Authentication and Authorisation for Research and Collaboration

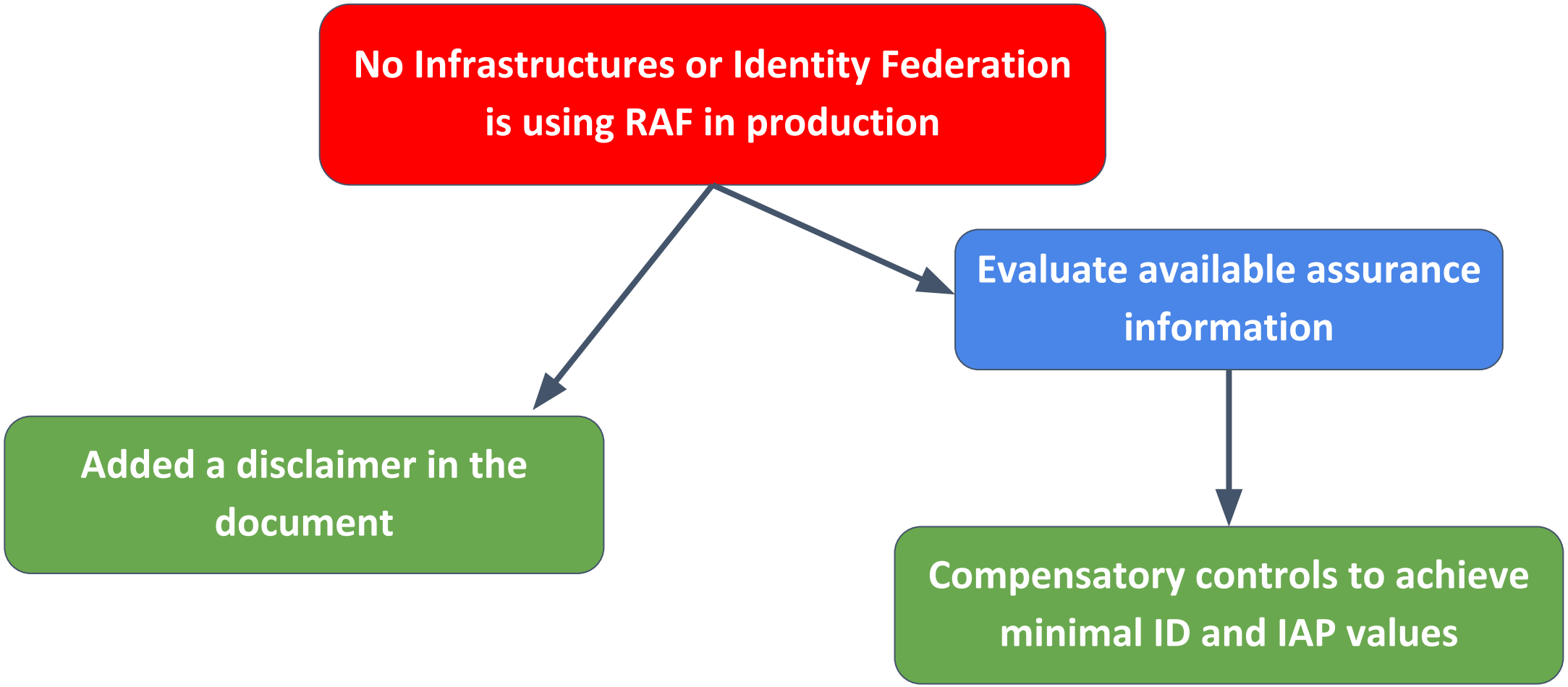
Combined assurance evaluation and account linking

Davide Vaghetti
JRA1.3 TL
GARR

AARC2 All Hands Meeting, Athens
11 Apr 2018

FINAL DRAFT

RAF is draft


No Infrastructures or Identity Federation is using RAF in production
Evaluate available assurance information
Added a disclaimer in the document
Compensatory controls to achieve minimal ID and IAP values

Definitions

Infrastructure identity

The identity assigned by the Infrastructure.

External identities

The identities coming from IdPs external to and independent from the Infrastructure.

Identity linking

The Infrastructure leverage identity linking to provide access to the services.

Effective identity

The identity that will be used to authenticate to the Infrastructure.

Compensatory control: im_a_person

3.1.1. I'm a person

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.

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`

Compensatory control: contacts

3.1.2. 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.

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`

Compensatory control: R&S_EC

3.1.3. Research and Scholarship entity category

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.

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`

Compensatory control: conf_email

3.1.4. Confirmation email

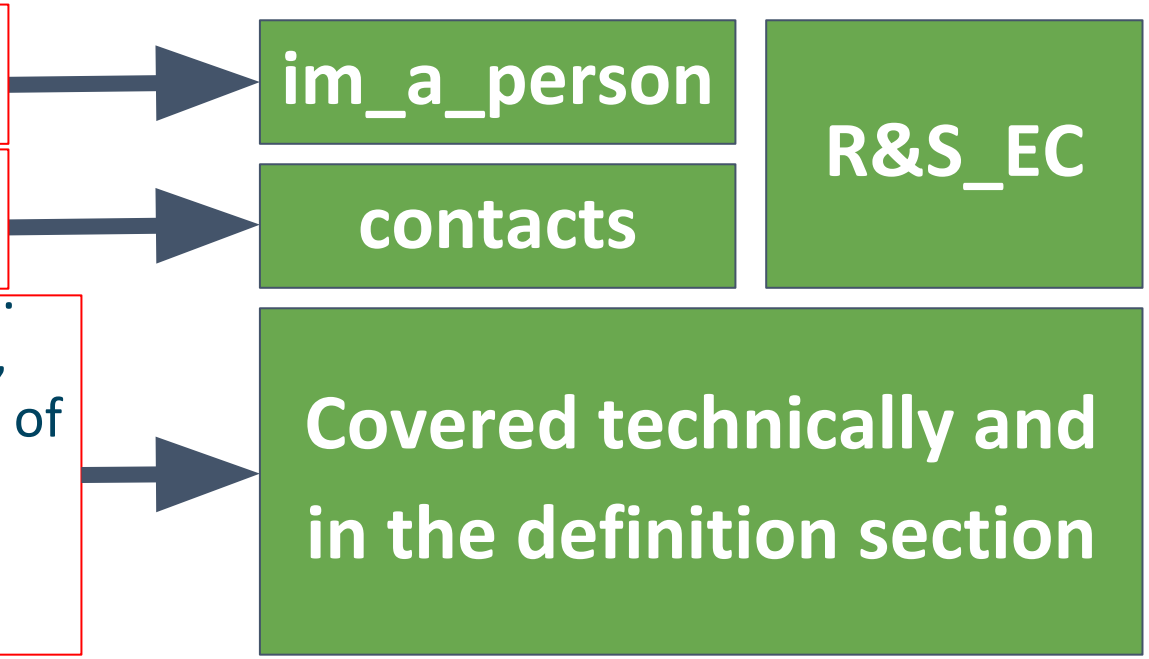
When a user wants to register to a service, it is common practice to send an email to the provided address with a confirmation link. Once received, the user will follow the link to complete the registration process. The same process will be embraced by the Infrastructure for the users registration.

Rationale	Obtain a verified email address for each user registering to the Infrastructure.
RAF requirement	The confirmation email 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`

Compensatory controls: ID component

ID component requirements for value *unique*:

1. User account belongs to a single natural person.
2. CSP can contact the person to whom the account is issued.
3. The user identifier will not be re-assigned.
4. The user identifier is eduPersonUniqueID, OpenID Connect sub (type: public) or one of the pairwise identifiers recommended by REFEDS.

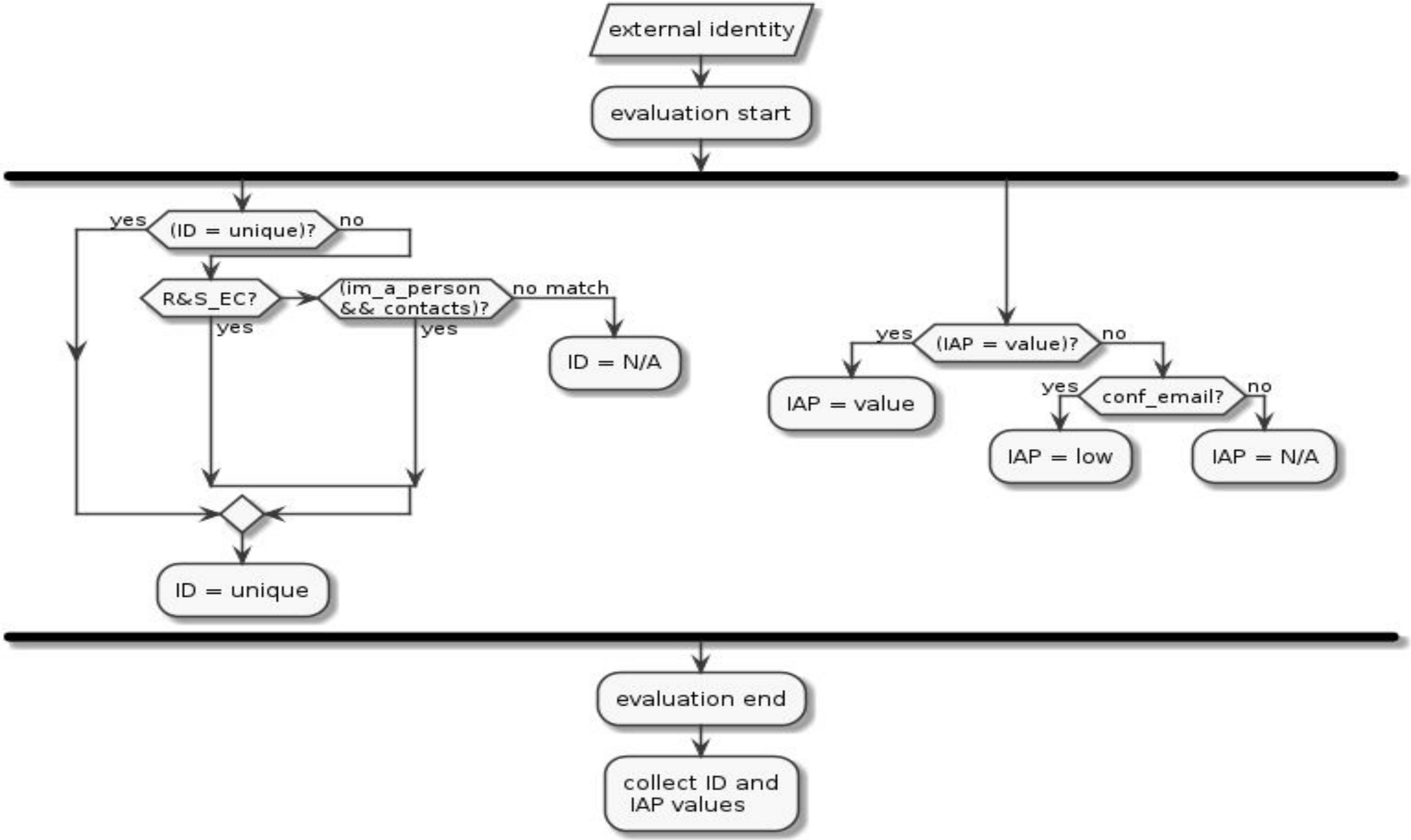


Compensatory controls: IAP component

IAP component requirements for value *low*:

either

- sections 5.1.2-5.1.2.9 and section 5.1.3 of Kantara assurance level 1 [Kantara SAC]
- IGTF level DOGWOOD [IGTF]
- IGTF level ASPEN [IGTF]


external identity
evaluation start
yes
(ID = unique)?
no
R&S_EC?
yes
(im_a_person
&& contacts)?
yes
no match
ID = N/A
ID = unique
yes
(IAP = value)?
no
IAP = value
yes
conf_email?
no
IAP = low
IAP = N/A
evaluation end
collect ID and
IAP values

Thank you

Any Questions?

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).