REFEDS update on RAF, SFA and MFA

Internet2 Technology Exchange 2018, 15 October 2018

Pål Axelsson, Jule Ziegler

Why we need a common language over the world:

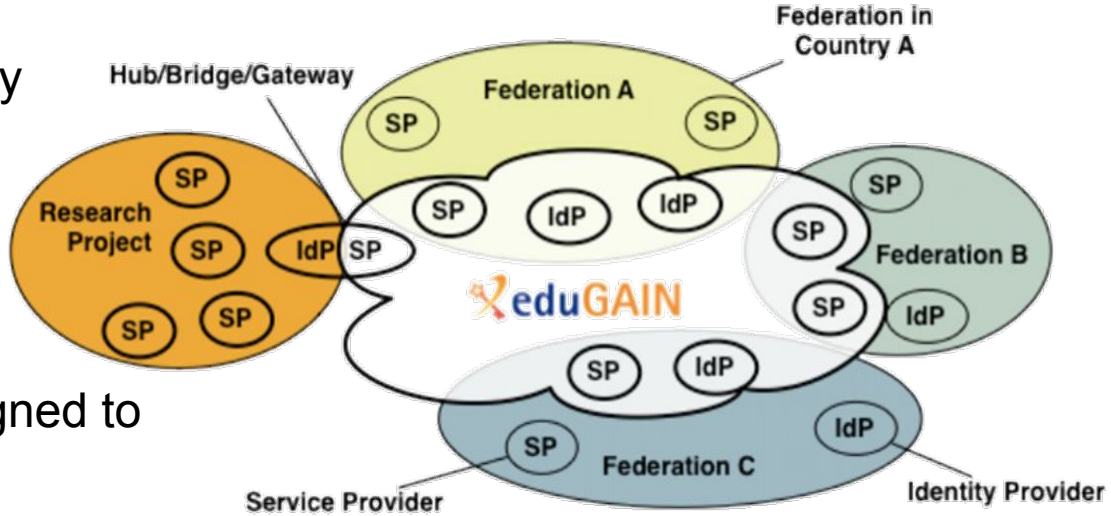
How was the registration/Identity Proofing done?

Is that a shared account (libraryuser1@university.org)?

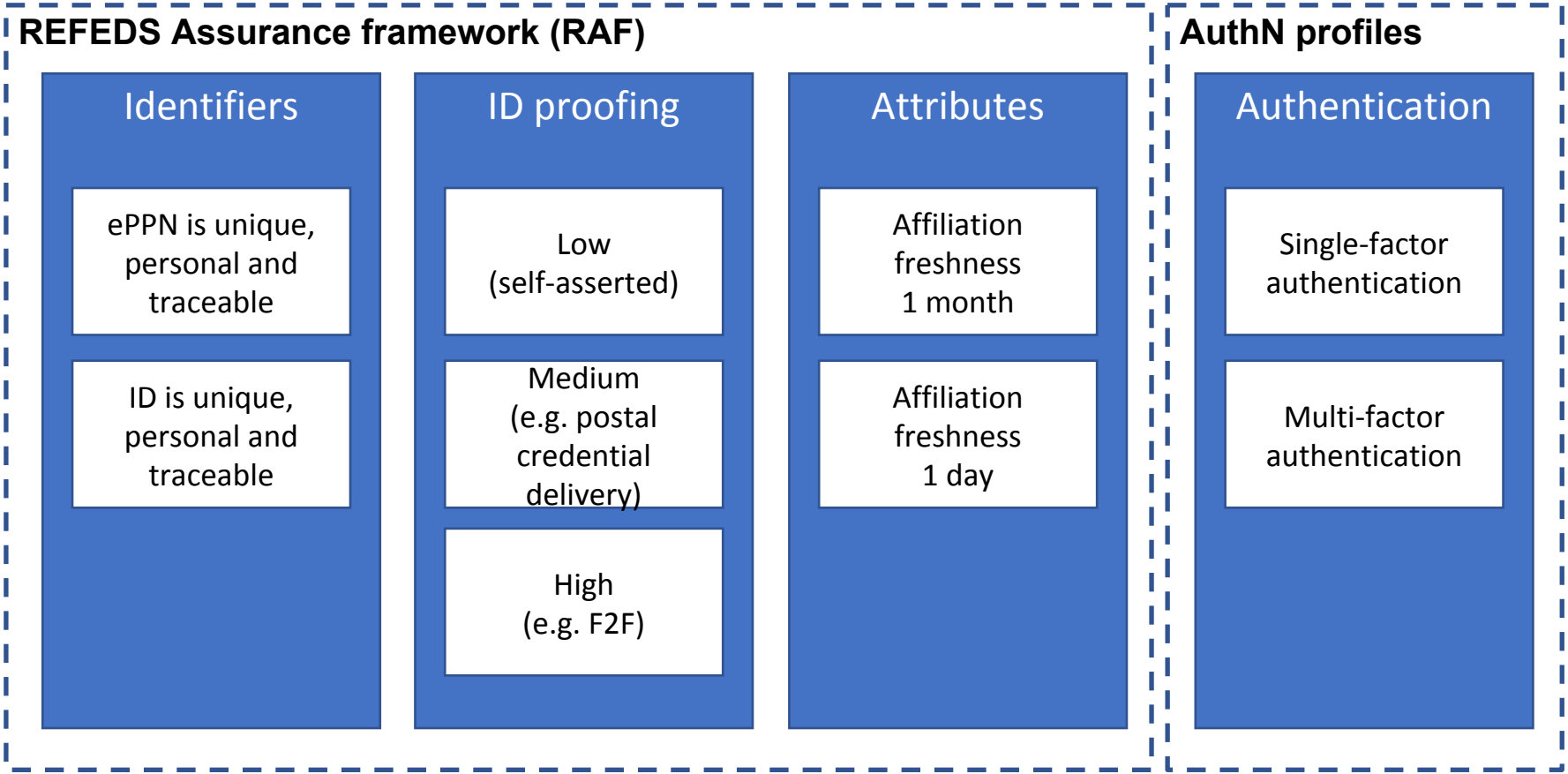
Can this user ID later be reassigned to some other person?

How fresh is that affiliation information?

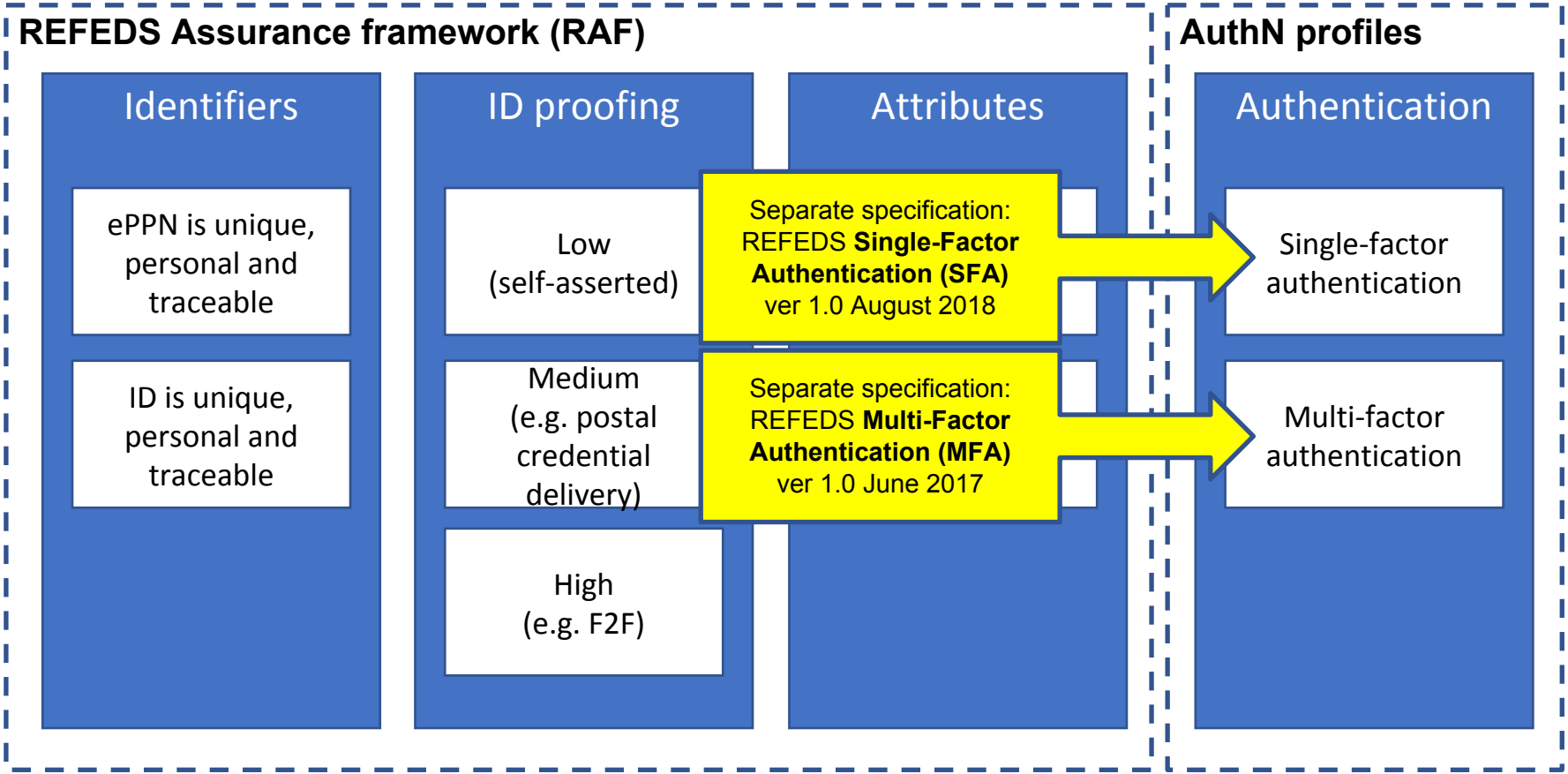
How was the user authentication done?



The big picture of assurance in REFEDS



Split of responsibility between REFEDS specs



RAF, MFA and SFA are self-assessed

- No independent evaluation of the Identity Provider REFEDS Assurance Framework (RAF), MFA, or SFA conformance
- No metadata assurance certification tag for RAF
- Identity Provider signals self-assessed conformance with the RAF conformance criteria and the three assurance components in the eduPersonAssurance attribute
- Identity Provider signals conformance with the SFA or MFA profiles by including corresponding values in the authenticationContext if requested by the Service Provider

RAF, MFA and SFA TechEx session

Identity and Authentication Assurance in the International Academic Arena

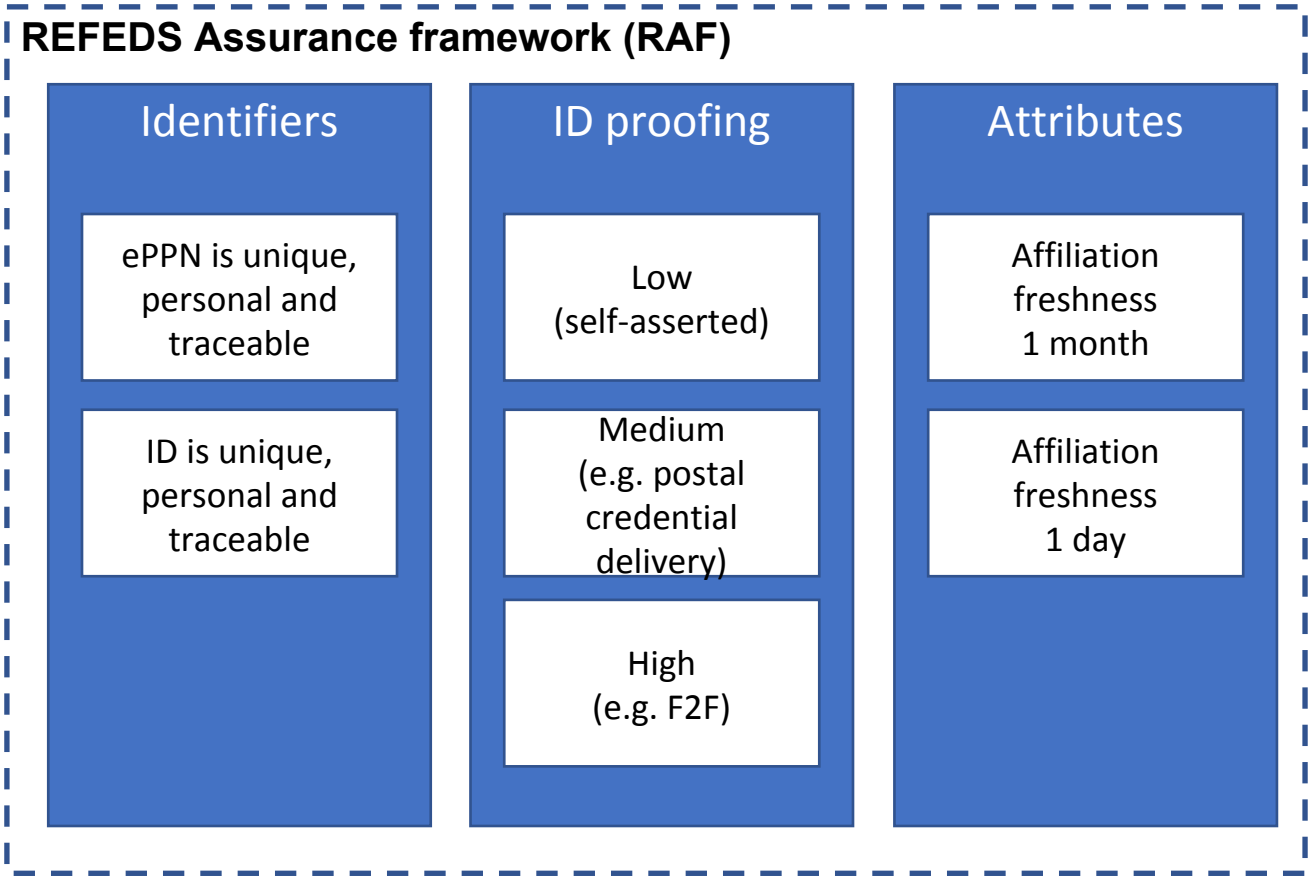
Tuesday 11:20AM

Pacifica Ballroom 4/5

We will dive deep into RAF, MFA and SFA with a start presentation and a more hands on part.

REFEDS Assurance Framework

REFEDS Assurance framework (RAF)



REFEDS Assurance Framework V1.0

https://refeds.org/assurance

When to send assurance info? **Always!**

- It is metadata about the binding of the authentication credential to the Subject
- It is **not** personally identifying information
- Send all values that apply for the user

- **The working group suggests that the attribute bundle in the entity category REFEDS Research and Scholarship should be updated with eduPersonAssurance**

RAF Conformance criteria

Value	Description
`$PREFIX$`	For a CSP to conform to this profile it is REQUIRED to conform to the following baseline expectations for Identity Providers: 1. The Identity Provider is operated with organizational-level authority 2. The Identity Provider is trusted enough that it is (or it could be) used to access the organization's own systems 3. Generally-accepted security practices are applied to the Identity Provider 4. Federation metadata is accurate, complete, and includes at least one of the following: support, technical, admin, or security contacts

$PREFIX$ in all values is replaced with https://refeds.org/assurance

RAF Unique identifier component

Value	Description
`$PREFIX$/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

Extra value to signal the eduPersonPrincipalName practice:

Value	Description
`$PREFIX$/ID/no-eppn-reassign`	eduPersonPrincipalName values will not be re-assigned.
`$PREFIX$/ID/eppn-reassign-1y`	eduPersonPrincipalName values may be re-assigned after a hiatus period of 1 year or longer.

RAF Identity proofing component

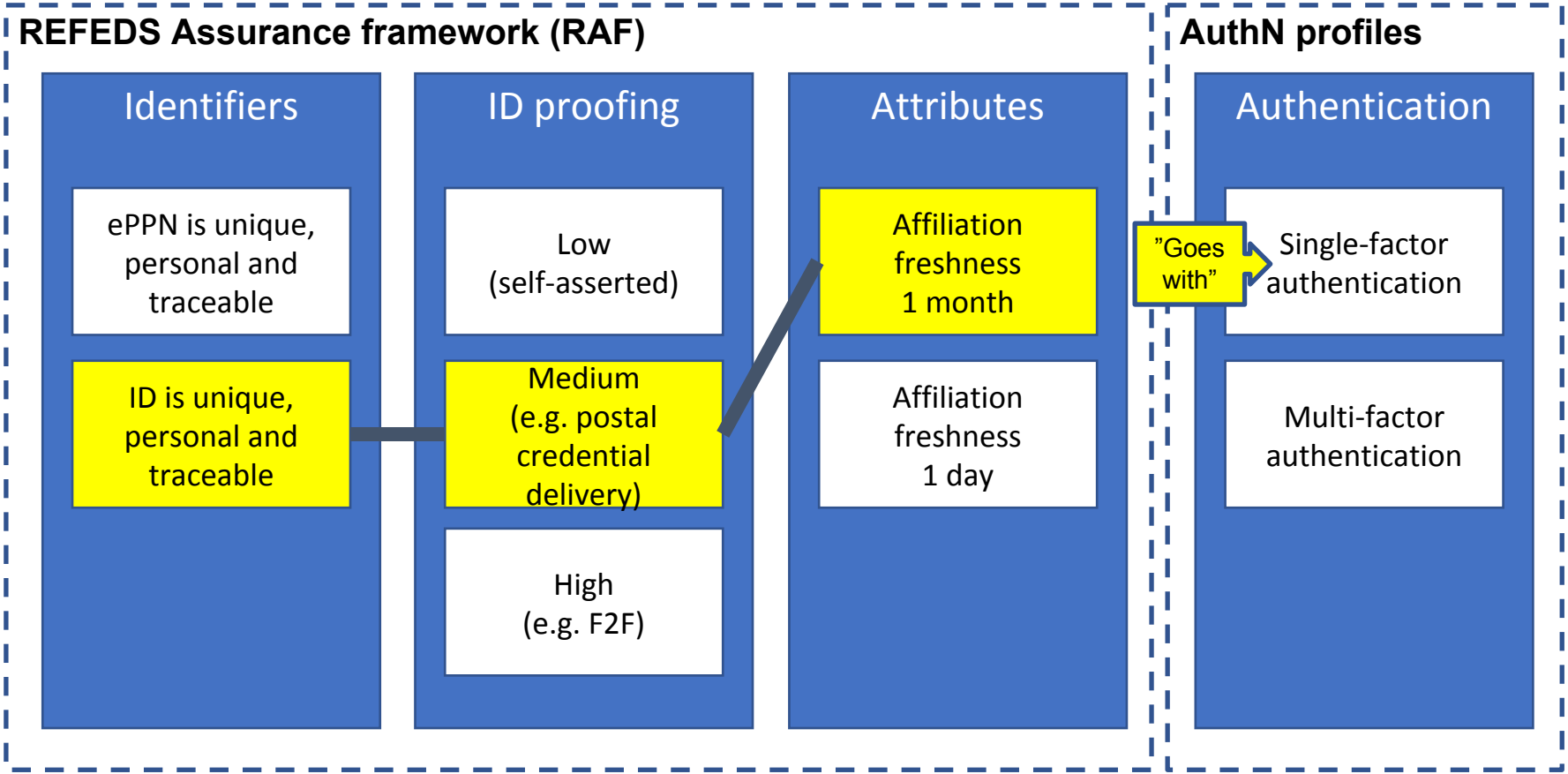
Value	Description
`$PREFIX$/IAP/low`	Identity proofing and credential issuance, renewal, and replacement qualify to any of - sections 5.1.2-5.1.2.9 and section 5.1.3 of Kantara assurance level 1 [Kantara SAC] - IGTF level DOGWOOD [IGTF] - IGTF level ASPEN [IGTF]
`$PREFIX$/IAP/medium`	Identity proofing 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]
`$PREFIX$/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]

Attribute Freshness component

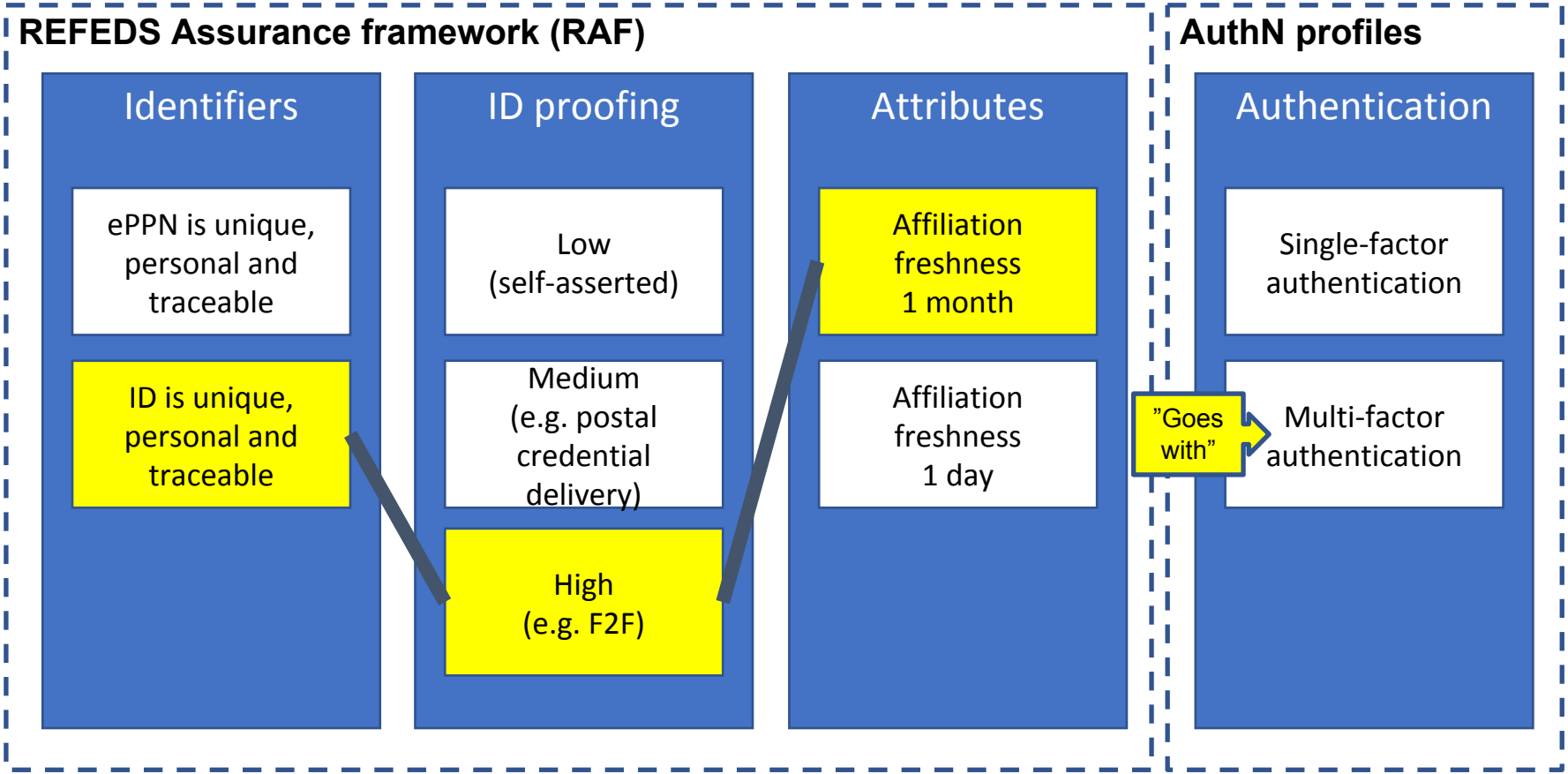
Value	Description
`$PREFIX$/ATP/ePA-1m`	eduPersonAffiliation, eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes (if populated and released to the RP) reflect user's departure within 30 days time
`$PREFIX$/ATP/ePA-1d`	eduPersonAffiliation, and eduPersonScopedAffiliation and eduPersonPrimaryAffiliation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

NB: The cycle times above start ticking when your institution's policy says that an affiliation has ended, ie, this is about the lag time until that change is reflected by the IdP, not what policy your institution must implement

“Cappuccino” for low-risk research use cases



“Espresso” for more demanding use cases



REFEDS Authentication Profiles

REFEDS Single Factor Authentication Profile

- SFA Profile: https://refeds.org/profile/sfa
- V1.0 Published 18 August 2018 (current)
- Defines a security baseline for AuthN using a single factor
- SAML and OIDC authentication context
- Terminology used in this document based on NIST 800-63B
- Two main criteria:
    1) Requirements for authentication factors
        - Properties of the factor itself:
            Minimum secret length, Basis for secret generation, Maximum secret life span
        - Threat protection:
            Prevent online guessing, Protect the secret cryptographically
    2) Requirements for replacement of a lost authentication factor
- Appendix A (Terminology), Appendix B (Memorized Secret Example)

REFEDS Single Factor Authentication Profile

4.1. Authenticator secret length

Authenticator type	Secret basis	Minimum length
Memorized Secret	≥52 characters *(e.g. 52 letters)*	12 characters
	≥72 characters *(e.g. 52 letters + 10 digits + 10 special characters)*	8 characters
Time based OTP-Device Out-of-Band Device	10-51 characters *(e.g. 10 digits)*	6 characters
	≥52 characters *(e.g. 52 letters)*	4 characters
Look-Up Secret Sequence based OTP-Device	10-51 characters *(e.g. 10 digits)*	10 characters
	≥52 characters *(e.g. 52 letters)*	6 characters
Cryptographic Software/Device	RSA/DSA	2048 bit
	ECDSA	256 bit

REFEDS Single Factor Authentication Profile

4.2. Maximum secret life span

Way of delivery	Maximum life time
Time based OTP Device	5 minutes
Telephone network (e.g. SMS, phone)	10 minutes
E-mail (e.g. recovery link)	24 hours
Postal mail	1 month

4.3. Protection against online guessing attacks (e.g. rate limiting)
4.4. Cryptographic protection of secrets at rest and in online transit

REFEDS Single Factor Authentication Profile

4.2 Replacement of a lost authentication factor

4.2.1. An existing secret must not be sent to the user (e.g. a stored password).

4.2.2. The replacement procedure does not solely rely on knowledge-based authentication (e.g. answer a secret question).

4.2.3. Human based procedures (e.g. service desk) ensure a comparable level of assurance of the requesting user identity as the initial identity vetting.

4.2.4. In order to restore a lost authentication factor, an OTP may be sent to the users address of record. All corresponding requirements apply as though this OTP would be a Look-Up Secret, except that it may be transmitted without being cryptographically protected.

4.2.5. For authenticators which are provided to the user as a backup, all requirements of the corresponding authentication factor apply.

REFEDS Single-Factor Authentication Profile

Appendix B - Memorized Secret Example

Character set size	Example character set	Example secret
≥ 52	(a-z)(A-Z)	doHskLAnPaEb
≥ 52	(A-Z)(26 special french characters)	ÆZHéIÔMNúYPU
≥ 72	(a-z)(A-Z)(0-9)(10 special characters)	L&Qn3?hM
≥ 72	(48 greek letters)(0-9)(14 special characters)	α1Σ%β34σ

Although all other authenticator types are generated (not user chosen), the secret and secret basis are handled analogously.

REFEDS Multi-Factor Authentication Profile

- Interoperability profile
- MFA Profile: https://refeds.org/profile/mfa
- V1.0 Published 07 June 2017 (current)
- MFA FAQ: https://wiki.refeds.org/display/PRO/MFA+Profile+FAQ
- SAML authentication context
- Three main criteria:
    1) Combination of at least two of the four distinct types of factors (something you *know* / *have* / *are* / *do*).
    2) Independence(*) of factors
    3) Mitigation of single-factor only risks related to non-real-time attacks (e.g., phishing, offline cracking, online guessing and theft of a (single) factor)
- Satisfies different use cases

(*) initial second factor registration may be bootstrapped via the first factor

Next step
Outreach

Questions later? Send them to:

assurance@refeds.org

or to the presenters

ziegler@lrz.de
pax@sunet.se