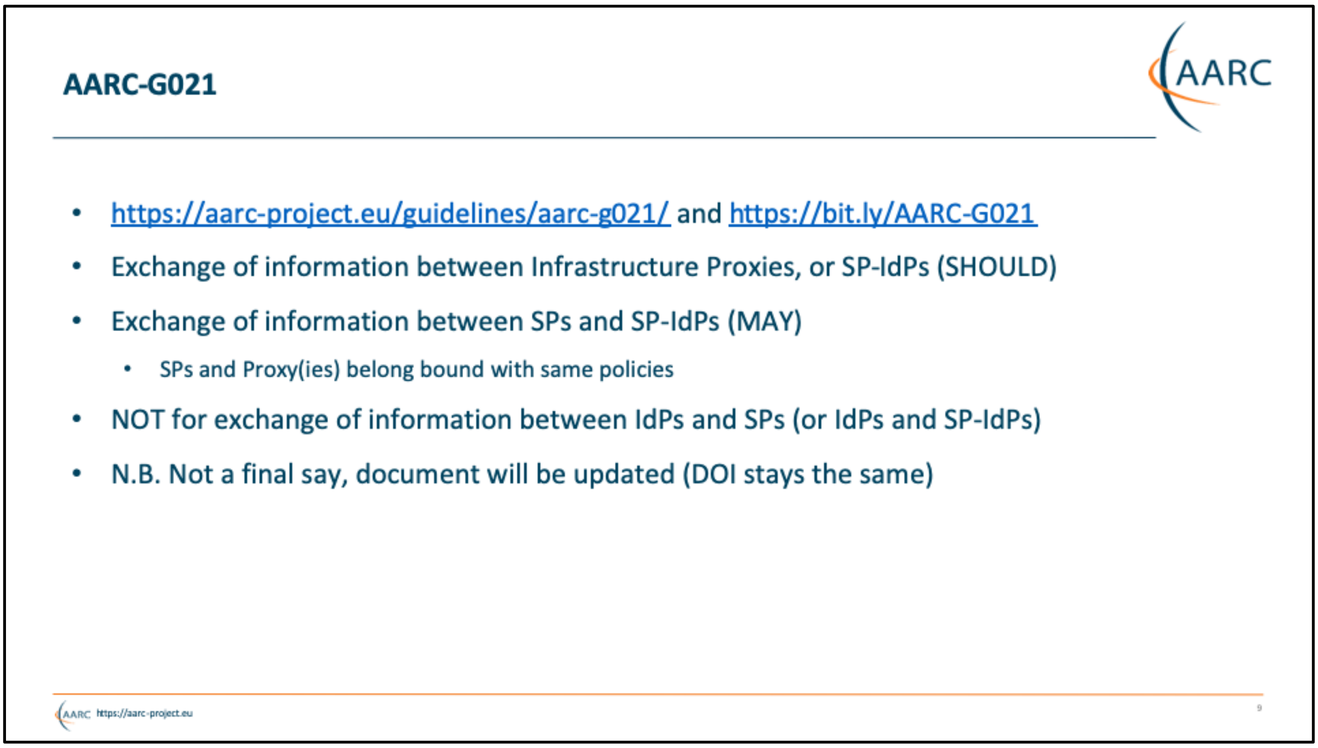
- Limited to **eduPersonAffiliation**, **eduPersonScopedAffiliation** and **eduPersonPrimaryAffiliation**
- Limited only to **faculty**, **student**, and **member**
- Two values defined:
  - $PREFIX$/ATP/ePA-1m (reflect user's departure within 31 days time)
  - $PREFIX$/ATP/ePA-1d (reflect user's departure within one days time)



AARC Authentication and Authorisation for Research and Collaboration

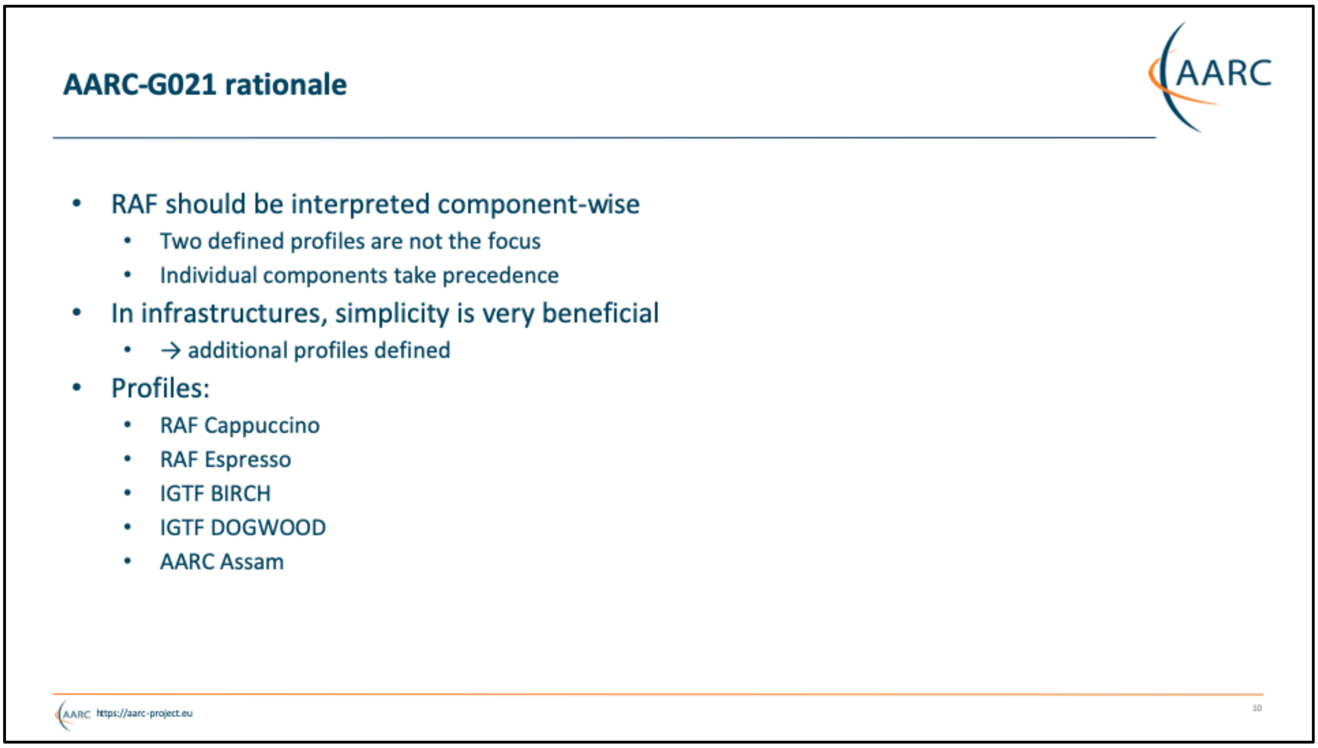
AARC-G021 Exchange of specific assurance information between Infrastructures

AARC-G031 provides guidelines for enabling the AAI of a research collaboration to evaluate the assurance of the identity of a researcher to which grants access to specific resources of the collaboration.



AARC-G021

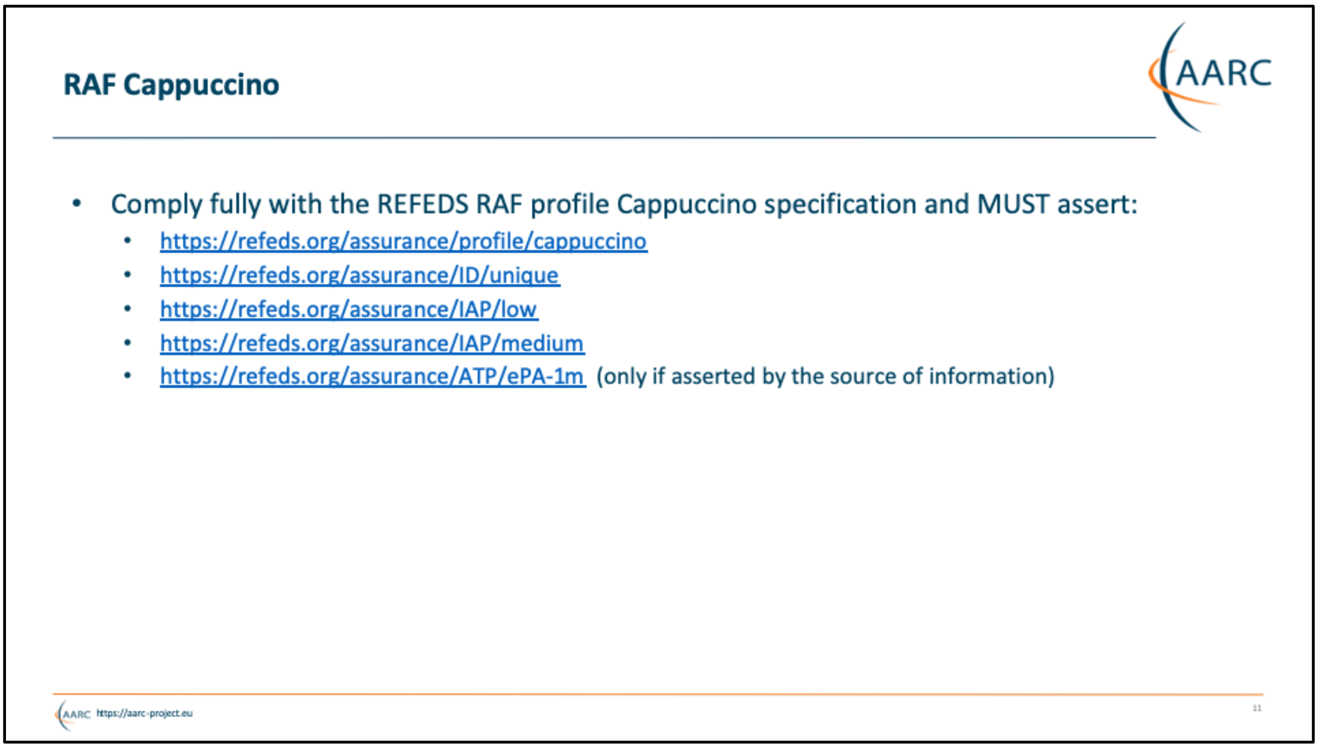
- https://aarc-project.eu/guidelines/aarc-g021/ and https://bit.ly/AARC-G021
- Exchange of information between Infrastructure Proxies, or SP-IdPs (SHOULD)
- Exchange of information between SPs and SP-IdPs (MAY)
  - SPs and Proxy(ies) belong bound with same policies
- NOT for exchange of information between IdPs and SPs (or IdPs and SP-IdPs)
- N.B. Not a final say, document will be updated (DOI stays the same)



AARC-G021 rationale

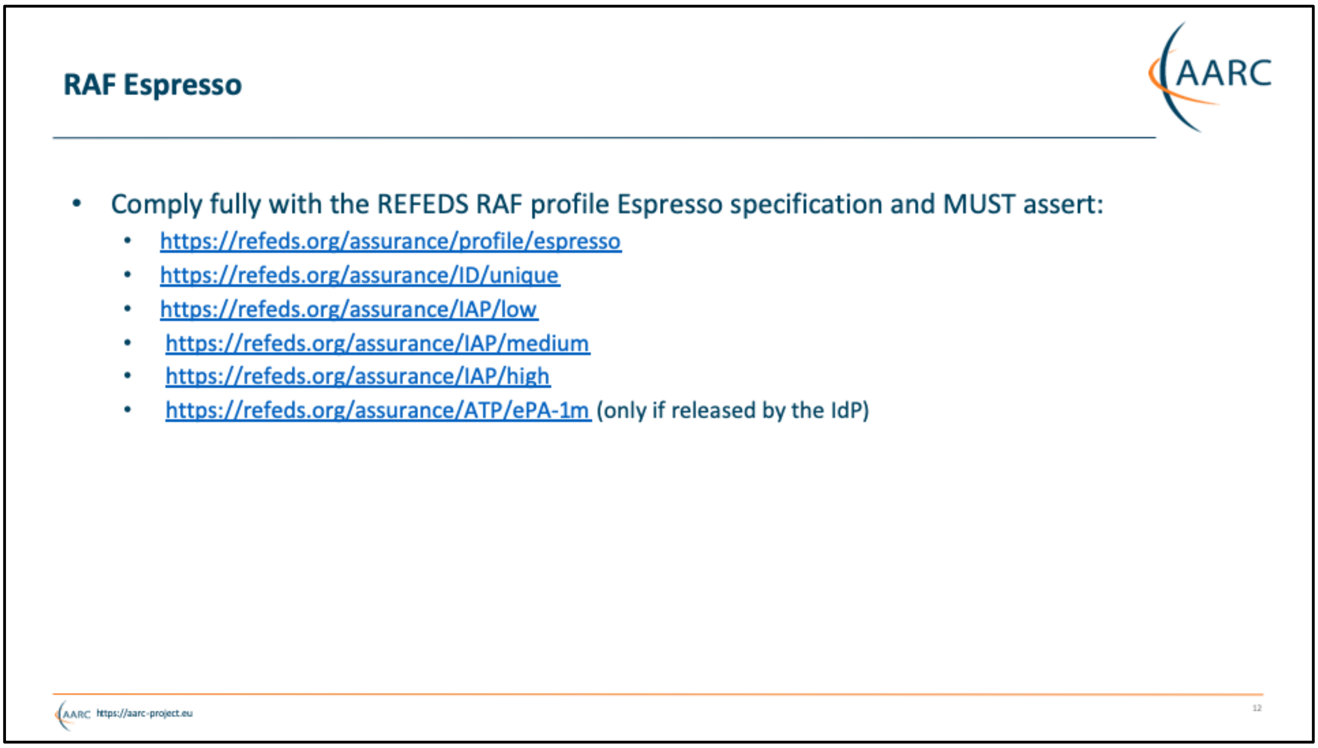
- RAF should be interpreted component-wise
  - Two defined profiles are not the focus
  - Individual components take precedence
- In infrastructures, simplicity is very beneficial
  - → additional profiles defined
- Profiles:
  - RAF Cappuccino
  - RAF Espresso
  - IGTF BIRCH
  - IGTF DOGWOOD
  - AARC Assam

https://aarc-project.eu



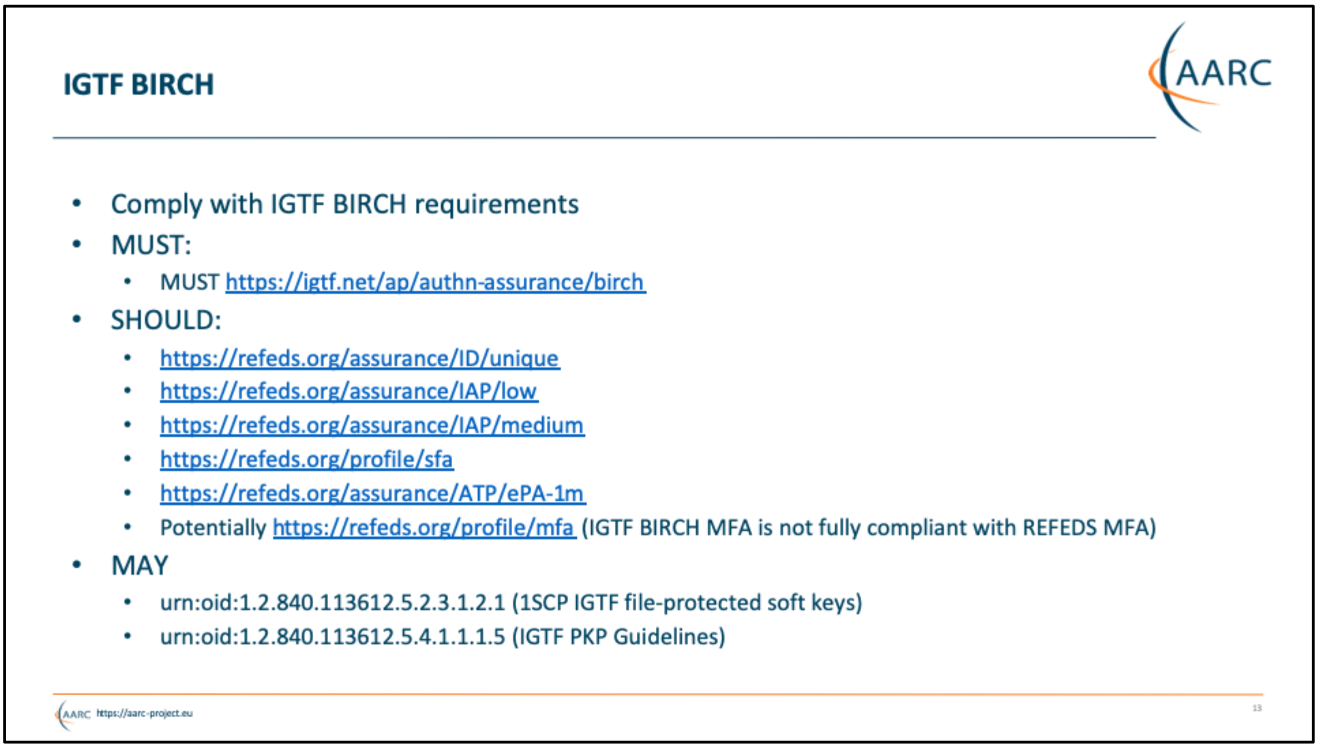
RAF Cappuccino

- Comply fully with the REFEDS RAF profile Cappuccino specification and MUST assert:
  - https://refeds.org/assurance/profile/cappuccino
  - https://refeds.org/assurance/ID/unique
  - https://refeds.org/assurance/IAP/low
  - https://refeds.org/assurance/IAP/medium
  - https://refeds.org/assurance/ATP/ePA-1m (only if asserted by the source of information)



RAF Espresso

- Comply fully with the REFEDS RAF profile Espresso specification and MUST assert:
  - https://refeds.org/assurance/profile/espresso
  - 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/assurance/ATP/ePA-1m (only if released by the IdP)

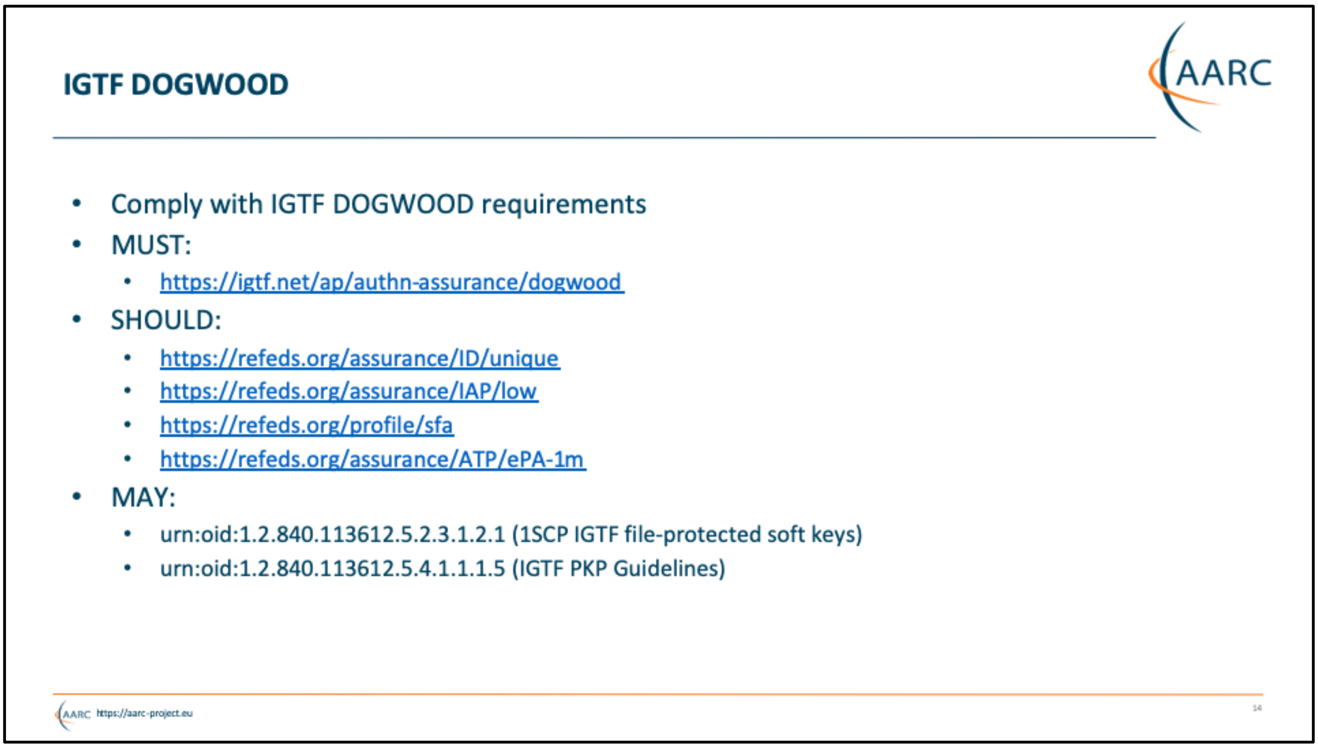


IGTF BIRCH

- Comply with IGTF BIRCH requirements
- MUST:
  - MUST https://igtf.net/ap/authn-assurance/birch
- SHOULD:
  - 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
  - Potentially https://refeds.org/profile/mfa (IGTF BIRCH MFA is not fully compliant with REFEDS MFA)
- 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)

https://aarc-project.eu 13

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.

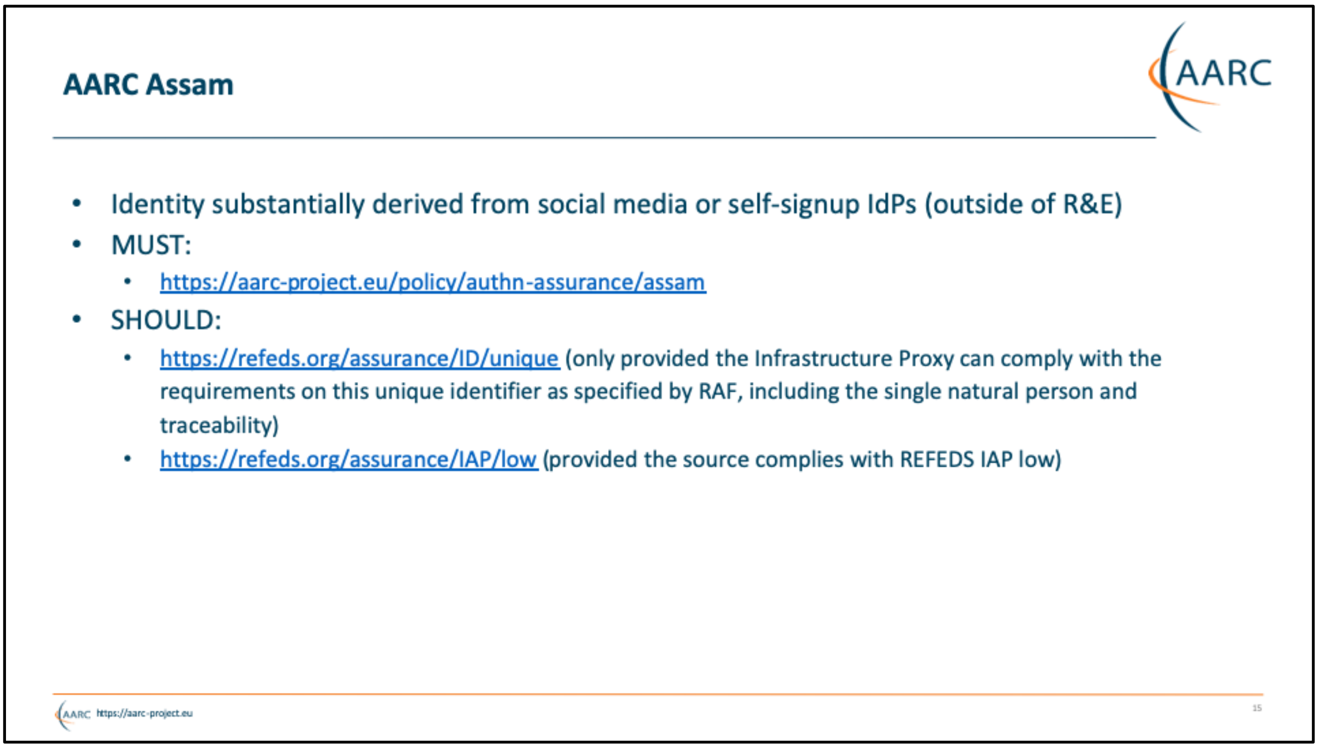


IGTF DOGWOOD

- Comply with IGTF DOGWOOD requirements
- MUST:
  - https://igtf.net/ap/authn-assurance/dogwood
- SHOULD:
  - https://refeds.org/assurance/ID/unique
  - 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)

AARC https://aarc-project.eu 14

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.

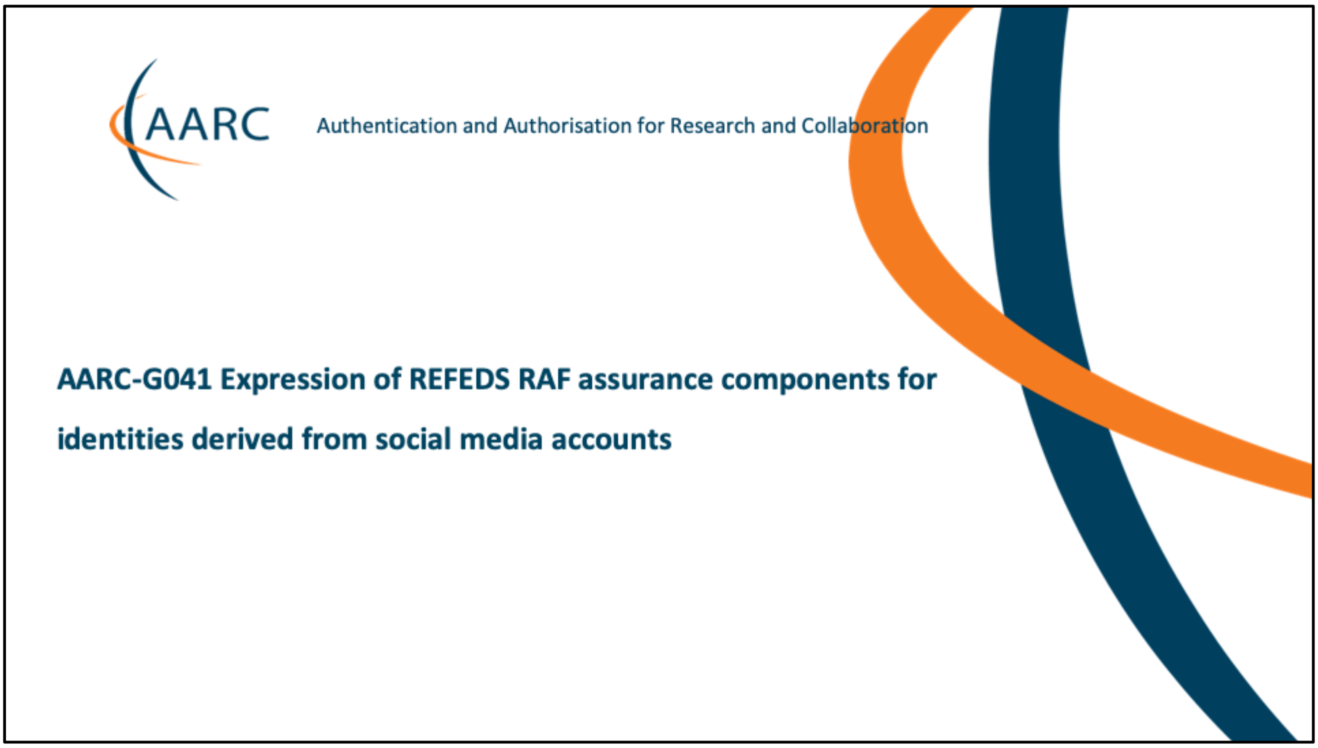


AARC Assam

- Identity substantially derived from social media or self-signup IdPs (outside of R&E)
- 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 by RAF, including the single natural person and traceability)
  - https://refeds.org/assurance/IAP/low (provided the source complies with REFEDS IAP low)

https://aarc-project.eu

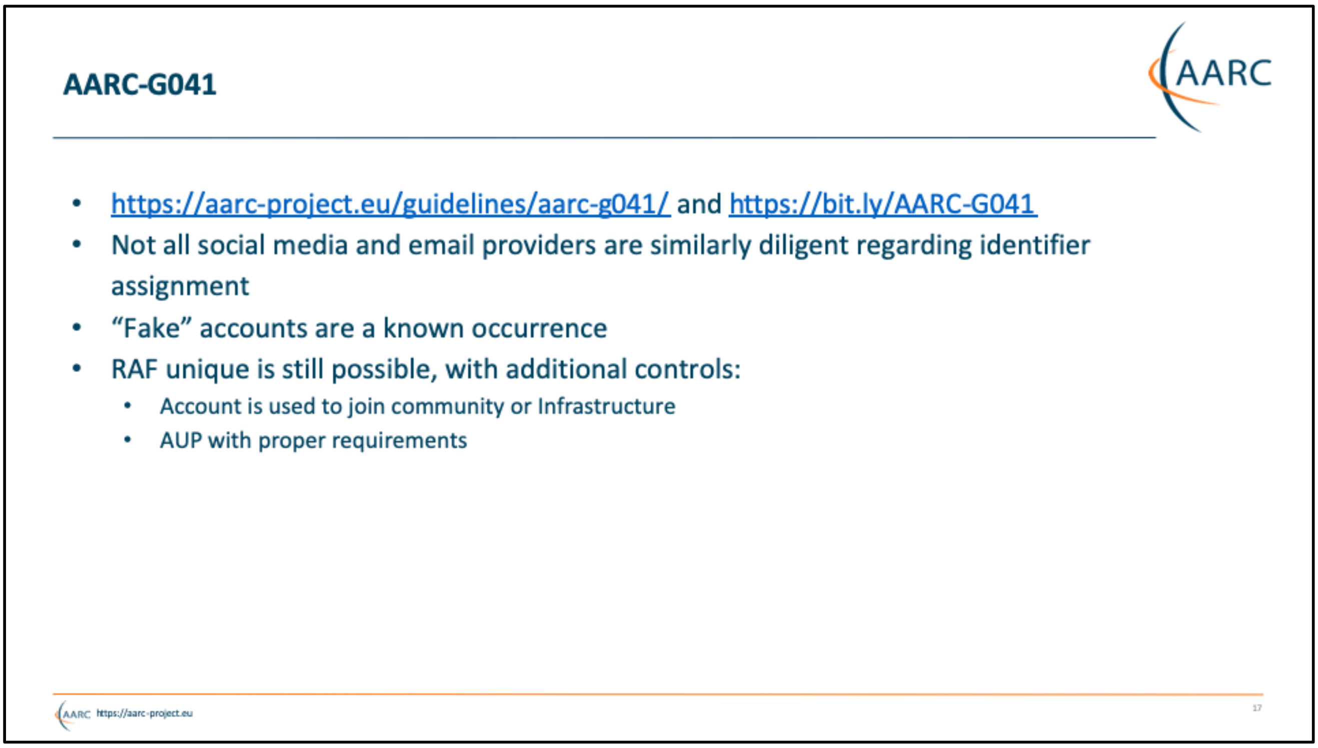
15



AARC Authentication and Authorisation for Research and Collaboration

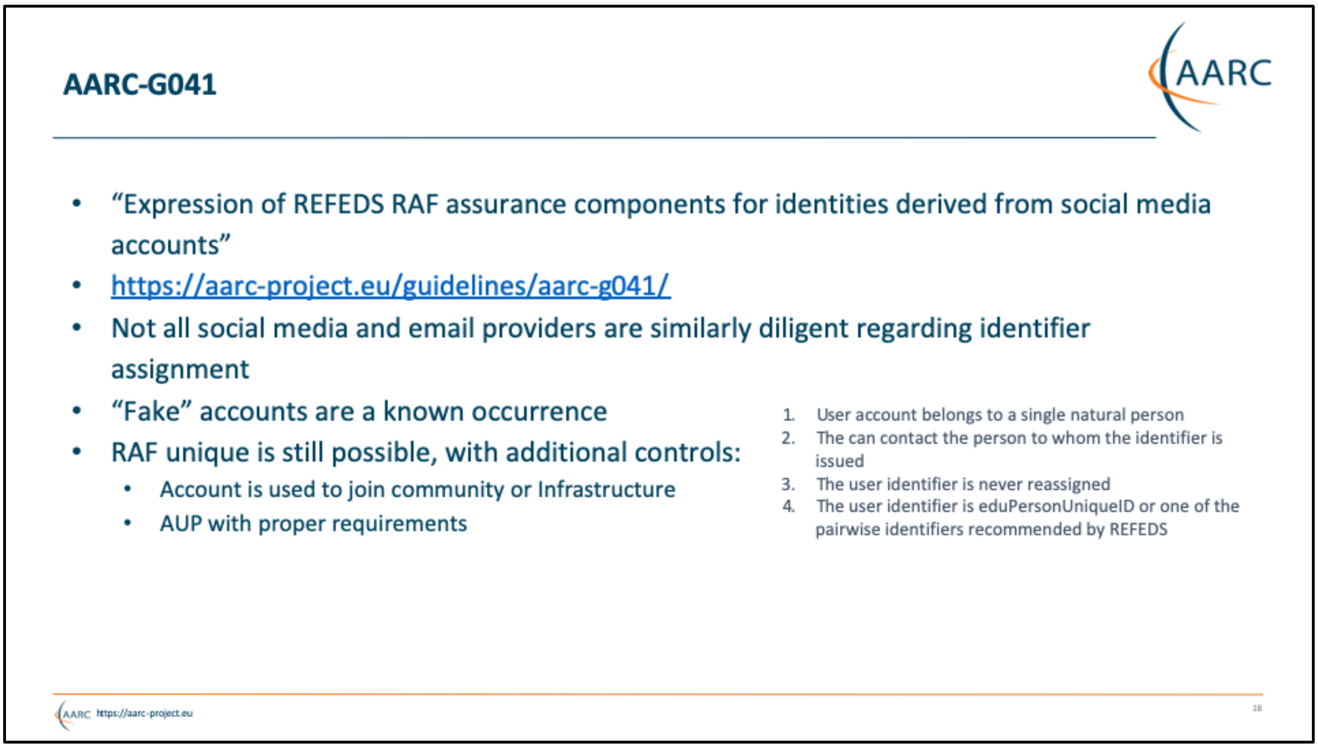
AARC-G041 Expression of REFEDS RAF assurance components for identities derived from social media accounts

AARC-G031 provides guidelines for enabling the AAI of a research collaboration to evaluate the assurance of the identity of a researcher to which grants access to specific resources of the collaboration.



AARC-G041

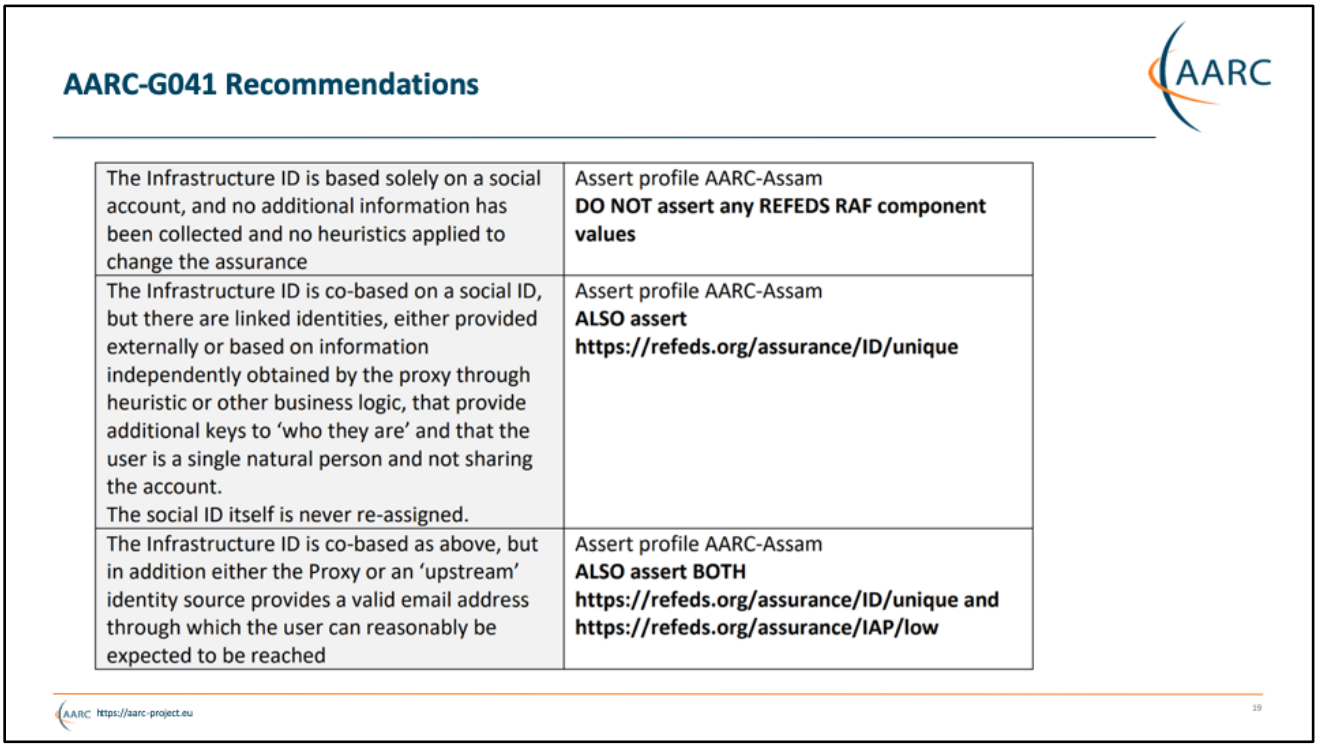
- https://aarc-project.eu/guidelines/aarc-g041/ and https://bit.ly/AARC-G041
- Not all social media and email providers are similarly diligent regarding identifier assignment
- “Fake” accounts are a known occurrence
- RAF unique is still possible, with additional controls:
  - Account is used to join community or Infrastructure
  - AUP with proper requirements



AARC-G041

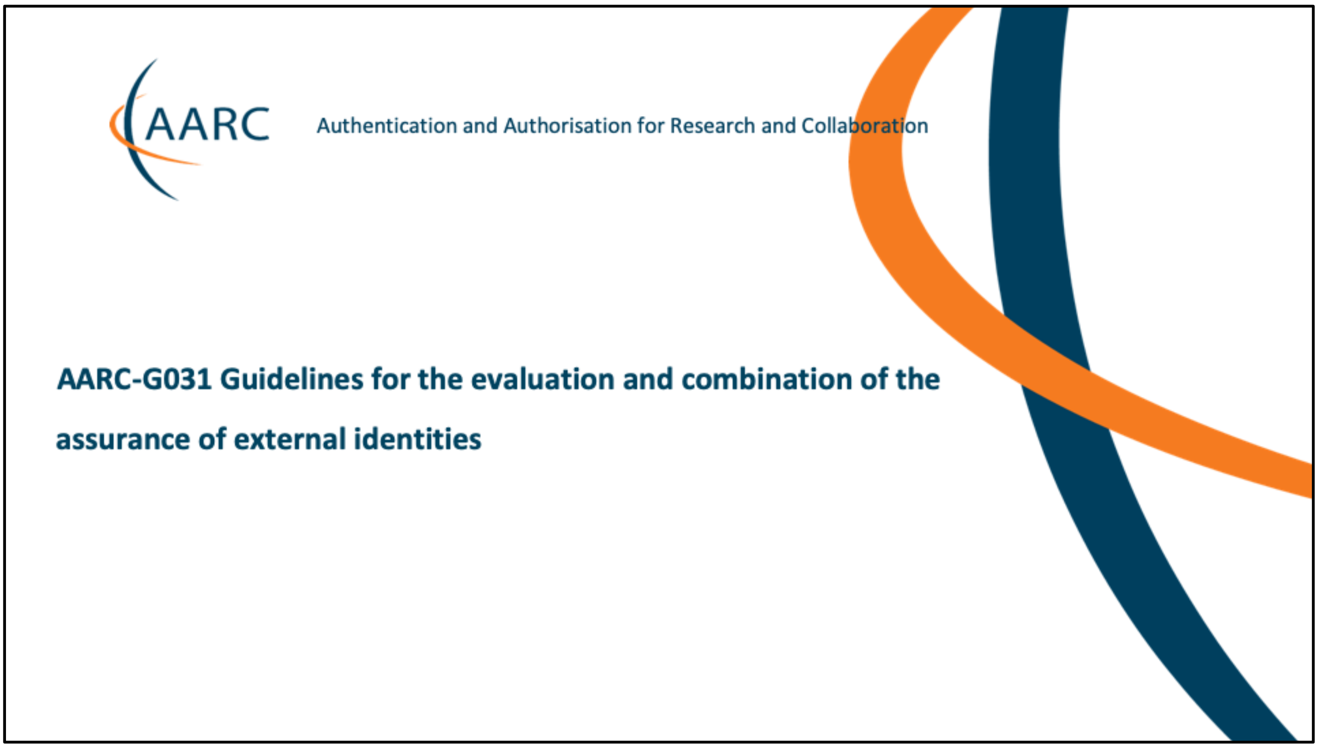
- “Expression of REFEDS RAF assurance components for identities derived from social media accounts”
- https://aarc-project.eu/guidelines/aarc-g041/
- Not all social media and email providers are similarly diligent regarding identifier assignment
- “Fake” accounts are a known occurrence
- RAF unique is still possible, with additional controls:
  - Account is used to join community or Infrastructure
  - AUP with proper requirements

1. User account belongs to a single natural person
2. The can contact the person to whom the identifier is issued
3. The user identifier is never reassigned
4. The user identifier is eduPersonUniqueID or one of the pairwise identifiers recommended by REFEDS



AARC-G041 Recommendations

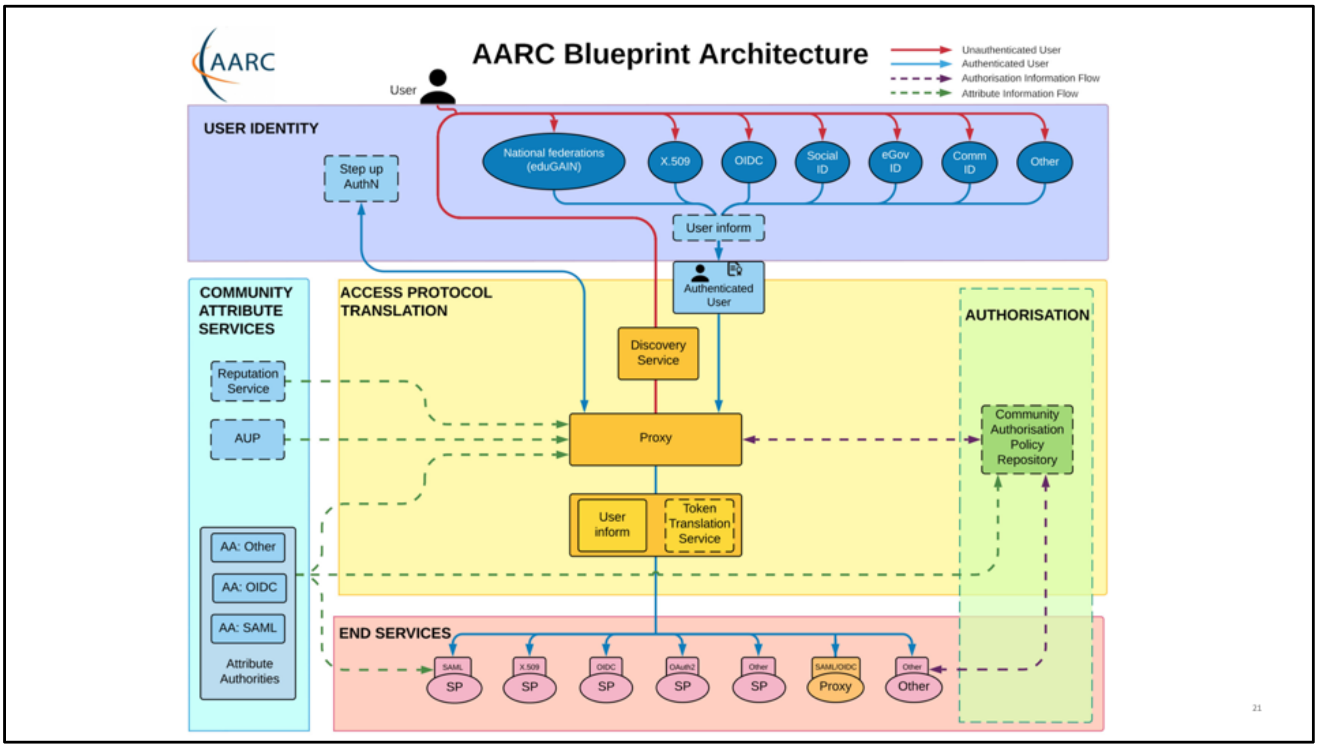
The Infrastructure ID is based solely on a social account, and no additional information has been collected and no heuristics applied to change the assurance	Assert profile AARC-Assam **DO NOT assert any REFEDS RAF component values**
The Infrastructure ID is co-based on a social ID, but there are linked identities, either provided externally or based on information independently obtained by the proxy through heuristic or other business logic, that provide additional keys to 'who they are' and that the user is a single natural person and not sharing the account. The social ID itself is never re-assigned.	Assert profile AARC-Assam **ALSO assert** **https://refeds.org/assurance/ID/unique**
The Infrastructure ID is co-based as above, but in addition either the Proxy or an 'upstream' identity source provides a valid email address through which the user can reasonably be expected to be reached	Assert profile AARC-Assam **ALSO assert BOTH** **https://refeds.org/assurance/ID/unique and** **https://refeds.org/assurance/IAP/low**



AARC Authentication and Authorisation for Research and Collaboration

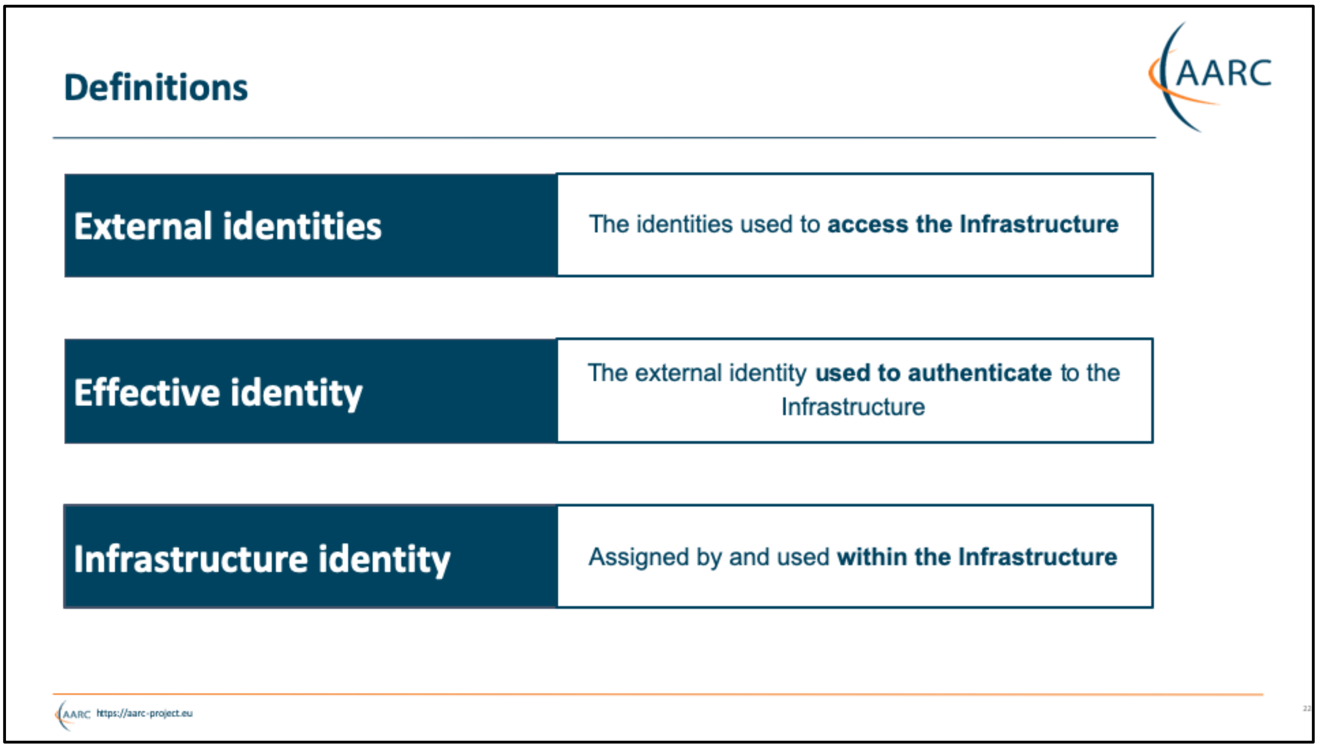
AARC-G031 Guidelines for the evaluation and combination of the assurance of external identities

AARC-G031 provides guidelines for enabling the AAI of a research collaboration to evaluate the assurance of the identity of a researcher to which grants access to specific resources of the collaboration.



A research infrastructure that follows the AARC Blueprint Architecture will set up an AAI based on a central IdP-SP proxy that acts as a gateway for its own services and resources. Infrastructures AAIs rely on existing external identity providers in order to identify and authenticate their users.
The Infrastructures need also to define one or more assurance profiles tailored to a specific risk assessment (think for example at an Infrastructure dedicated to give access to human genomic data sets).

In order to assign an assurance profile to a user, the Infrastructure shall evaluate the assurance components of the external identity, or identities, used to register to the Infrastructure’s AAI. These guidelines provide a method to combine assurance information and to compensate for the lack of it.



Definitions

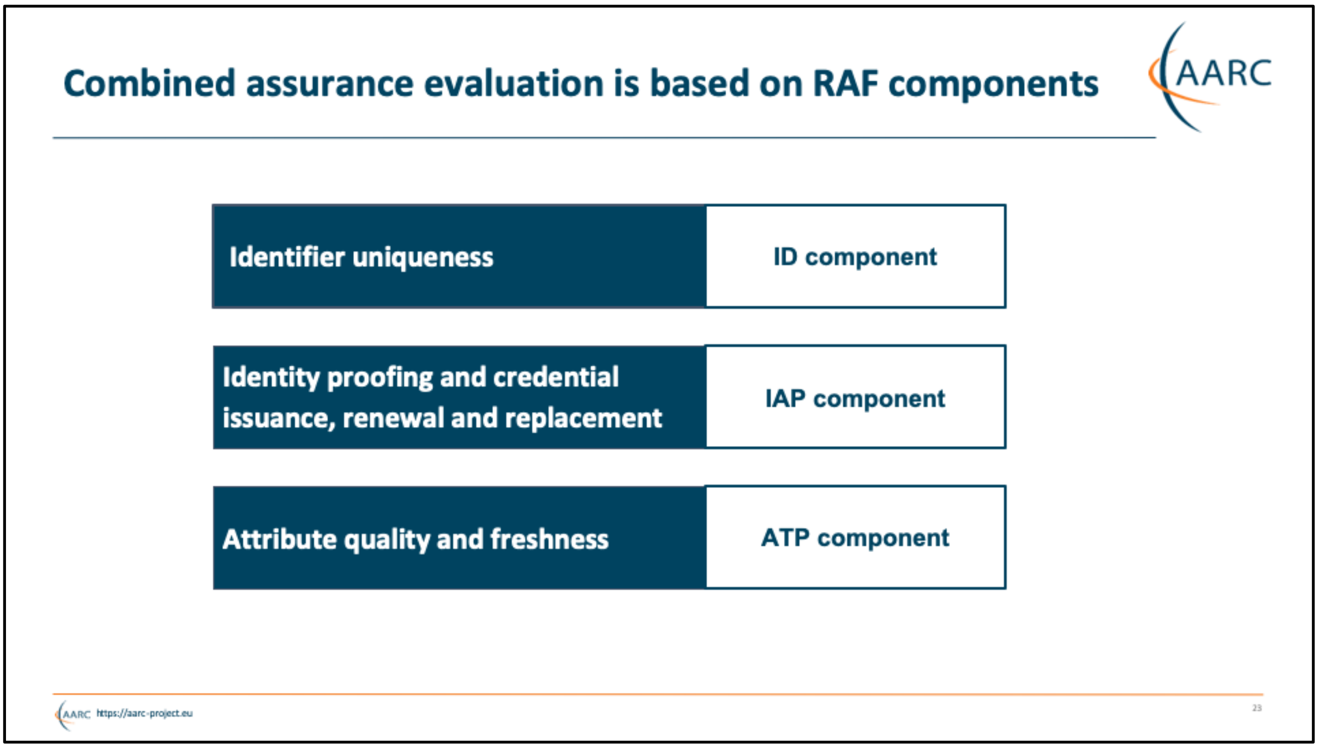
External identities	The identities used to **access the Infrastructure**
Effective identity	The external identity **used to authenticate** to the Infrastructure
Infrastructure identity	Assigned by and used **within the Infrastructure**

https://aarc-project.eu 22

In this context it is assumed that a user has one or more identity provided by an external identity provider (external to and independent of the infrastructure), be they home organisation, social media, community managed virtual organizations, etc. These external identities provide both identity information, such as profile attributes, affiliation and assurance information, and authentication.

When a user links multiple external identities to an Infrastructure, we will refer to the one used to authenticate as the effective identity.

The Infrastructure will assign another identity to the user. An “Infrastructure identity” that will be used within Infrastructure to access local services and resources. Following the lines of the AARC-BPA, this identity will be based on a personal, unique, non-reassignable, non-targeted identifier, and additional attributes containing profile information, as well as group membership and role information. The Infrastructure identity can be associated with a set of credentials issued by the Infrastructure itself, but the identity bootstrap is generally accomplished through an external identity.



Combined assurance evaluation is based on RAF components

Identifier uniqueness	ID component
Identity proofing and credential issuance, renewal and replacement	IAP component
Attribute quality and freshness	ATP component

https://aarc-project.eu

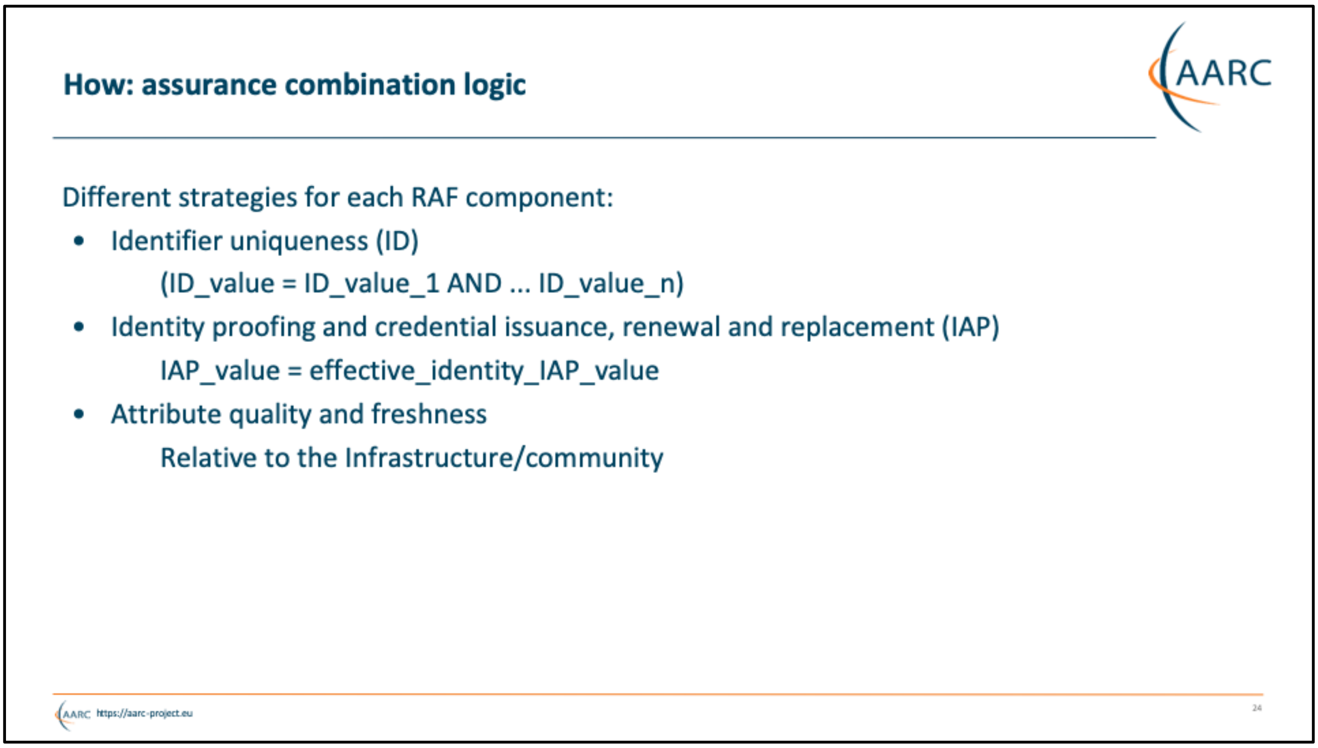
23

How can we combine different assurance information into one?

As already seen, the RAF splits assurance into three separate, orthogonal, components:

- the ID component, which expresses the identifier uniqueness
- the IAP component, or the Identity proofing and credential issuance, renewal and replacement
- The ATP component, that represents the attribute quality and freshness.

The combinations of values of these components result in different assurance profiles which can be tailored to specific requirements.



How: assurance combination logic

Different strategies for each RAF component:

- Identifier uniqueness (ID)

  (ID_value = ID_value_1 AND ... ID_value_n)
- Identity proofing and credential issuance, renewal and replacement (IAP)

  IAP_value = effective_identity_IAP_value
- Attribute quality and freshness

  Relative to the Infrastructure/community

https://aarc-project.eu 24

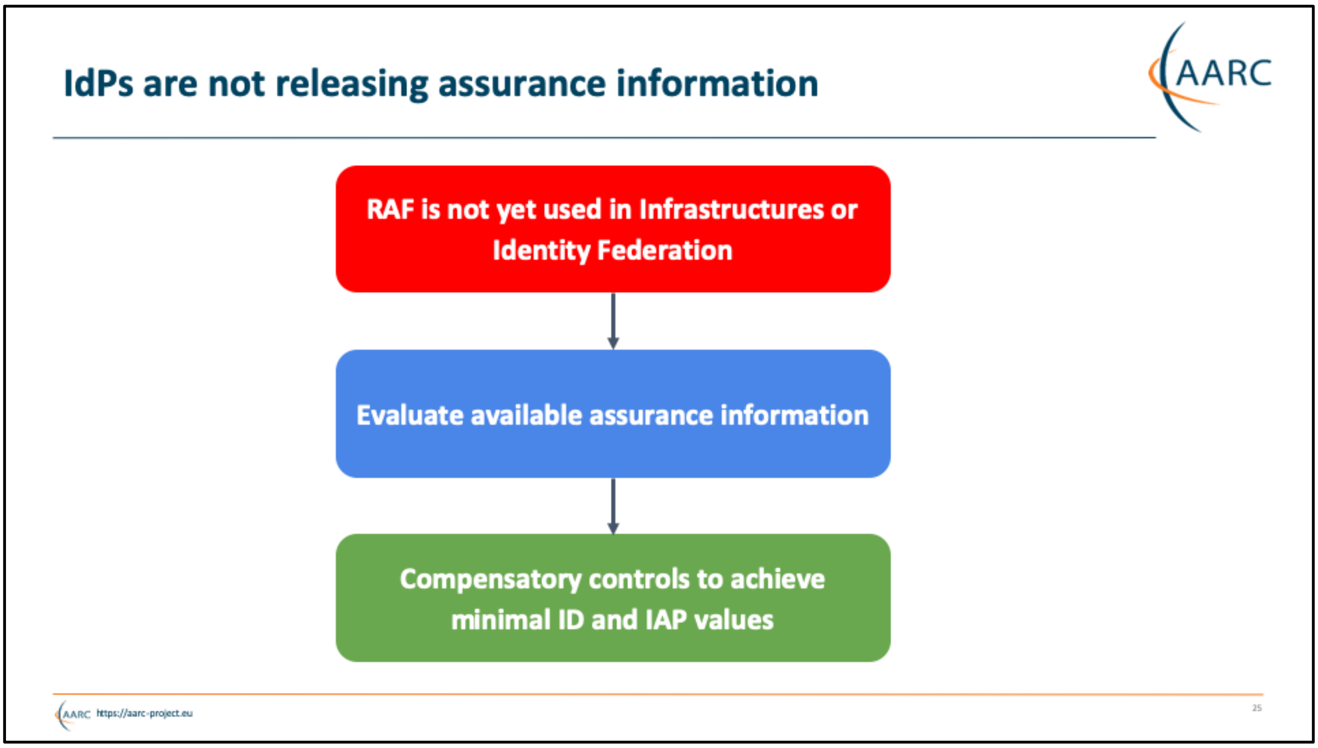
In order to combine assurance component values in a way that makes it possible to implement it in an algorithm, we defined an assurance combination logic. For the ID component the value for the Infrastructure identity SHOULD be calculated with an AND operation where a value `unique` is equal to TRUE and a not available value is equal to FALSE.

The outcome of the combined evaluation will make it impossible to assert the value `unique` for the Infrastructure Identity when one of the linked identities lacks it. This is done with a purpose: to prevent the whitewashing of shared and reassignable accounts through the combination with properly ID `unique` value accounts.

When combining IAP component values that belong to two or more linked identities, the value for the Infrastructure identity will be equivalent to the value of the effective identity.

The ATP component is used to describe the quality and the freshness of some of the attributes that the IdP delivers to the SP and as such it does not make sense to combine ATP values coming from different IdPs. Currently it is used only for the affiliation and specifically to reflect users' departure within a fixed period of time.

Thus, ATP value MUST be relative to the Infrastructure.



IdPs are not releasing assurance information

RAF is not yet used in Infrastructures or Identity Federation

Evaluate available assurance information

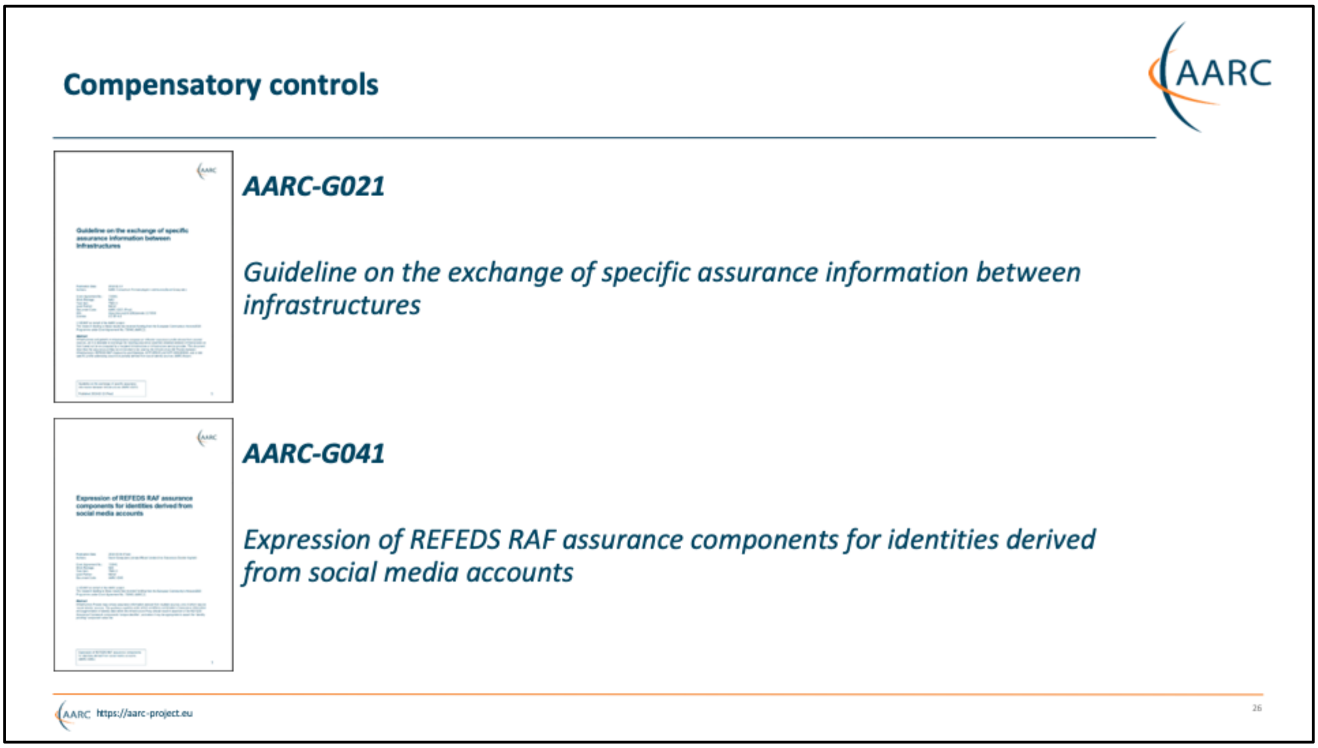
Compensatory controls to achieve minimal ID and IAP values

https://aarc-project.eu

25

As many of us know, currently the adoption rate of the RAF among research Infrastructure and Identity Federations is low, adoption just started. At the same time, many Identity Federations do not have independent assurance profiles on which we can base the assurance evaluation.

When no assurance information is directly provided by the IdP during the authentication, the Infrastructure SHOULD NOT make any assumption on the assurance of the external identities, but it can rely on other evidences and compensatory controls to ascertain the relevant assurance features of the incoming identity, as it will be shown in the following sections on a component by component base.



Compensatory controls

AARC-G021

Guideline on the exchange of specific assurance information between infrastructures

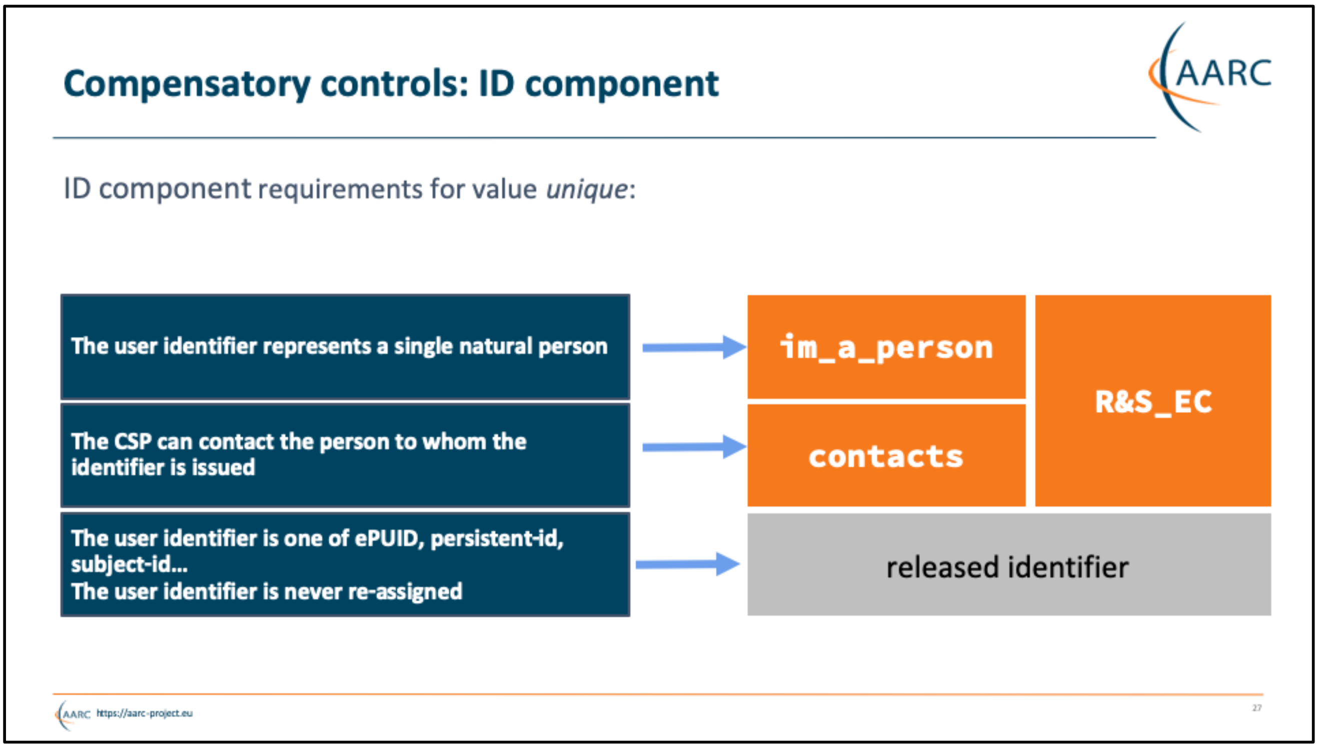
AARC-G041

Expression of REFEDS RAF assurance components for identities derived from social media accounts

https://aarc-project.eu

26

The compensatory controls defined by AARC-G031 are based on *Guideline on the exchange of specific assurance information between infrastructures* and *Expression of REFEDS RAF assurance components for identities derived from social media accounts.*



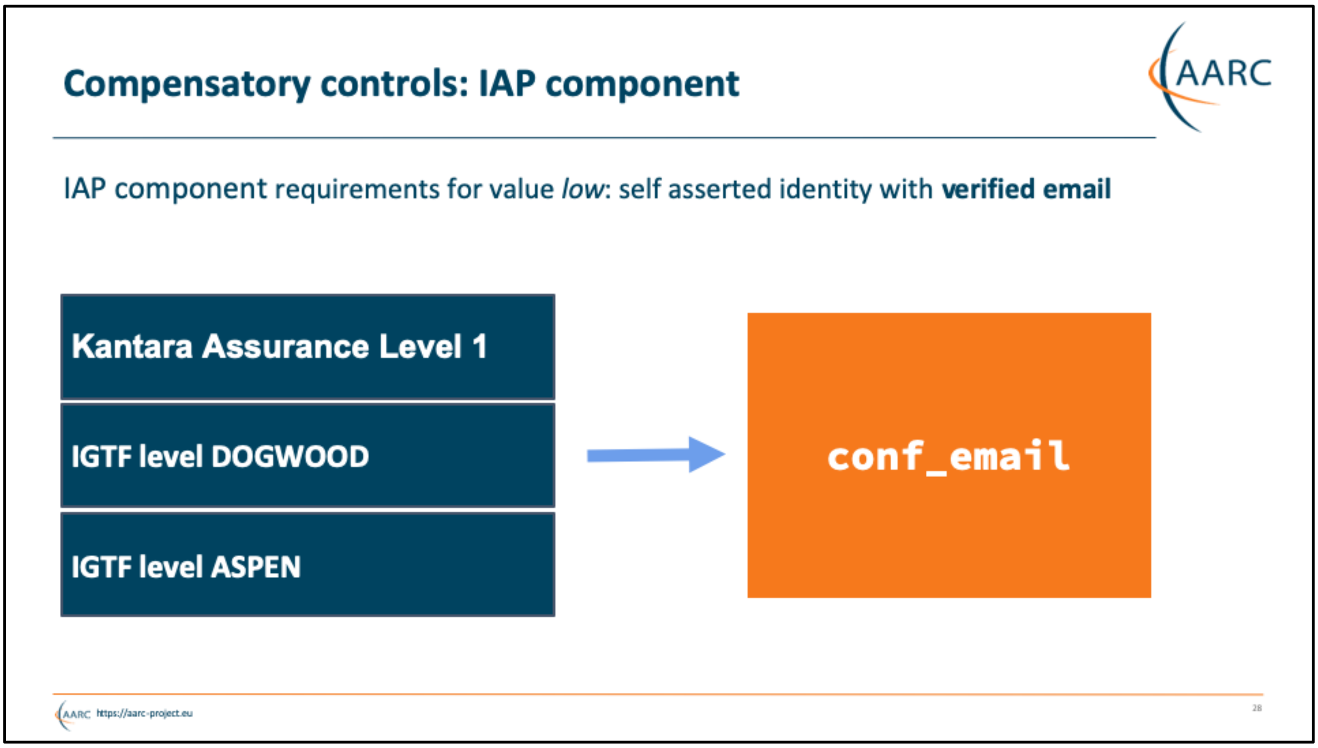
Compensatory controls: ID component

ID component requirements for value *unique*:

The user identifier represents a single natural person
im_a_person
The CSP can contact the person to whom the identifier is issued
contacts
R&S_EC
The user identifier is one of ePUID, persistent-id, subject-id…
The user identifier is never re-assigned
released identifier
https://aarc-project.eu
27

The requirements for the value unique of the ID component are that the user MUST be a single natural person, that the CSP, that is the IdP, can contact the person to whom the identifier is issued and also that the identifier itself is one of ePUID, persistent-id, subject-id, pairwise-id, non-reassigned ePPN and for OIDC the public or the pairwise subject.

To match the “single natural person” requirement we defined the “im_a_person” compensatory control --- which is based on an AUP as we will see --- to match the “contact” we created the “contacts” compensatory control. Both of them can be substituted by the support of the REFEDS R&S EC by the IdP, because.



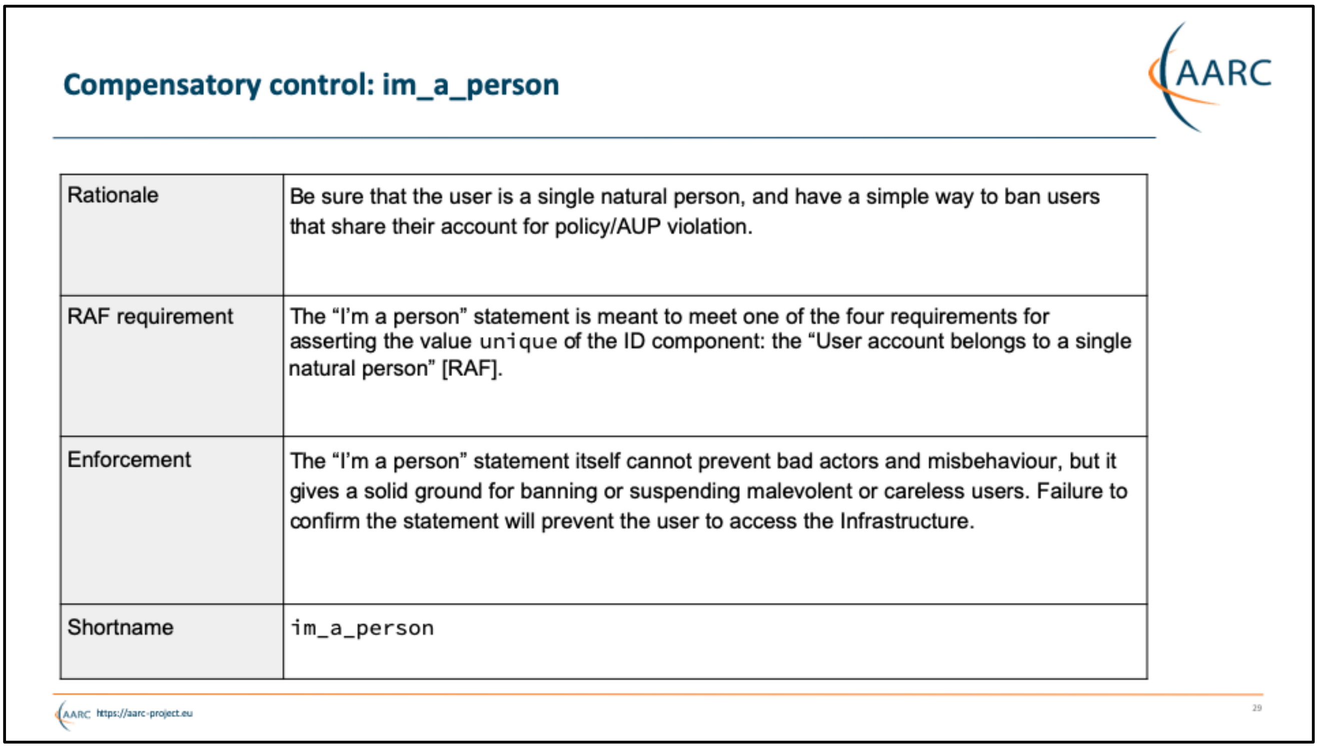
Compensatory controls: IAP component

IAP component requirements for value *low*: self asserted identity with **verified email**

https://aarc-project.eu

28

In the case of the IAP component, which is heavily based on the identity proofing procedures accomplished by the CSP, the compensatory control for the value low is a “verified email”.



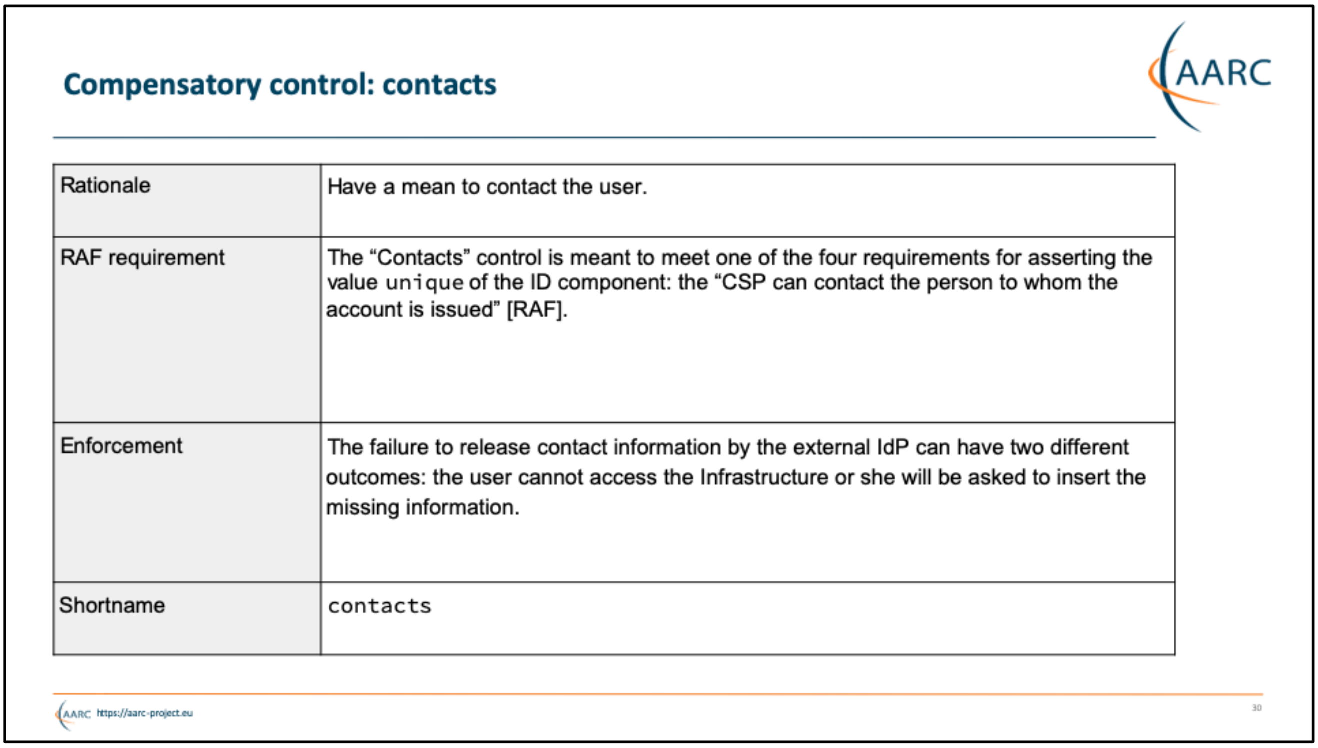
Compensatory control: im_a_person

Rationale	Be sure that the user is a single natural person, and have a simple way to ban users that share their account for policy/AUP violation.
RAF requirement	The "I'm a person" statement is meant to meet one of the four requirements for asserting the value `unique` of the ID component: the "User account belongs to a single natural person" [RAF].
Enforcement	The "I'm a person" statement itself cannot prevent bad actors and misbehaviour, but it gives a solid ground for banning or suspending malevolent or careless users. Failure to confirm the statement will prevent the user to access the Infrastructure.
Shortname	`im_a_person`

https://aarc-project.eu

29

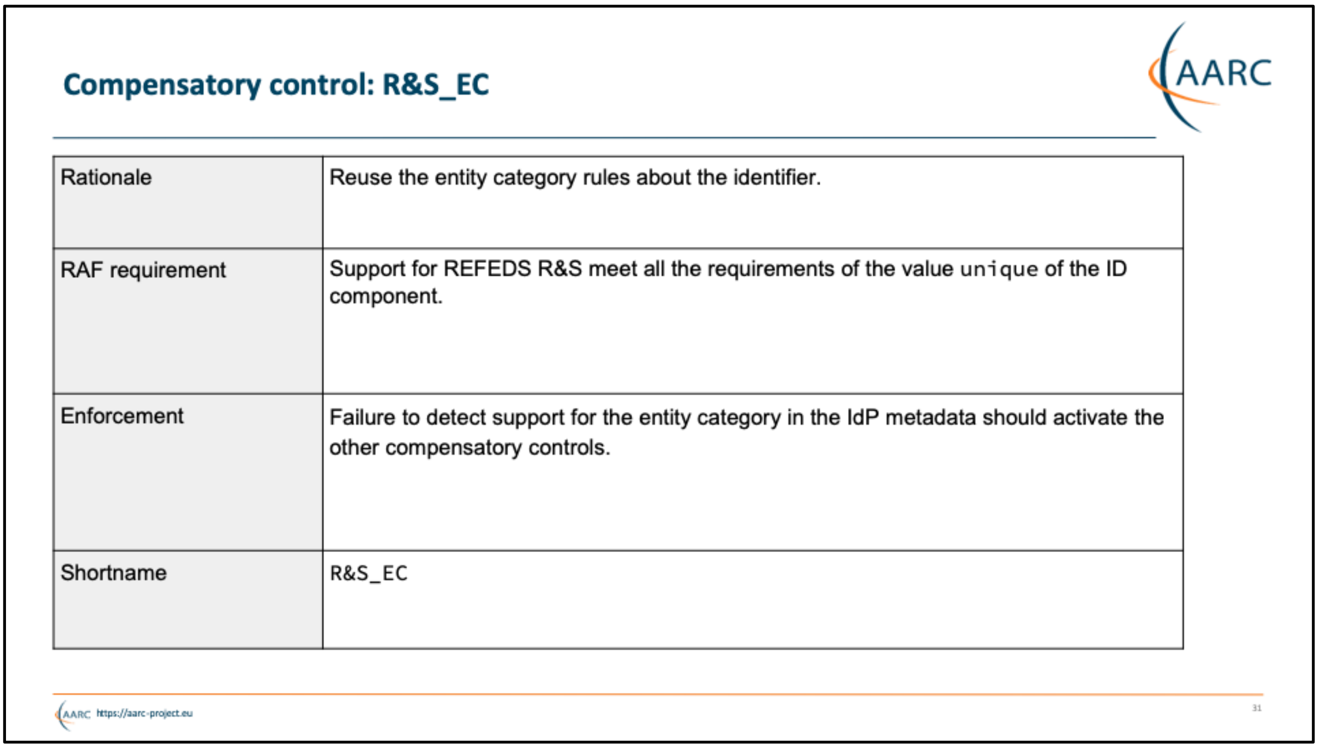
The user registering to the Infrastructure will be required to confirm that she is a single natural person and that she will not share the account with other people. Those requirements MAY also be included in the Infrastructure AUP.



Compensatory control: contacts

Rationale	Have a mean to contact the user.
RAF requirement	The “Contacts” control is meant to meet one of the four requirements for asserting the value `unique` of the ID component: the “CSP can contact the person to whom the account is issued” [RAF].
Enforcement	The failure to release contact information by the external IdP can have two different outcomes: the user cannot access the Infrastructure or she will be asked to insert the missing information.
Shortname	`contacts`

When a user register to the Infrastructure, their (external) identity providers will be required to release contacts information as email or mobile phone number. The “Confirmation mail” compensatory control can substitute “Contacts”, but not vice versa.



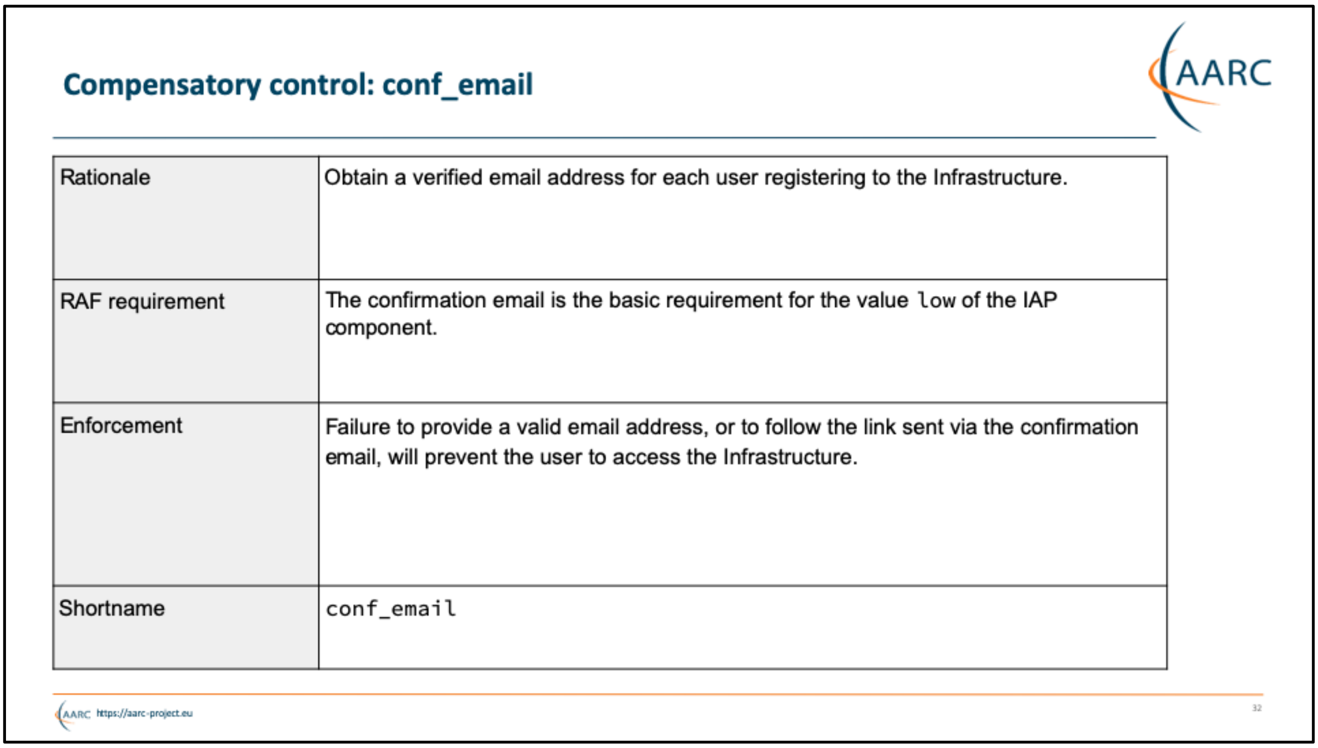
Compensatory control: R&S_EC

Rationale	Reuse the entity category rules about the identifier.
RAF requirement	Support for REFEDS R&S meet all the requirements of the value `unique` of the ID component.
Enforcement	Failure to detect support for the entity category in the IdP metadata should activate the other compensatory controls.
Shortname	`R&S_EC`

https://aarc-project.eu

31

eduGAIN IdPs asserting the support for the REFEDS Research and Scholarship entity category [REFEDS-R&S] commit to release a set of attributes following specific rules on the quality of the identifier and thus qualify for both the single natural person requirement and the “contact provided by the CSP” one.



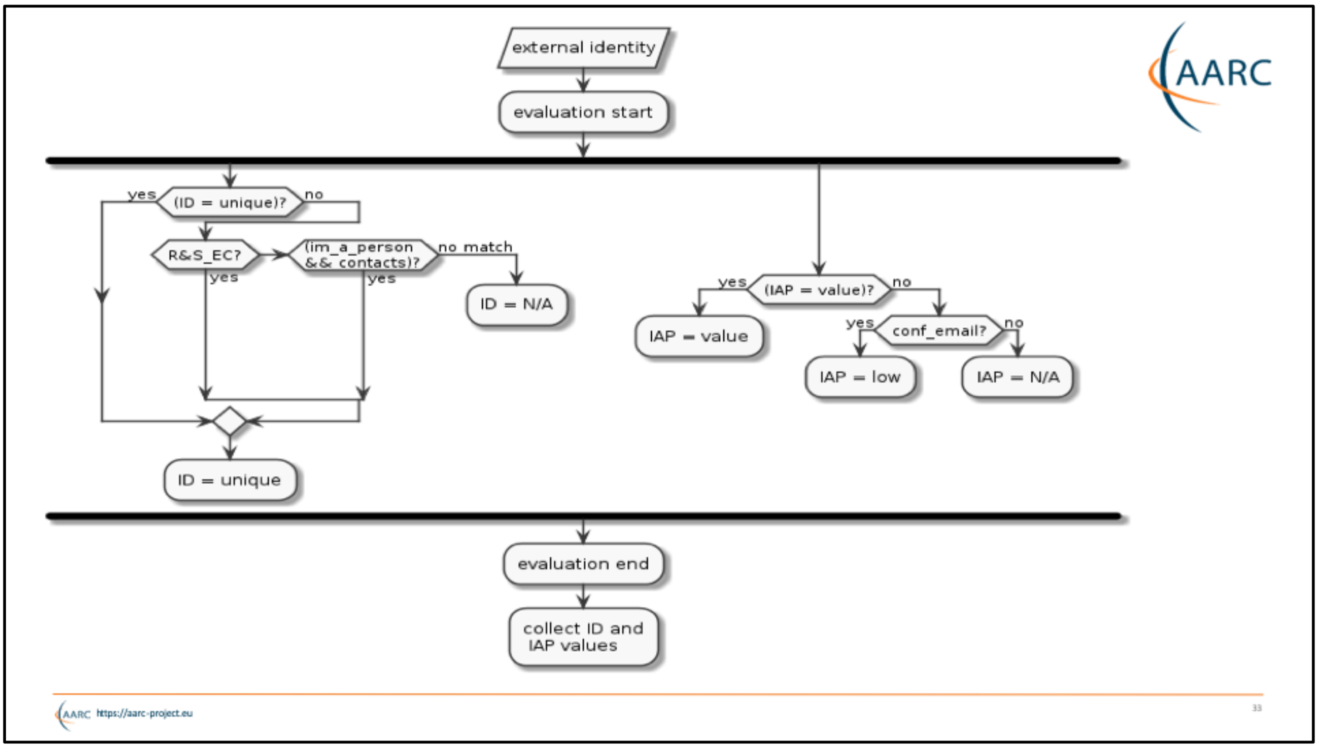
Compensatory control: conf_email

Rationale	Obtain a verified email address for each user registering to the Infrastructure.
RAF requirement	The confirmation email is the basic requirement for the value `low` of the IAP component.
Enforcement	Failure to provide a valid email address, or to follow the link sent via the confirmation email, will prevent the user to access the Infrastructure.
Shortname	`conf_email`

https://aarc-project.eu 32

When a user wants to register to a service, it is common practice to send an email to the provided address with a confirmation link. Once received, the user will follow the link to complete the registration process. The same process will be embraced by the Infrastructure for the users registration.

In this context, the Infrastructure MUST positively verifies that the email is valid and in control of the registering user, which means that this information cannot be extracted or deduced by other attributes, or conveyed with claims such as the OIDC "email_verified" one.



external identity

evaluation start

(ID = unique)?

yes

no

R&S_EC?

yes

(im_a_person && contacts)?

yes

no match

ID = N/A

ID = unique

(IAP = value)?

yes

no

IAP = value

conf_email?

yes

no

IAP = low

IAP = N/A

evaluation end

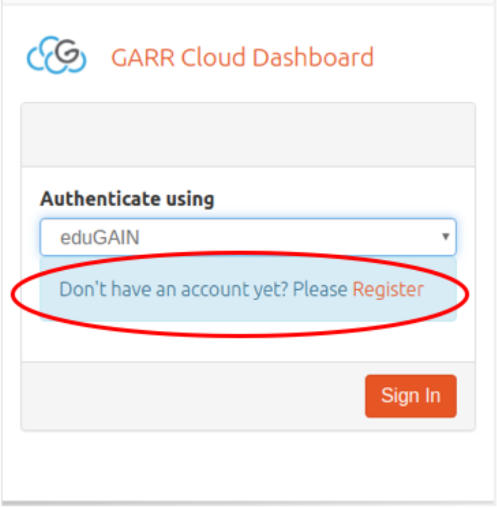
collect ID and IAP values

https://aarc-project.eu

33

In this flowchart we summarized the controls

Where to implement the compensatory controls

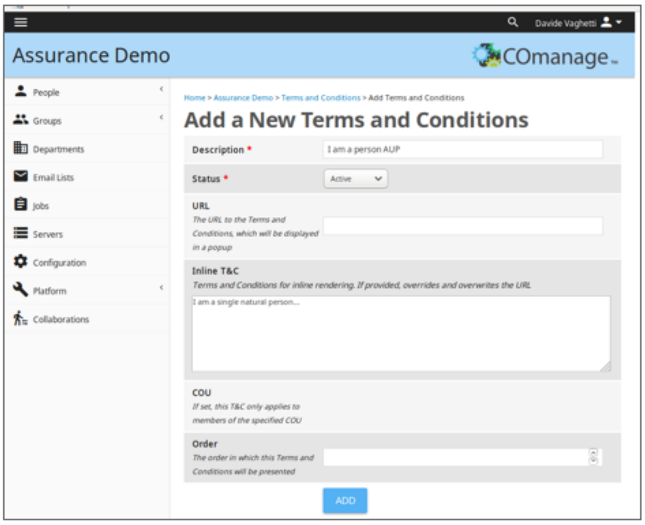


Authenticate using

eduGAIN

Don't have an account yet? Please Register

`im_a_person` compensatory control



Add a New Terms and Conditions

Description * I am a person AUP

Status * Active

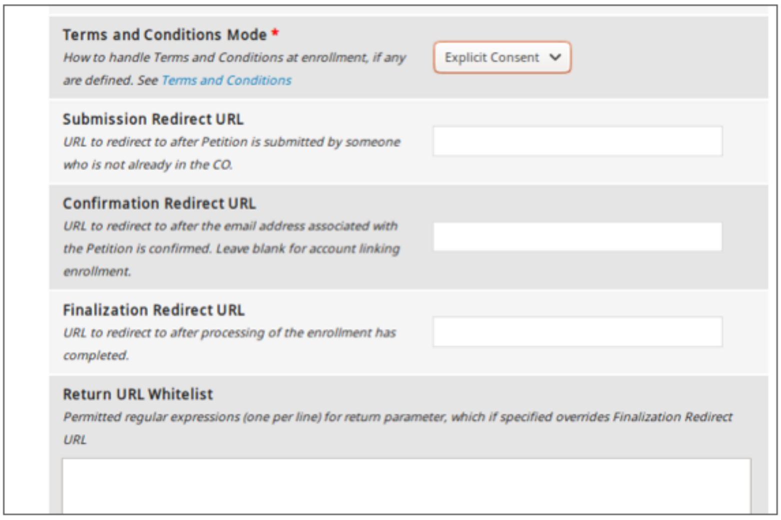
URL
The URL to the Terms and Conditions, which will be displayed in a popup

Inline T&C
Terms and Conditions for inline rendering. If provided, overrides and overwrites the URL
I am a single natural person...

COU
If set, this T&C only applies to members of the specified COU

Order
The order in which this Terms and Conditions will be presented

`im_a_person` compensatory control



Terms and Conditions Mode *

How to handle Terms and Conditions at enrollment, if any are defined. See Terms and Conditions

Explicit Consent

Submission Redirect URL

URL to redirect to after Petition is submitted by someone who is not already in the CO.

Confirmation Redirect URL

URL to redirect to after the email address associated with the Petition is confirmed. Leave blank for account linking enrollment.

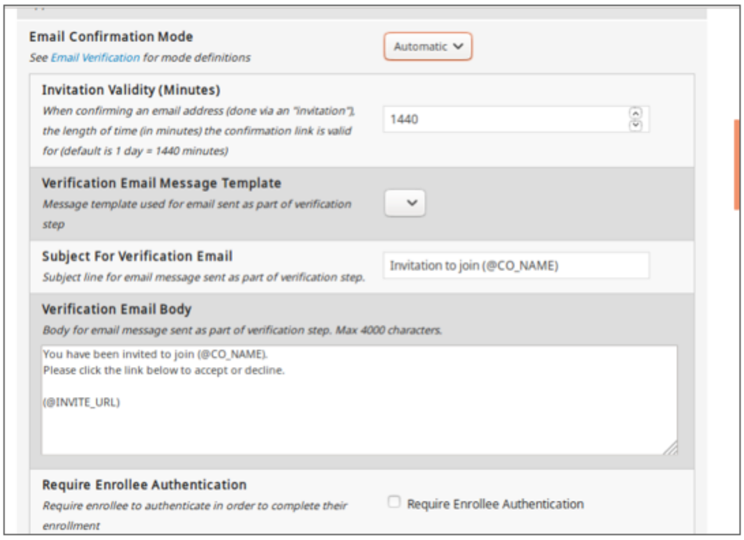
Finalization Redirect URL

URL to redirect to after processing of the enrollment has completed.

Return URL Whitelist

Permitted regular expressions (one per line) for return parameter, which if specified overrides Finalization Redirect URL

conf_email compensatory control



Email Confirmation Mode
See Email Verification for mode definitions
Automatic

Invitation Validity (Minutes)
When confirming an email address (done via an "invitation"), the length of time (in minutes) the confirmation link is valid for (default is 1 day = 1440 minutes)
1440

Verification Email Message Template
Message template used for email sent as part of verification step

Subject For Verification Email
Subject line for email message sent as part of verification step.
Invitation to join (@CO_NAME)

Verification Email Body
Body for email message sent as part of verification step. Max 4000 characters.

```
You have been invited to join (@CO_NAME).
Please click the link below to accept or decline.

(@INVITE_URL)
```

Require Enrollee Authentication
Require enrollee to authenticate in order to complete their enrollment
□ Require Enrollee Authentication

JOIN the appint mailing list: appint@lists.geant.org
https://lists.geant.org/sympa/info/appint

Thank you

Any Questions?

uros.stevanovic@kit.edu
davide.vaghetti@garr.it

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).

https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0
https://aarc-project.eu/guidelines/aarc-g031/
https://aarc-project.eu/guidelines/aarc-g021/
https://aarc-project.eu/guidelines/aarc-g041/
https://wiki.refeds.org/display/ASS/Assurance+Home