# Combined assurance evaluation and account linking updates

Authentication and Authorisation for Research and Collaboration

**Davide Vaghetti**

JRA1.3 TL

GARR

AARC2 All Hands Meeting, Amsterdam

22 Nov 2017

# Combined assurance evaluation and account linking

## The beginning

- took an agnostic point of view
- embraced REFEDS Assurance Framework (RAF) as our reference
- no more levels of assurance, but assurance components and profiles

## Definitions

- BPA infrastructure identity (the one assigned by the infra)
- account linking: inaccurate, switched to identity linking
- assurance components from RAF

# First developments

## Benchmarking social logins on RAF components

- **WARNING: github policy on account name reassignability:**

  if you delete your user account:

  *The account name also becomes available to anyone else to use on a new account* [1]
- lack of information for most of the RAF assurance components

## Combined assurance evaluation components

- **identifier uniqueness is a prerequisite** for both solid account linking and combined assurance evaluation
- **ruled out authentication**: no combination is possible, authentication assurance value is related to the authenticating identity

[1] https://help.github.com/articles/deleting-your-user-account/

# Combined assurance components evaluation matrix

| Assurance components values | $PREFIX$/IAP/assumed | $PREFIX$/IAP/verified | N/A | $PREFIX$/ATP/ePA-1m | N/A |
|---|---|---|---|---|---|
| $PREFIX$/IAP/assumed | $PREFIX$/IAP/assumed | $PREFIX$/IAP/verified | $PREFIX$/IAP/assumed | | |
| $PREFIX$/IAP/verified | $PREFIX$/IAP/verified | $PREFIX$/IAP/verified | $PREFIX$/IAP/verified | | |
| N/A | $PREFIX$/IAP/assumed | $PREFIX$/IAP/verified | N/A | | |
| $PREFIX$/ATP/ePA-1m | | | | $PREFIX$/ATP/ePA-1m | $PREFIX$/ATP/ePA-1m |
| N/A | | | | $PREFIX$/ATP/ePA-1m | N/A |

LINKED IDENTITY A

LINKED IDENTITY B

INFRASTRUCTURE IDENTITY

# Issues so far

- RAF (understandably) is a moving target
- IPA values for linked account expiration policy
- How to manage the no available affiliation use case
- Components value freshness/update process
- (risk) Linking to weak password institutional account:
  - is the related IPA value still reliable?
  - What if I link the weak password institutional account to a MFA social one?
  - **Possible solutions:**
    - **no account linking for weak password account**
    - **complementary security check (not trivial)**

# 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).