Identity & Authentication Assurance in the International Academic Arena

Internet2 Technology Exchange 2018, 16 October 2018
Pål Axelsson, Thomas Barton, Jule Ziegler

Session Agenda

- Introduction to REFEDS Assurance Framework & AuthN Profiles
- REFEDS Assurance Framework Pilot
- **Live!** Assurance Clinic

Why we need a common language over the world:

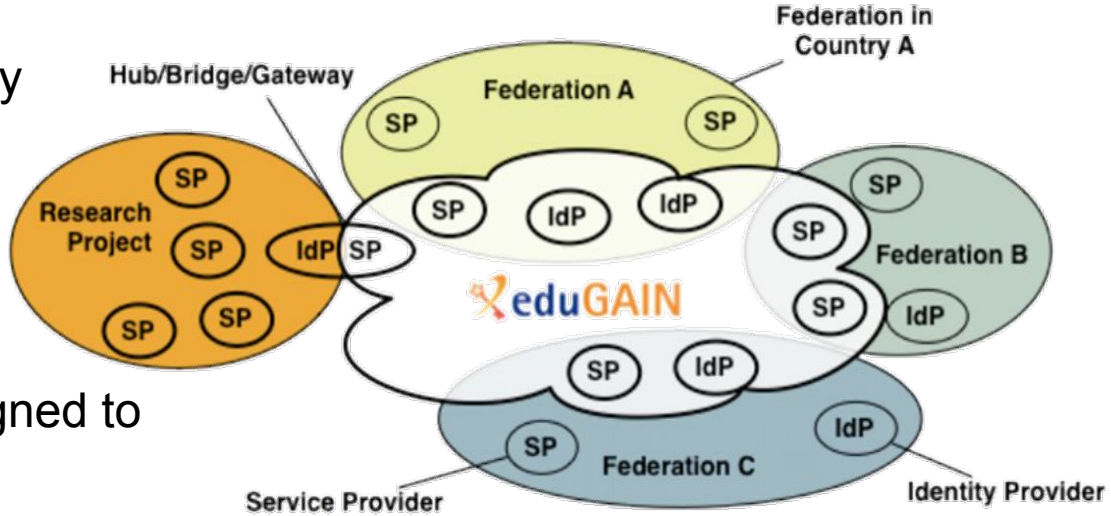
How was the registration/Identity Proofing done?

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

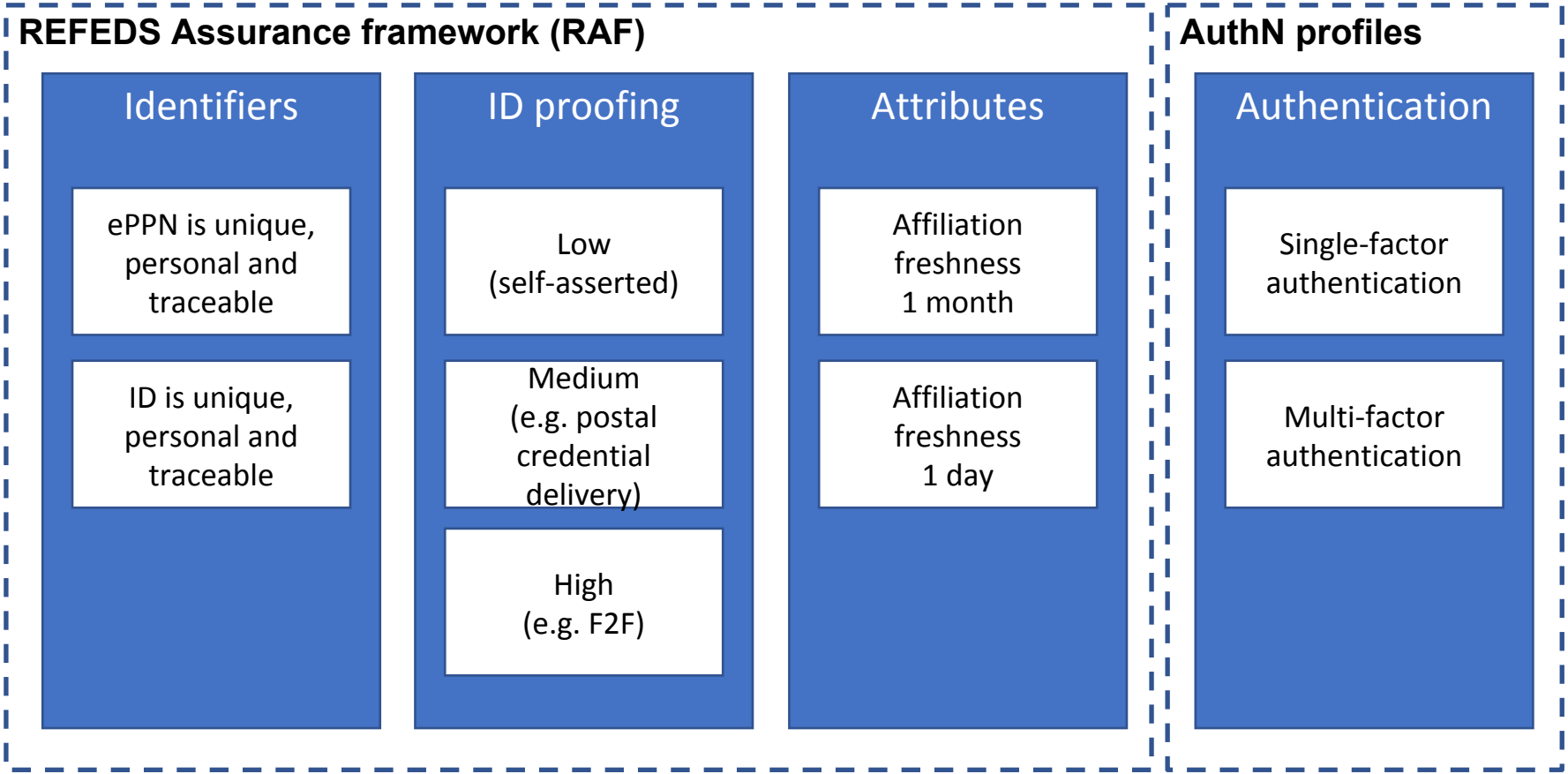
Can this user ID be later reassigned to some other person?

How fresh is that affiliation information?

How was the user authentication done?



The big picture of assurance in REFEDS



RAF, MFA, SFA are self-assessed

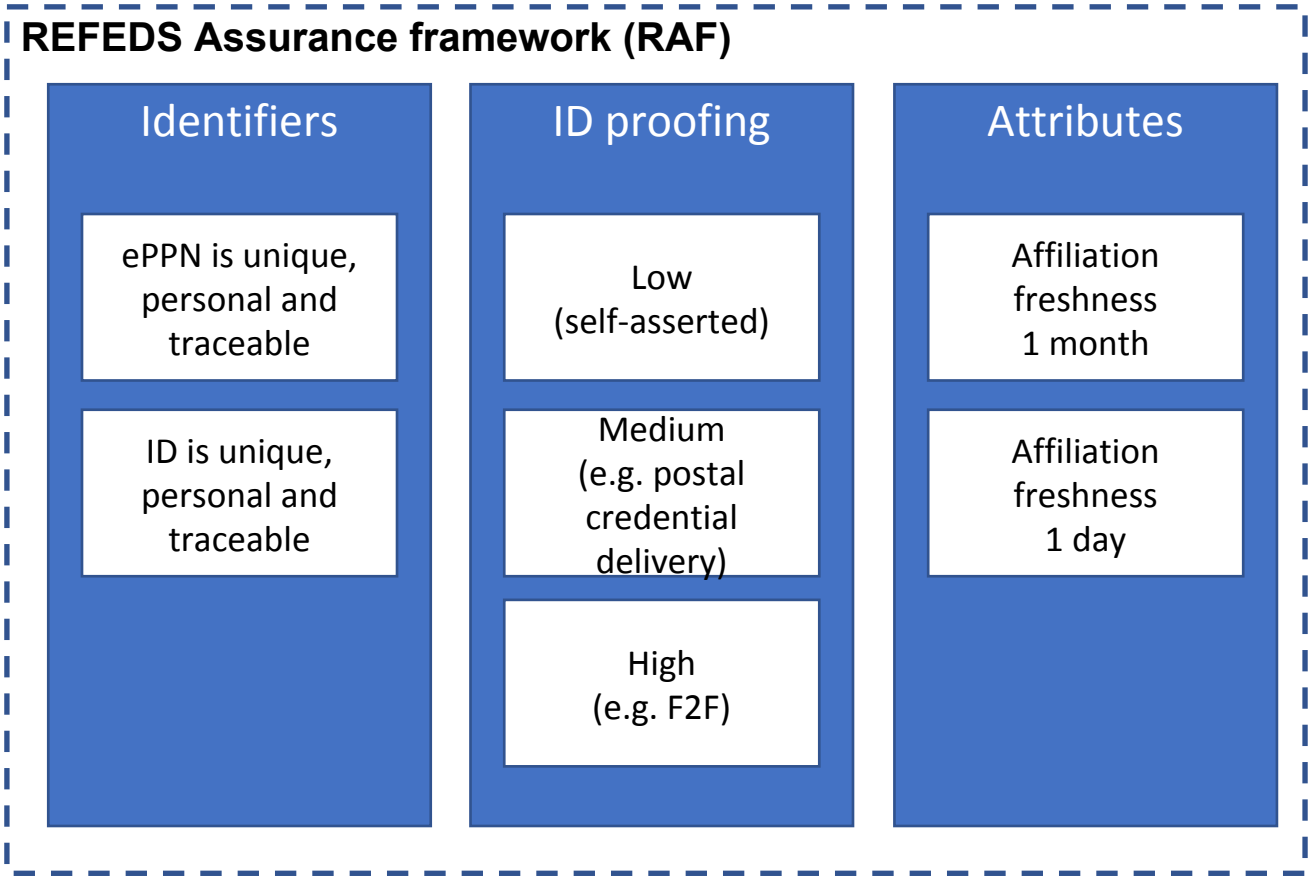
- No independent evaluation of the Identity Provider REFEDS Assurance Framework (RAF), MFA, or SFA conformance
- No metadata assurance certification tag for RAF
- Identity Provider signals self-assessed conformance with the RAF conformance criteria and the three assurance components in the eduPersonAssurance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

REFEDS Assurance Framework

REFEDS Assurance framework (RAF)

- REFEDS Assurance framework: https://refeds.org/assurance
- V1.0 Published (current)
- Defines a set of assurance tags for the eduPersonAssurance attribute in three different areas
  - Uniqueness of identifiers
  - Identity proofing
  - Affiliation attribute freshness
- Defines two combined assurance profiles
  - Cappuccino for medium risk services
  - Espresso for high risk services

REFEDS Assurance framework (RAF)



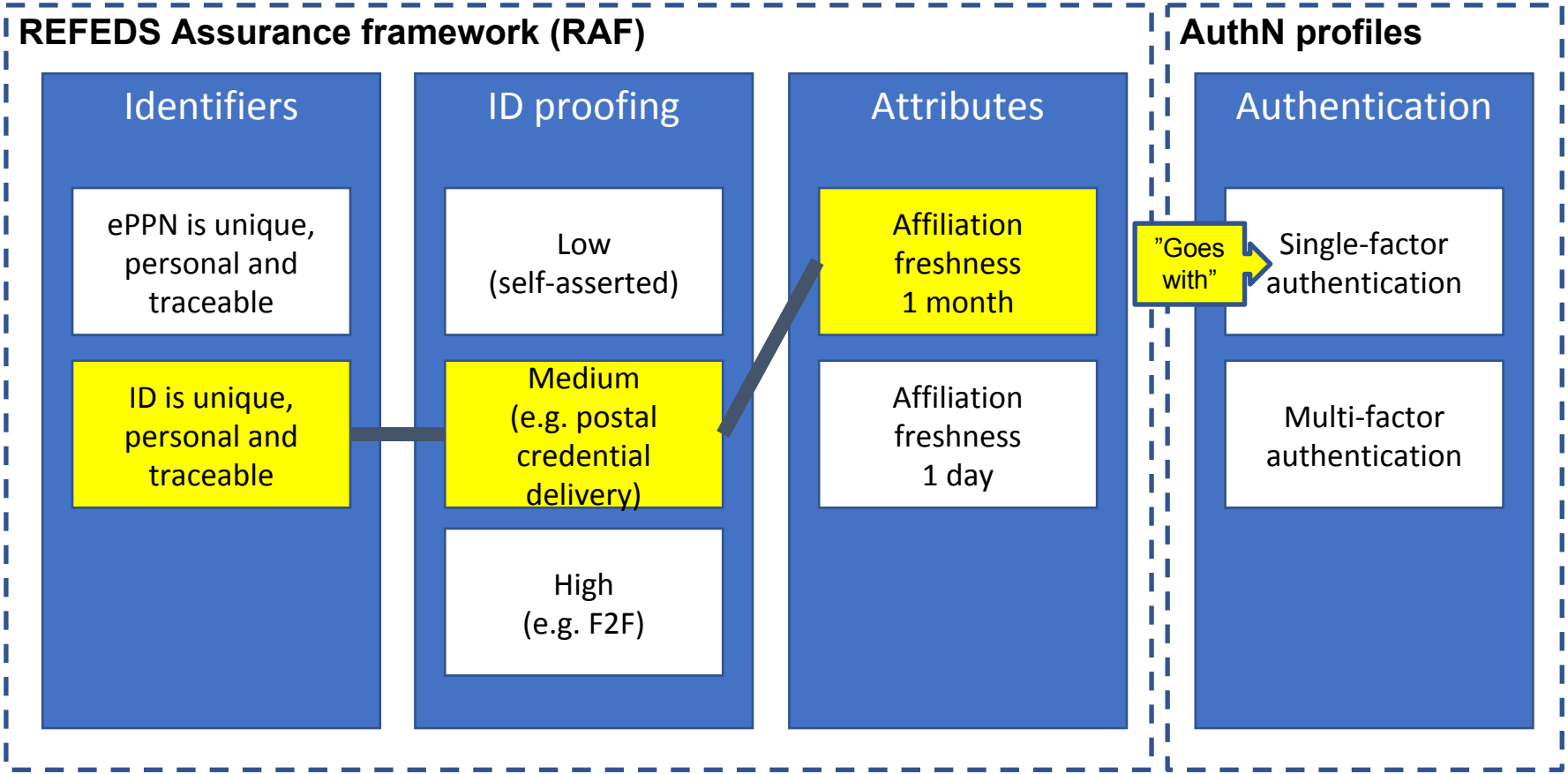
When to send assurance info? **Always!**

- It is metadata about the binding of the authentication credential to the Subject
- It is **not** personally identifying information

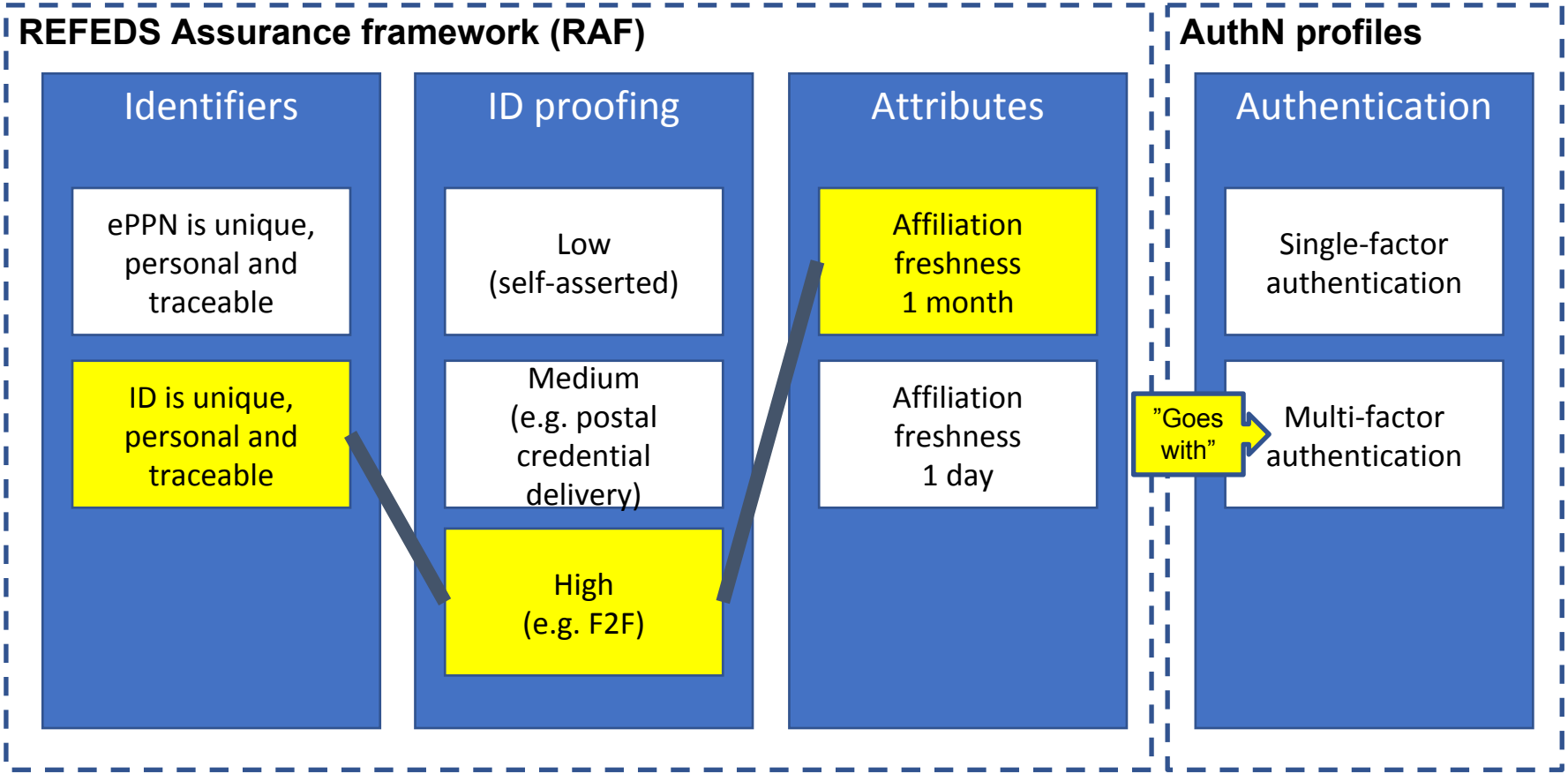
- So simplest is to always send if you've got it

- Send all values that apply for the user

“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 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

REFEDS Assurance Framework Pilot

Background

To get practical experience on REFEDS Assurance framework (RAF) and REFEDS Single-factor authentication (SFA) profile, including

- any remaining vagueness or obscurity in RAF and SFA specifications
- any issues with deploying the RAF and SFA specifications on existing SAML products

The pilot will deploy the RAF and SFA specifications to a handful of SAML IdPs and SPs exposed to eduGAIN from different federations. If an IdP can deliver REFEDS MFA, it should be deployed as well to support the assurance profile Espresso.

Participants

SAML Identity Providers

- The University of Chicago (Shibboleth IdP)
- XSEDE (Shibboleth IdP)
- Aalto university in Finland (Shibboleth IdP)
- CSC - IT Center for Science in FInland (Shibboleth IdP)

SAML Service Providers

- ELIXIR (SimpleSAMLphp)
- EGI Check-in (SimpleSAMLphp)
- CILogon (Shibboleth SP)
- SWITCHaai attribute test (Shibboleth SP)

Results

- The participating Shibboleth IdPs were successfully configured to handle the authentication context requests/responses and release eduPersonAssurance attribute to the SP.
- For the roll-out of the RAF, attention needs to be paid for making sure the IdPs actually release the eduPersonAssurance attribute to the SPs.
- The REFEDS community should consider adding the eduPersonAssurance to the R&S attribute bundle.

Results (continued)

- SimpleSAMLphp can handle custom authentication context classes
- The IdP/SP proxy Satosa can forward custom authentication context class requests and replies
- ADFS can not react on REFEDS SFA and REFEDS MFA
  - ADFS can not handle custom authentication context classes, only a predefined set
  - At Ignite in September SWAMID Operations talked to Microsoft ADFS developers about custom authentication context classes, they will add a change request.
    - If you've any contact deep into Microsoft please make them aware of the need.

Assurance Clinic

Clinic objectives

- Basic understanding of the elements that go into RAF, SFA, MFA
- Identify obstacles to adoption at your institutions
- Identity a couple of ACAMP session topics for deeper follow-up

- Now let’s head into the weed patch ...

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

This conformance criteria is covered by inCommon Baseline Expectations for Trust in Federation!

$PREFIX$ 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]

Identity Proofing highlights

Low	Medium	High
Unique user identifier	Identity proofing policy	Verification of identity evidence
Self-asserted identity evidence	Mild validation of identity evidence	
Confirm user's email/phone	Retain log of proofing facts	
Allow user to change PIN/password	Credential delivery confirms email/phone	
	Modest constraint on password renewal	

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

REFEDS Single Factor Authentication Profile

4.1.1 Authenticator secrets have at least the following minimum 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

4.1.2 Secrets that are transmitted must have a maximum life span according to the way of delivery.

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

4.1.3 Accounts are protected against online guessing attacks (e.g. rate limiting).
4.1.4 Authentication secrets at rest and in online transit must be cryptographically protected.

REFEDS Single Factor Authentication Profile

4.2 Replacement of a lost authentication factor ensures all of the following, as applicable:

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.

Questions later? Send them to:

assurance@refeds.org

or to the presenters

ziegler@lrz.de
pax@sunet.se
tbarton@uchicago.edu