REFEDS Assurance Framework (RAF)

IDEM DAY 2018
Roma 7-9 Giugno 2018
Davide Vaghetti - IDEM GARR AAI
davide.vaghetti@garr.it

REFEDS Assurance Framework

- AARC – Authentication and Authorisation for Research & Collaboration
  - Progetto finanziato dalla Commissione Europea
  - Fase 1 Maggio 2015 - Aprile 2017, Fase 2 Maggio 2017 - Aprile 2019
  - Coordinato da GEANT
  - 20 partner: research infrastructure, electronic infrastructure, operatori di federazione, progetti internazionali
  - **Forte partecipazione di GARR (secondo partecipante per numero di PM)**
  - https://aarc-project.eu/
- AARC NA3 Task 1: Level of Assurance (LoA)
  - Recommendations on Minimal Assurance Level Relevant for Low-risk Research Use Cases, 11/2015
    - https://aarc-project.eu/wp-content/uploads/2015/11/MNA31-Minimum-LoA-level.pdf
  - Differentiated LoA recommendations for policy and practices of identity and attribute providers, applicable to research use cases, 4/2017
    - https://aarc-project.eu/wp-content/uploads/2017/04/DNA3.1-Differentiated-Assurance.pdf

AARC Minimal AL for low-risk R&E

- Gli account delle organizzazioni devono essere assegnati solo ad utenti identificabili
- Gli identificatori assegnati devono essere persistenti
- Le procedure di verifica dell'identità devono essere documentate
- L'autenticazione basata su password è accettabile se accompagnata se rispetta buone pratiche
- L'affiliazione (ePA/ePSA) deve essere aggiornata tempestivamente in caso di cessazione del rapporto
- Proposto online tool di auto valutazione e pubblicazione del rispetto dei requisiti

REFEDS Assurance WG

Nel 2016 è stato creato il REFEDS Assurance Working Group:

- Scopo: prendere le raccomandazioni di AARC come punto di partenza e trasformarle in specifiche
- Aperto a tutti i membri di REFEDS - **NON SOLO** ai federation operator
- Internazionale: partecipanti da Europa, US, Canada, Australia
- Trasversale: federation operator e comunità della ricerca

REFEDS Assurance Framework 1.0 draft (2017/4/21)
https://wiki.refeds.org/x/JwBYAQ

REFEDS Assurance Framework 1.0

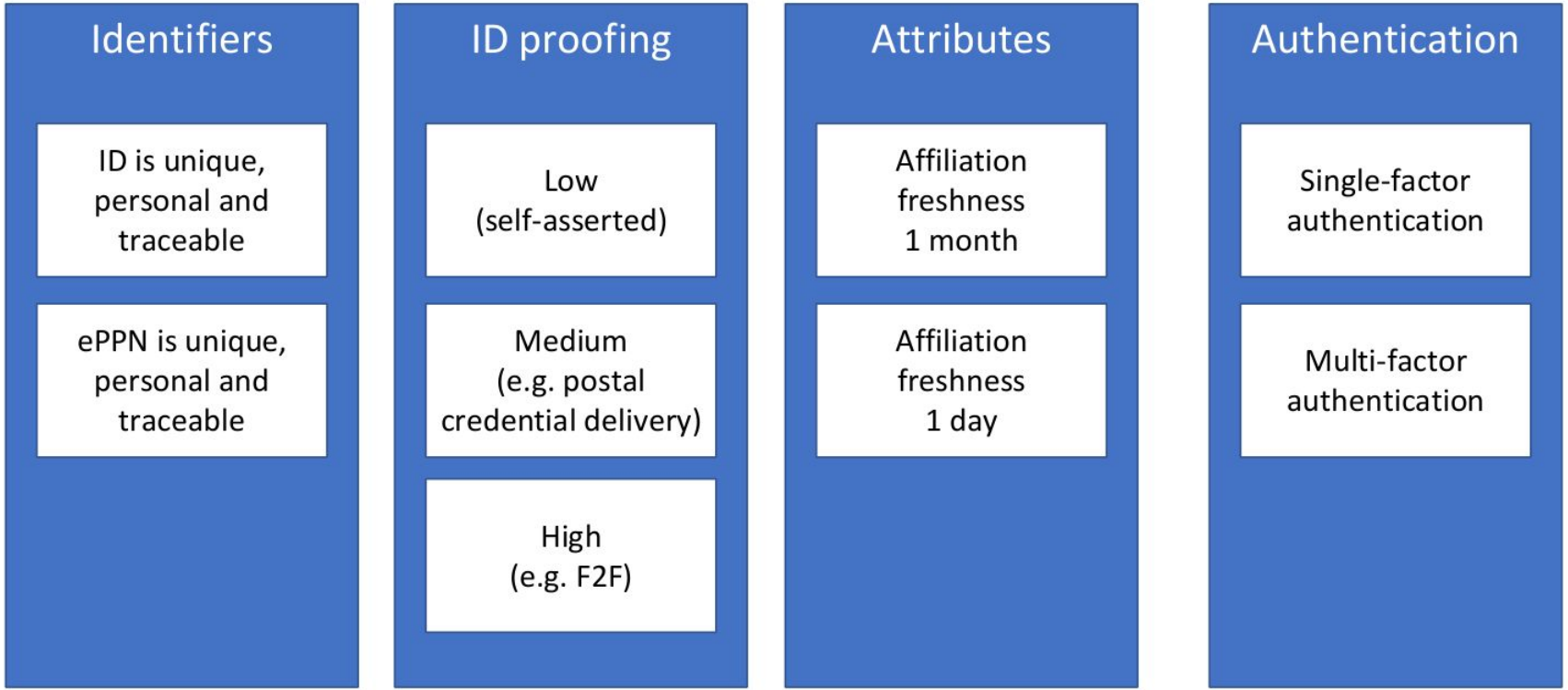
- **Multidimensionale**
  - Opposto ai framework monolitici basati su LoA
  - Assurance suddivisa in 4 dimensioni
  - Proposti due assurance profile
- **Semplice**
  - Lo scopo è l'adozione: più complicate sono le specifiche, minore sarà l'adozione
- **Non reinventa la ruota**
  - Specifiche e framework già esistenti: ITU X.1254, eIDAS LoA, NIST SP 800-63-3, Kantara Identity Assurance Framework, IGTF Levels of Authentication Assurance
- **Trasversale**
  - Pensato sia per le federazioni di identità della ricerca e dell'educazione, sia per le comunità della ricerca.

RAF update - Draft 2 Maggio 2018

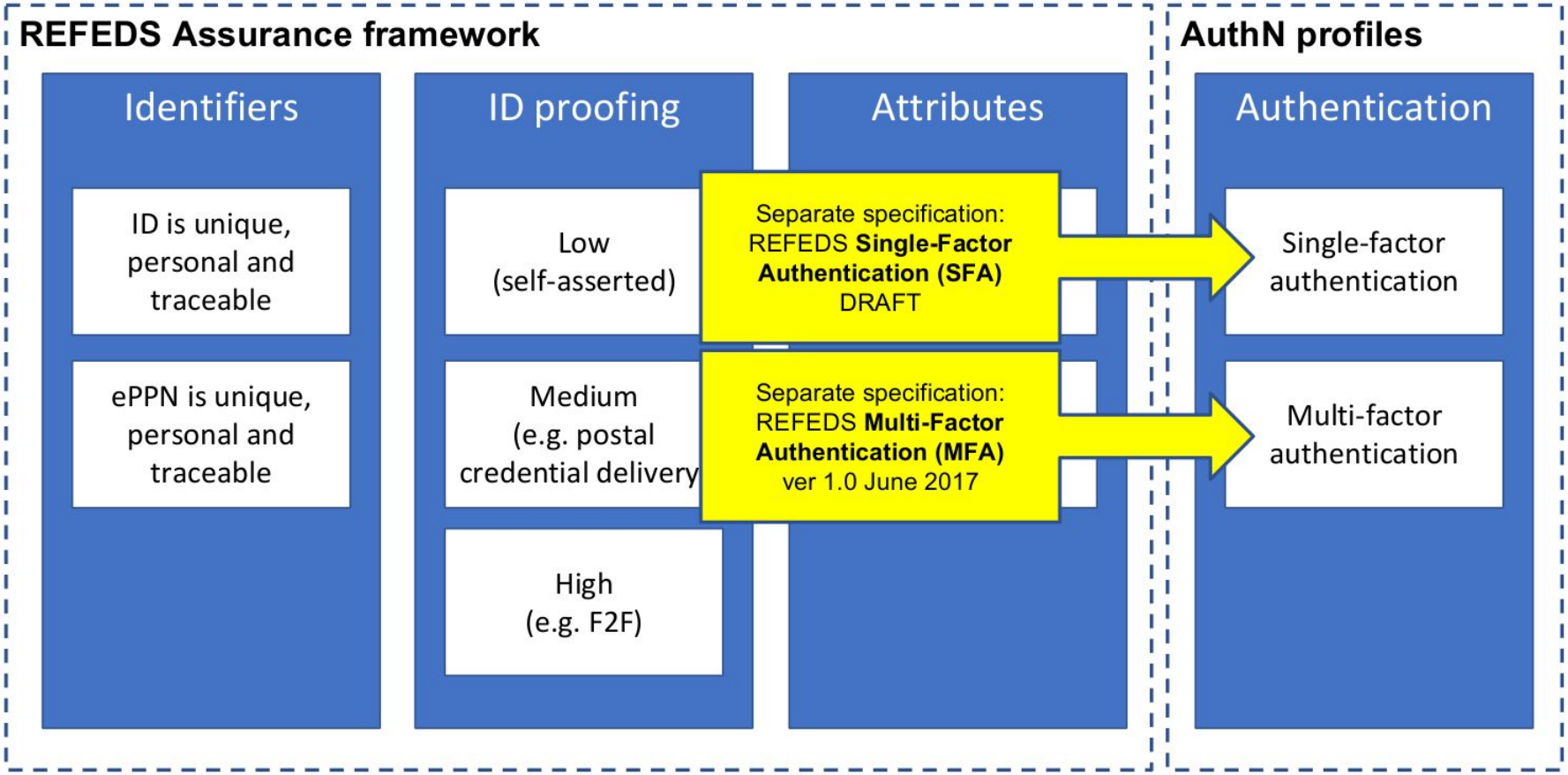
CONSULTAZIONE REFEDS IN CORSO

- **Multidimensionale**
  - Opposto ai framework monolitici basati su LoA
  - ~~**Assurance suddivisa in 4 dimensioni**~~
  - **Assurance suddivisa in 3 dimensioni**
  - **Authentication Assurance non più parte di RAF - specifiche separate sempre a cura di REFEDS**
  - Proposti due assurance profile
- **Semplice**
  - Lo scopo è l'adozione: più complicate sono le specifiche, minore sarà l'adozione
- **Non reinventa la ruota**
  - Specifiche e framework già esistenti: ITU X.1254, eIDAS LoA, NIST SP 800-63-3, Kantara Identity Assurance Framework, IGTF Levels of Authentication Assurance
- **Trasversale**
  - Pensato sia per le federazioni di identità della ricerca e dell'educazione, sia per le comunità della ricerca.

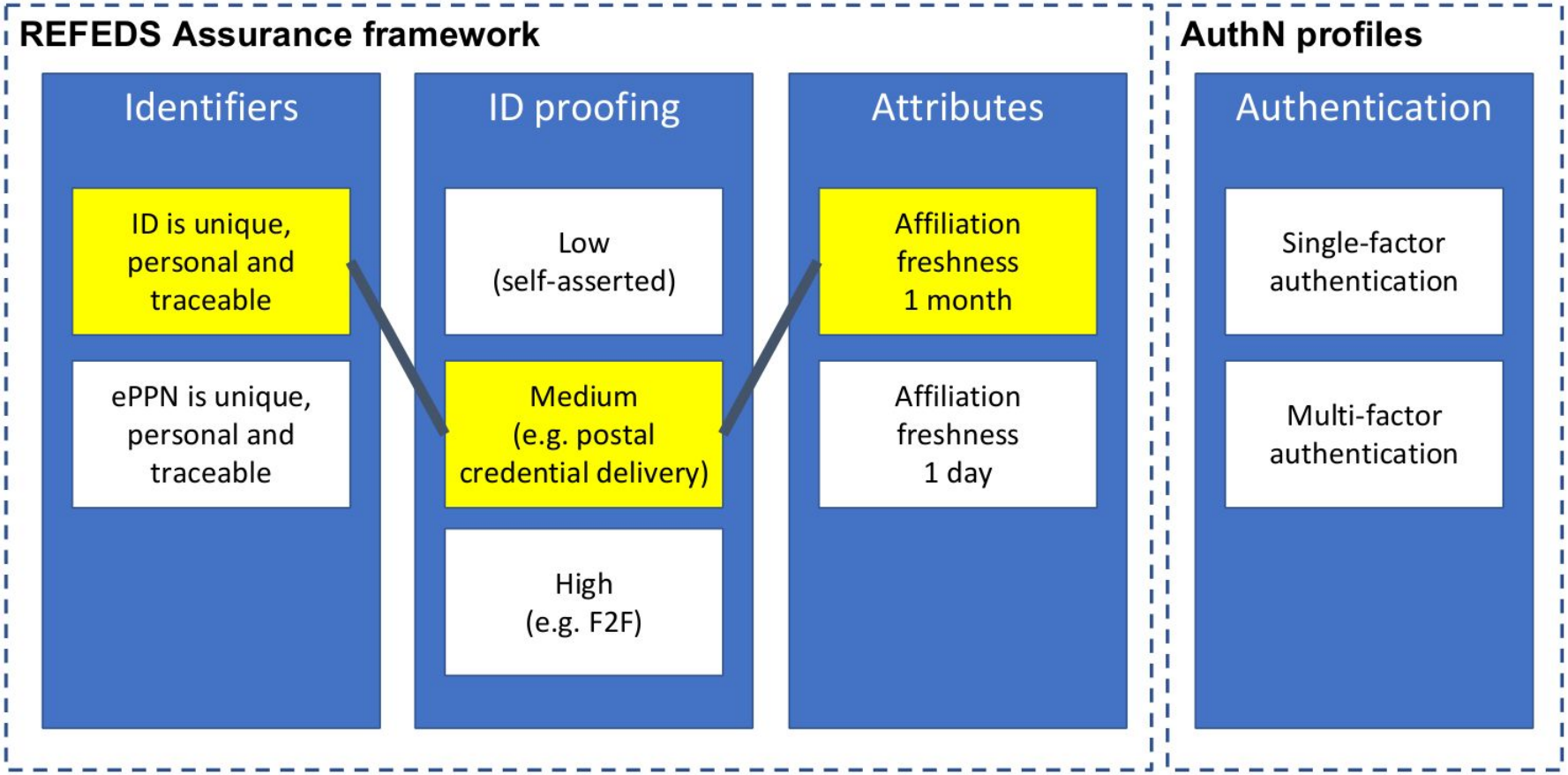
The big picture of assurance



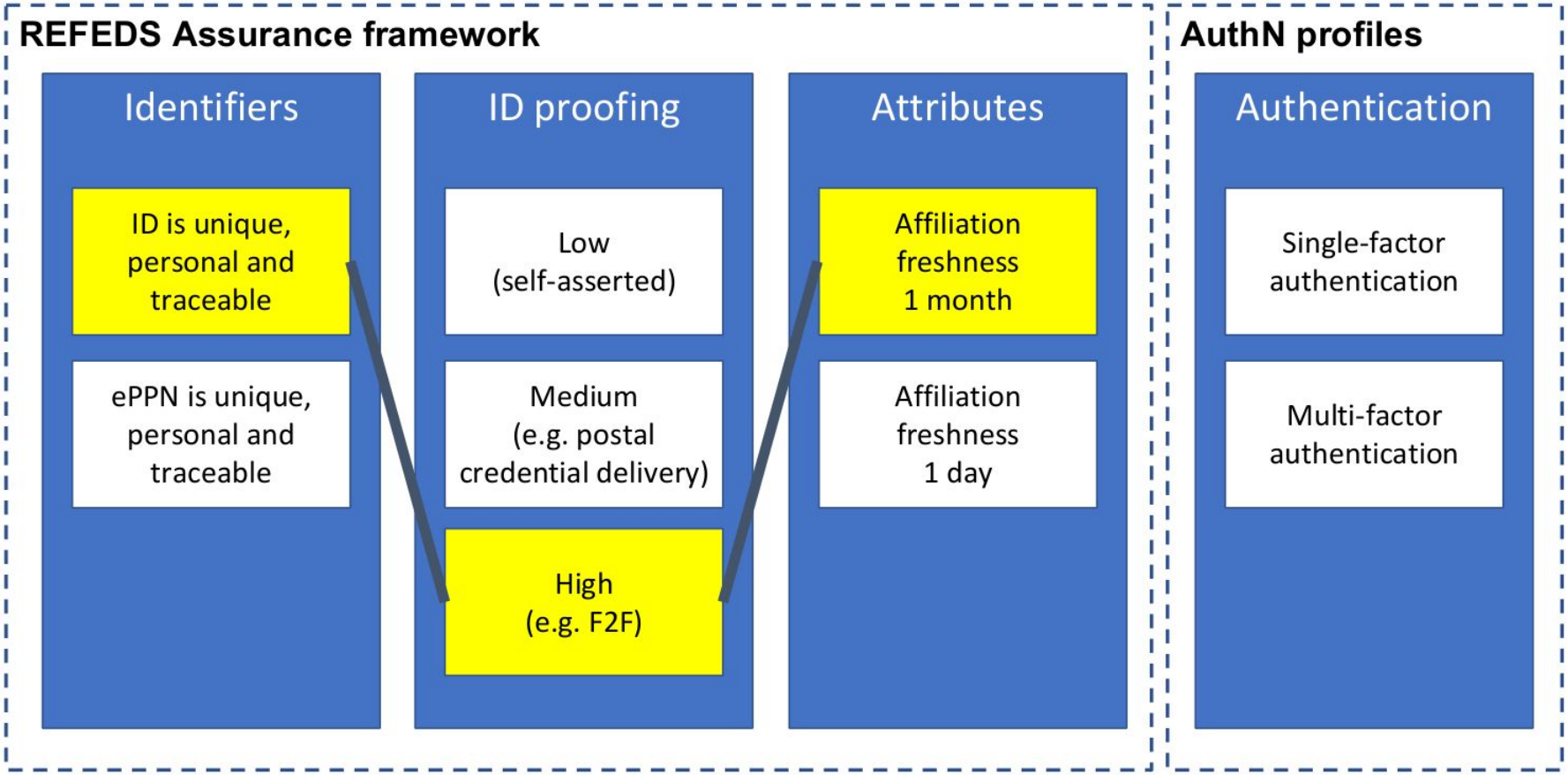
Split of responsibility clarified



"Cappuccino" for low-risk research use cases



“Espresso” for more demanding use cases



RAF Identity uniqueness

REFEDS Assurance Framework (round 2):
https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+Assurance+Framework+round+2.

Value	**Description**
`https://refeds.org/assurance/ID/unique`	- User account belongs to a single natural person - CSP can contact the person to whom the account is issued - The user identifier will not be re-assigned - The user identifier is eduPersonUniqueID, OpenID Connect sub (type: public) or one of the pairwise identifiers recommended by REFEDS

RAF ID Proofing

REFEDS Assurance Framework (round 2):
https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+Assurance+Framework+round+2.

Value	Description
`https://refeds.org/assurance/IAP/low`	Identity proofing and credential issuance, renewal, and replacement qualify to any of - 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]
`https://refeds.org/assurance/IAP/medium`	Identity proofing and credential issuance, renewal, and replacement qualify to any of - sections 5.2.2-5.2.2.9, section 5.2.2.12 and section 5.2.3 of Kantara assurance level 2 [Kantara SAC] - IGTF level BIRCH [IGTF] - IGTF level CEDAR [IGTF] - section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level low [eIDAS LoA]
`https://refeds.org/assurance/IAP/high`	Identity proofing and credential issuance, renewal, and replacement qualifies to any of - section 5.3.2-5.3.2.9, section 5.3.2.12 and 5.3.3 of Kantara assurance level 3 [Kantara SAC] - section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level substantial [eIDAS LoA]

RAF Attribute quality and freshness

REFEDS Assurance Framework (round 2):
https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+Assurance+Framework+round+2.

Value	Description
`https://refeds.org/assurance/ATP/ePA-1m`	eduPersonAffiliation, eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes (if populated and released to the RP) reflect user's departure within 30 days time
`https://refeds.org/assurance/ATP/ePA-1d`	eduPersonAffiliation, and eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes (if populated and released to the RP) reflect user's departure within one days time

REFEDS SFA & MFA

REFEDS Single Factor Authentication (SFA) Profile

- **DRAFT**: v0.2 pubblicato il 2 Maggio 2018
- https://refeds.org/profile/sfa (404)
- Consultazione REFEDS in corso:
  - https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+SFA+Profile

REFEDS Multi-Factor Authentication (MFA) Profile

- **STANDARD**: v1.0 pubblicato il 7 Giugno 2017
- https://refeds.org/profile/mfa

Domande?

GRAZIE

IDEM DAY 2018
Roma 7-9 Giugno 2018
Davide Vaghetti - IDEM GARR AAI
davide.vaghetti@garr.it