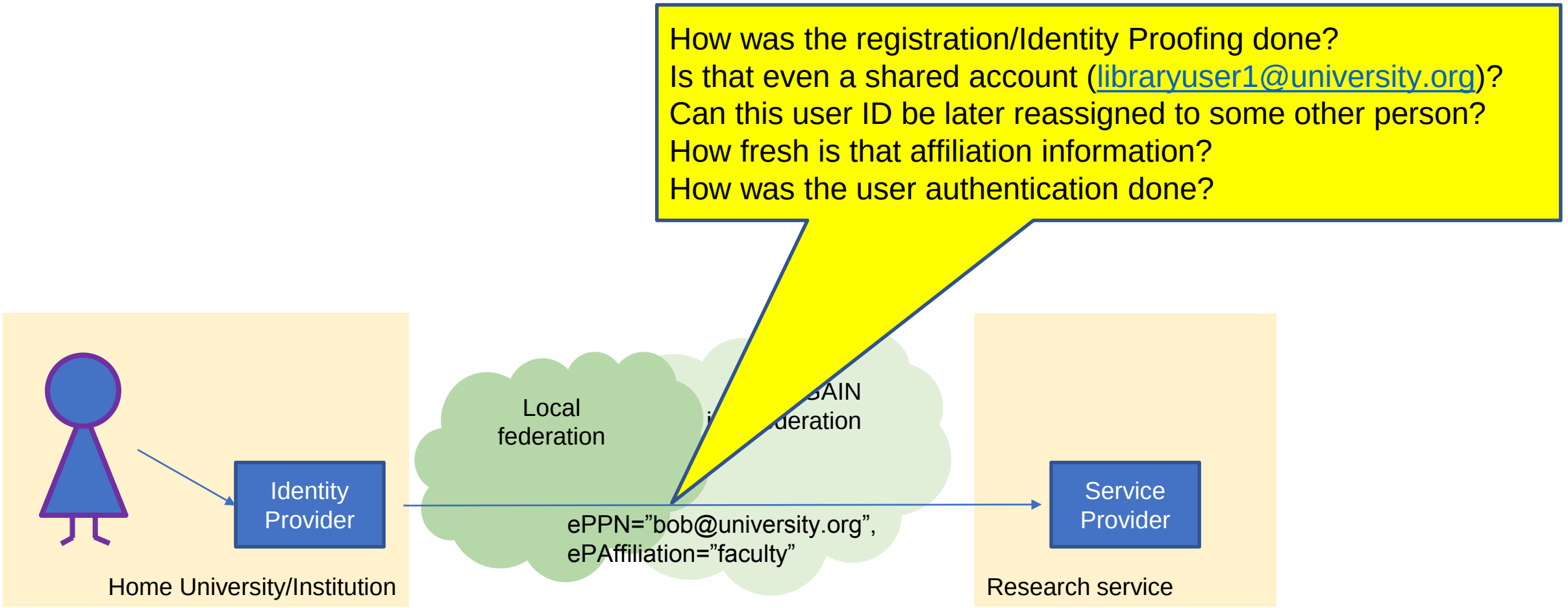
REFEDS Assurance Suite

FIM4R, 11 Feb 2019

Mikael Linden, REFEDS assurance wg chair
mikael.linden@csc.fi

Challenge


How was the registration/Identity Proofing done?
Is that even a shared account (libraryuser1@university.org)?
Can this user ID be later reassigned to some other person?
How fresh is that affiliation information?
How was the user authentication done?
Local federation
Identity Provider
Service Provider
ePPN=”bob@university.org”,
ePAffiliation=”faculty”
Home University/Institution
Research service

Short history of REFEDS Assurance Suite

- 11/2015 AARC publishes minimum requirements on assurance
- 6/2016 REFEDS establishes Assurance working group
- 4-6/2017 First public consultation on RAF
- 2-5/2018 Pilot on RAF, SFA and MFA
- 4-6/2018 Second public consultation on RAF and SFA
- 10/2018 RAF and SFA ver 1.0 published

REFEDS Assurance Suite

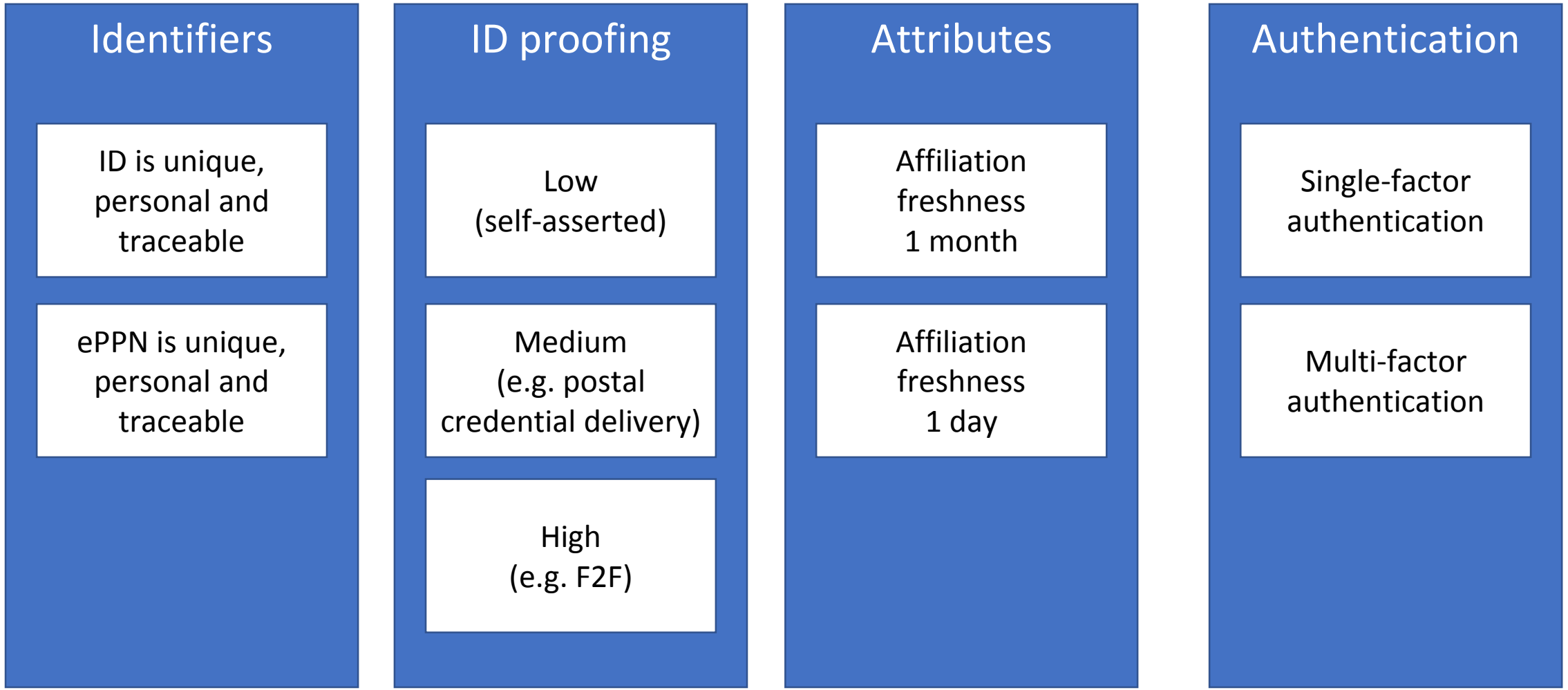
- REFEDS Assurance Framework (RAF) ver 1.0
  - Approved and published
  - https://refeds.org/assurance

- REFEDS Single-factor authentiation profile (SFA) ver 1.0
  - Approved and published
  - https://refeds.org/profile/sfa

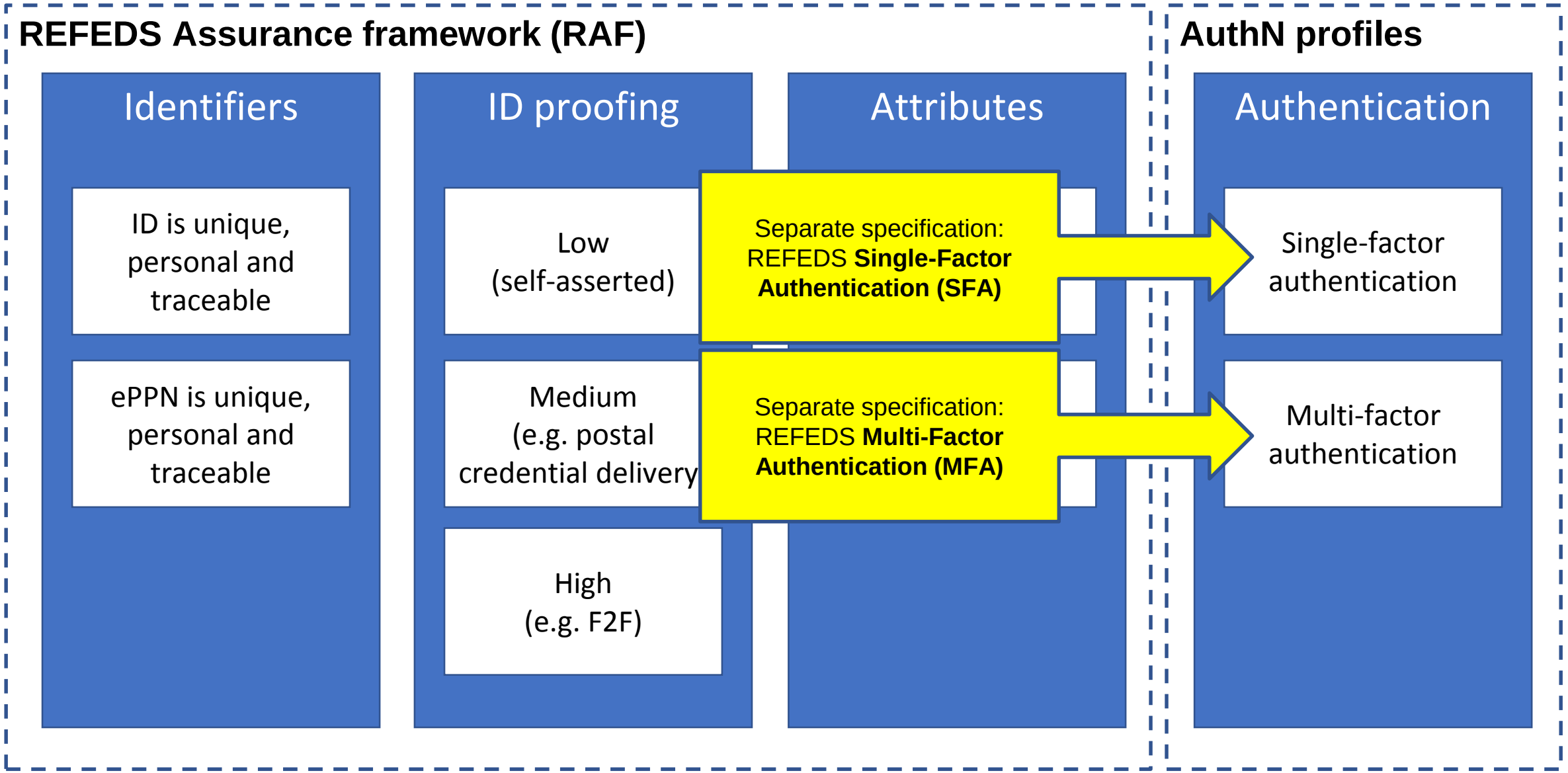
- REFEDS Multi-factor authentication profile (MFA) ver 1.0
  - approved in June 2017
  - https://refeds.org/profile/sfa

You can use them together or separately

The big picture of assurance in REFEDS



Split of responsibility between REFEDS specs

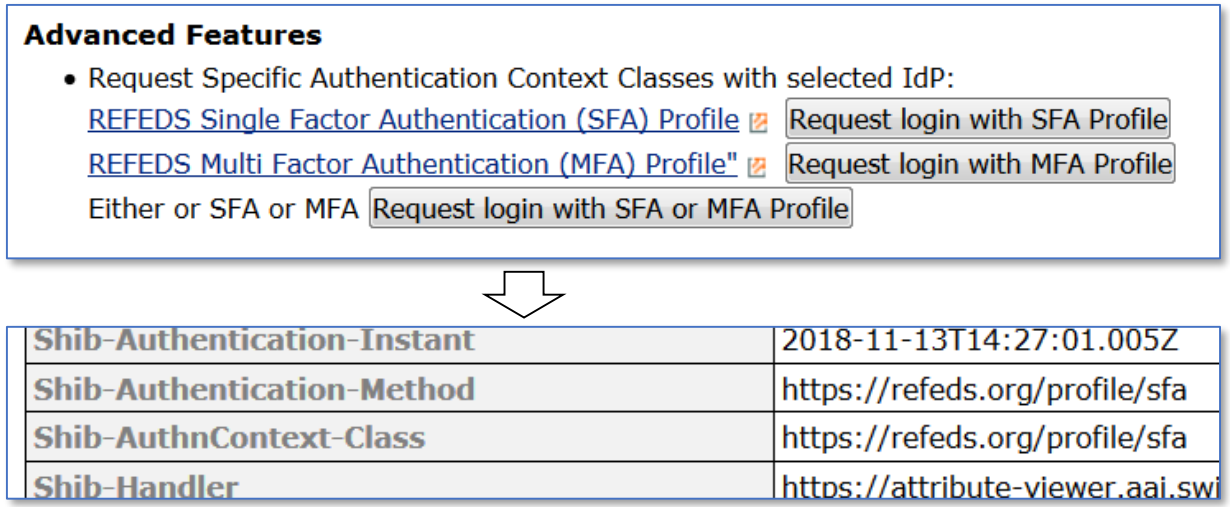


Test your IdP's conformance:
https://attribute-viewer.aai.switch.ch/aai/

SWITCH
AAI Attribute Viewer

assurance SAML2 Attribute Name: urn:oid:1.3.6.1.4.1.5923.1.1.1.11	• https://refeds.org/assurance/ID/no-eppn-reassign • https://refeds.org/assurance/profile/espresso • https://refeds.org/assurance/IAP/med • https://refeds.org/assurance/IAP/local-enterprise • https://refeds.org/assurance/ATP/ePA-1m • https://refeds.org/assurance/ATP/ePA-1d • https://refeds.org/assurance/ID/unique • https://refeds.org/assurance/IAP/high • https://refeds.org/assurance/profile/cappuccino • https://refeds.org/assurance/IAP/low
cn	Mikael Linden

RAF values released by your IdP



Advanced Features

- Request Specific Authentication Context Classes with selected IdP:

REFEDS Single Factor Authentication (SFA) Profile — Request login with SFA Profile

REFEDS Multi Factor Authentication (MFA) Profile" — Request login with MFA Profile

Either or SFA or MFA — Request login with SFA or MFA Profile

Shib-Authentication-Instant	2018-11-13T14:27:01.005Z
Shib-Authentication-Method	https://refeds.org/profile/sfa
Shib-AuthnContext-Class	https://refeds.org/profile/sfa
Shib-Handler	https://attribute-viewer.aai.swi

You can ask the test SP to request particular authentication context and display IdP's response

Outreach to federations

- Presentations REFEDS 38th in Trondheim
- Presentations REFEDS 39th meeting in Orlando
- TechEx 2018 session in Orlando
- Webinar December 2018
  - https://www.youtube.com/channel/UCussxbcR_OxG1e_kRp0pjpA

Start supporting it!

Start requiring it!

Otherwise the IdPs are not going to deploy it.

Questions?

The work has been funded by
AARC, AARC2 and GN4 projects

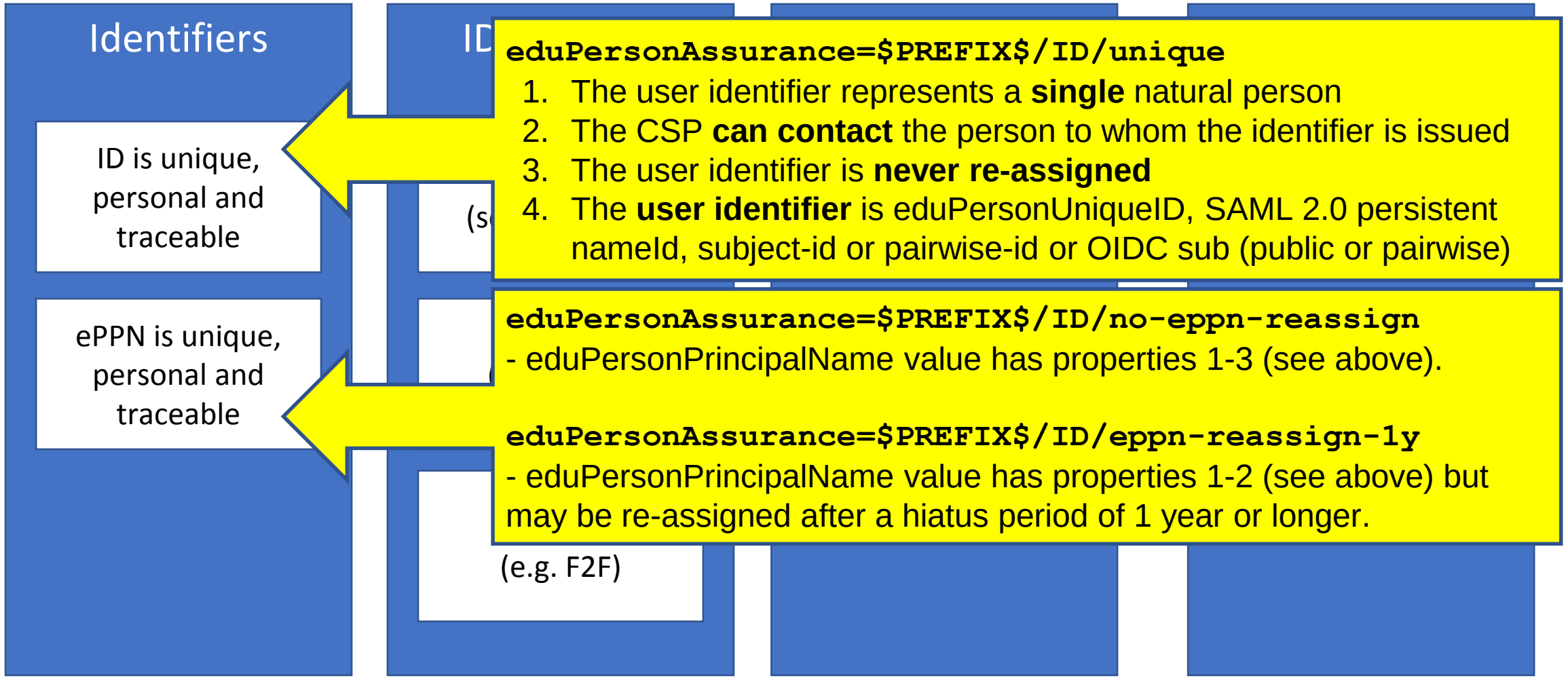
Backup slides

Assurance Framework assertions and profiles

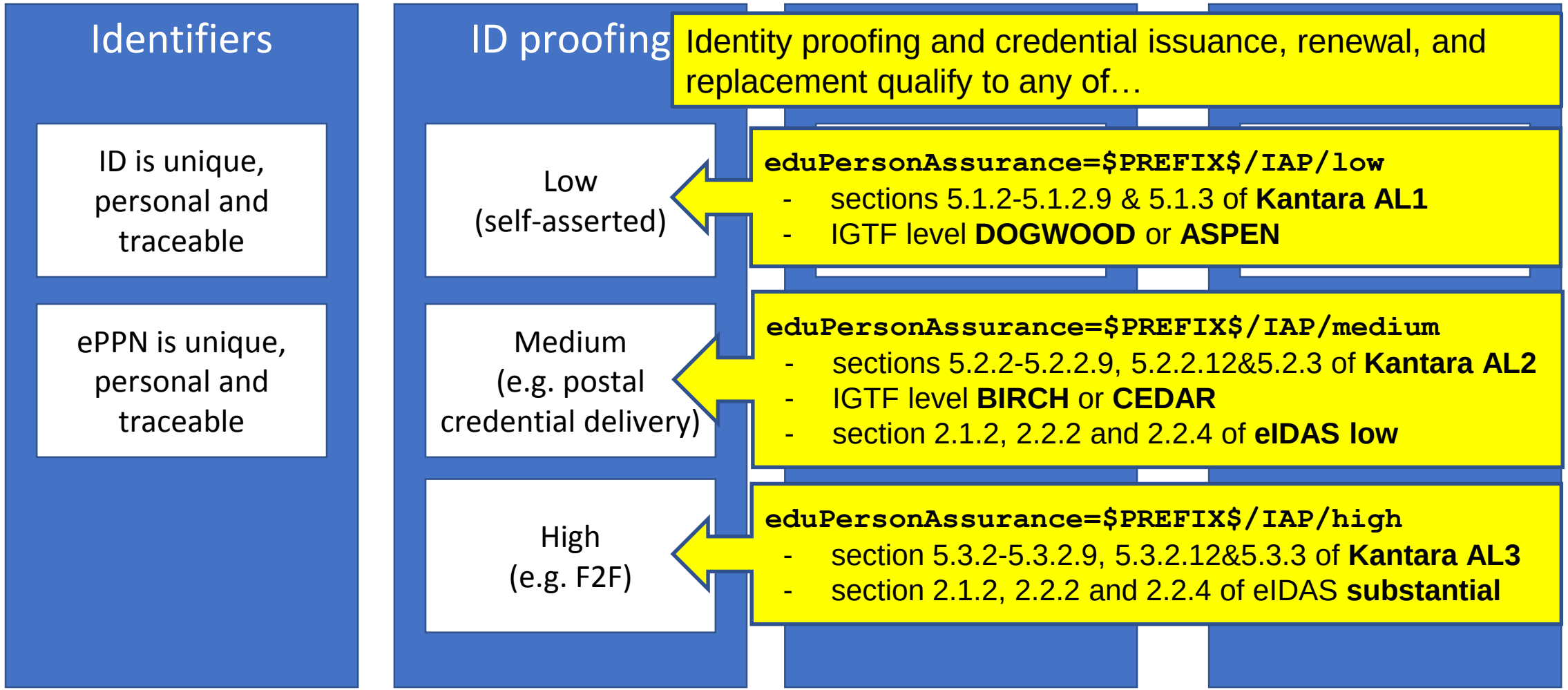
To be expressed by the CSP in the eduPersonAssurance attribute

`$PREFIX$=https://refeds.org/assurance`

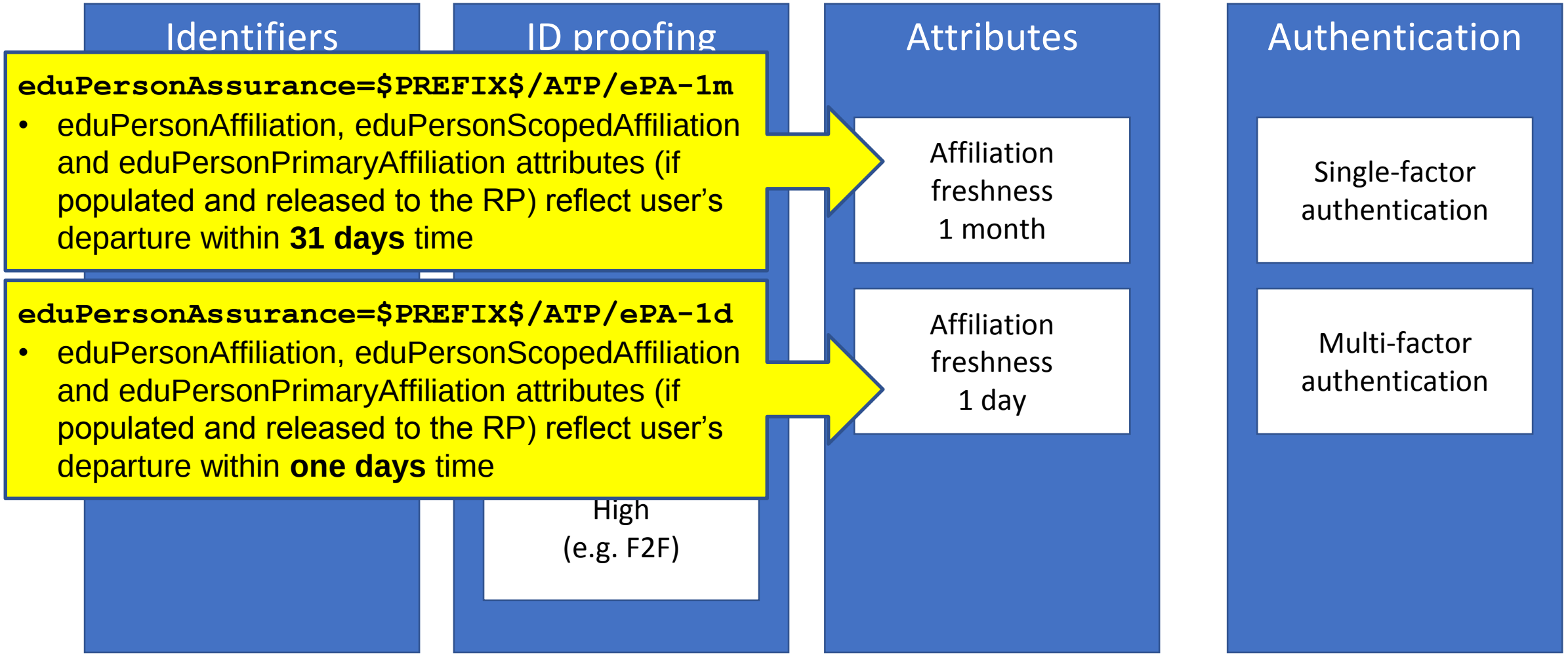
RAF values for properties of identifiers



RAF values for identity proofing



RAF values for attribute freshness



RAF conformance criteria

REFEDS Assurance framework (RAF)

Identifiers | ID proofing | Attributes

In all cases the CSP MUST (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

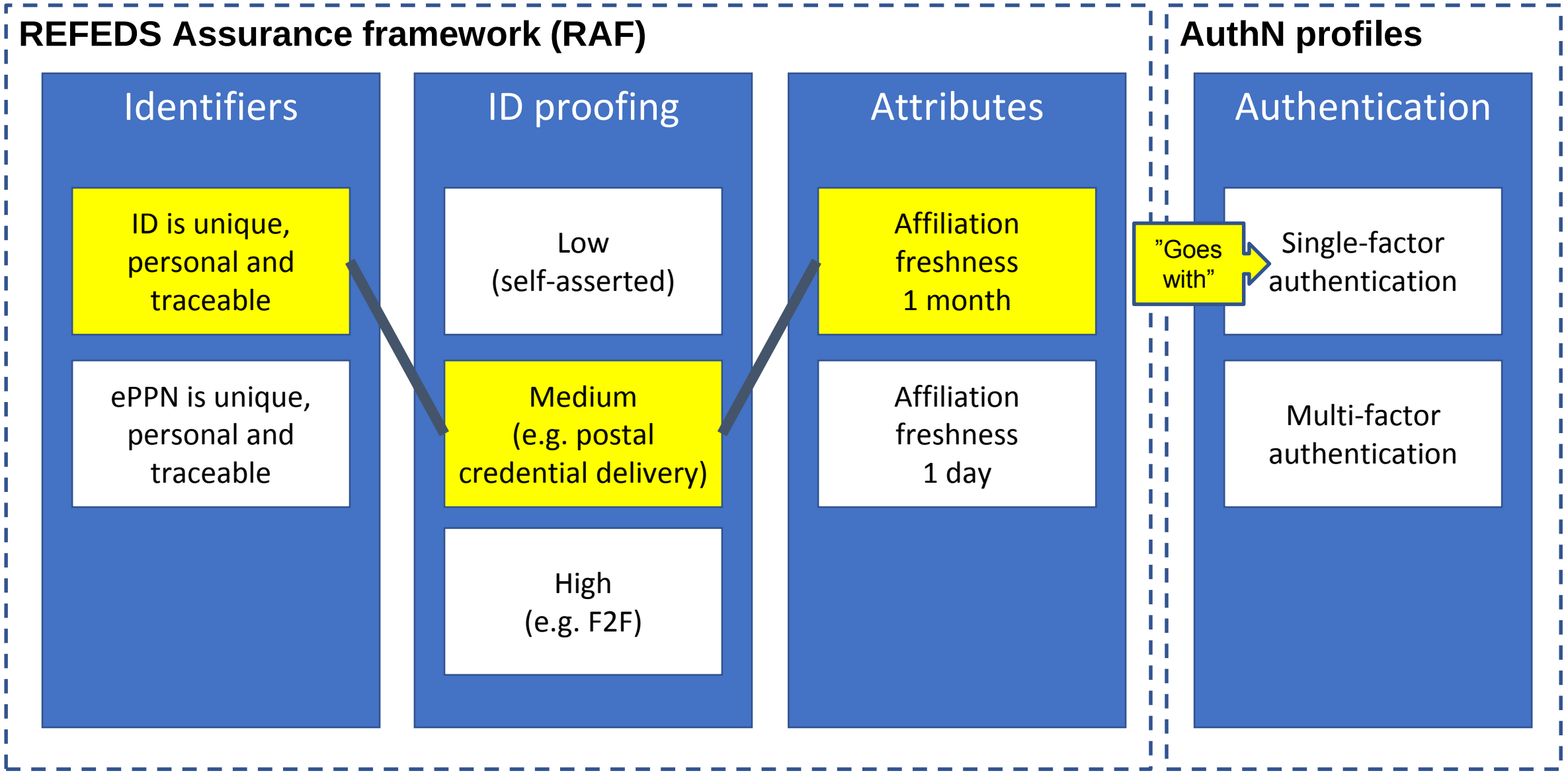
A CSP indicates its conformance to this profile by asserting `$PREFIX$`.

AuthN profiles

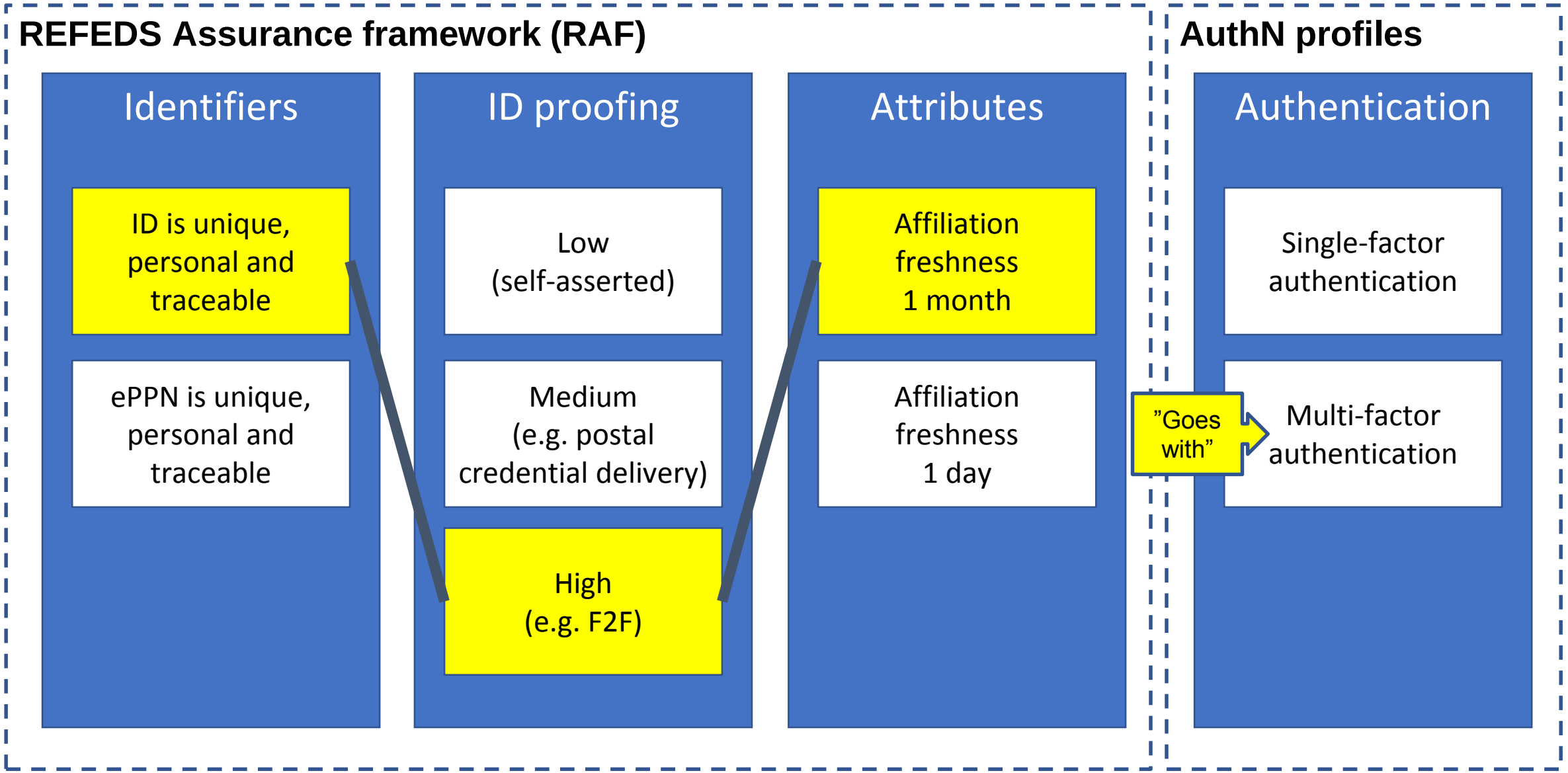
Authentication

- Single-factor authentication
- Multi-factor authentication

“Cappuccino” for low-risk research use cases



“Espresso” for more demanding use cases

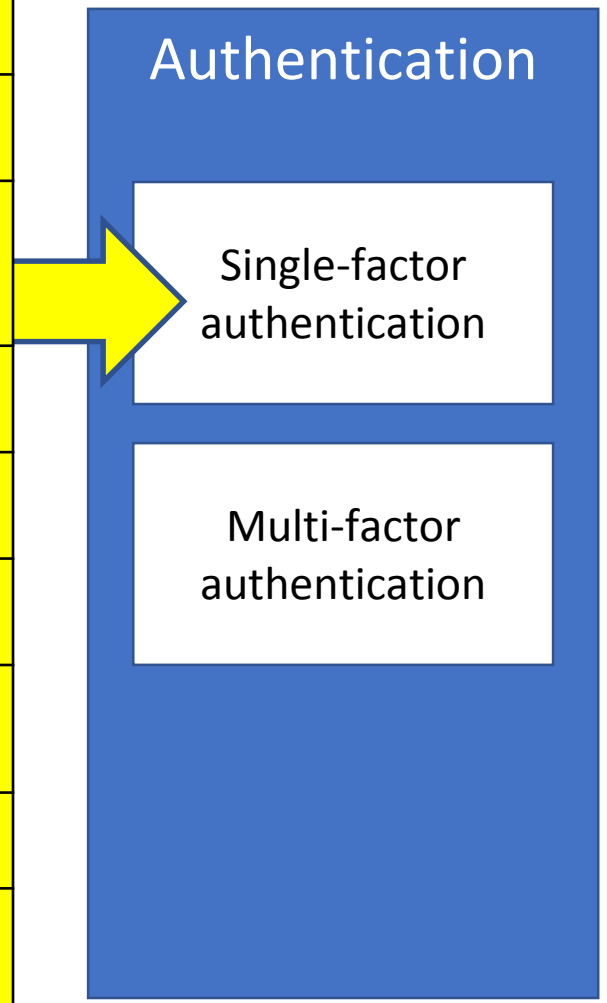


Single-factor authentication profile

https://refeds.org/profile/sfa

SFA profile requirements

Authenticator type	**Secret basis**	**Min 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



Further SFA requirements

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

- Protection against online guessing (e.g. rate limiting).
- Secrets cryptographically protected online and in transit

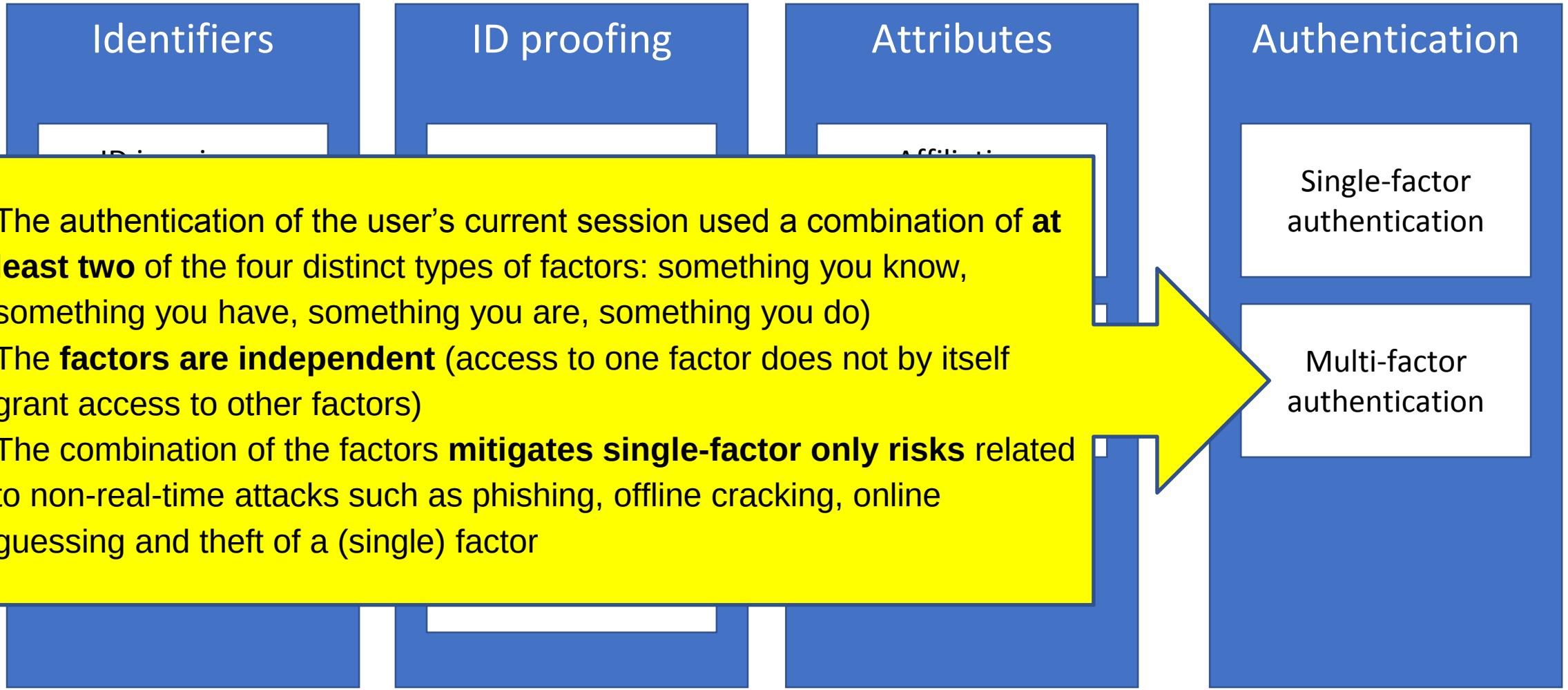
SFA requirements:
Replacement for a lost authentication factor

- An **existing secret** must not be sent to the user (e.g. a stored password).
- The replacement procedure does not **solely rely on knowledge-based authentication** (e.g. answer a secret question).
- Human based procedures (e.g. service desk) ensure a **comparable level** of assurance of the requesting user identity as the initial identity vetting.
- In order to restore a lost authentication factor, an OTP may be sent to the users **address of record**.
- For authenticators which are provided to the user as a **backup**, all requirements of the corresponding authentication factor apply.

Multi-factor authentication profile

https://refeds.org/profile/mfa

MFA profile requirements



- The authentication of the user's current session used a combination of **at least two** of the four distinct types of factors: something you know, something you have, something you are, something you do)
- The **factors are independent** (access to one factor does not by itself grant access to other factors)
- The combination of the factors **mitigates single-factor only risks** related to non-real-time attacks such as phishing, offline cracking, online guessing and theft of a (single) factor