REFEDS

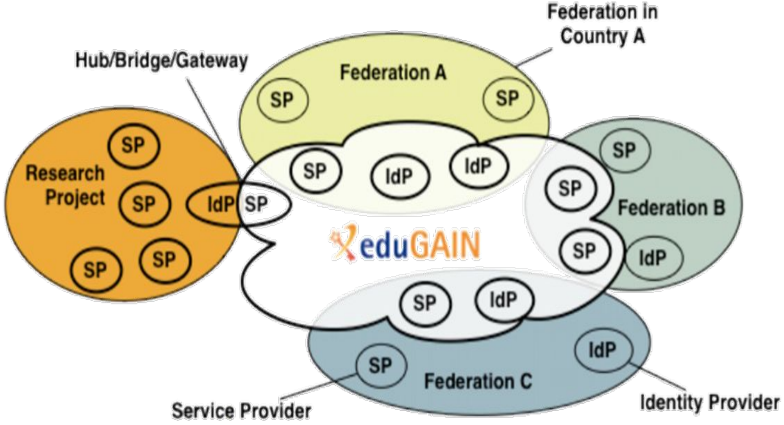
Assurance for Federated Identity Management

FIM4R Assurance Workshop, 17 June 2021

Jule Ziegler, Leibniz Supercomputing Centre, Germany

How sure can we be about a federated user's identity?

- How was the registration/Identity Proofing done? Is it a shared account (libraryuser1@university.org)?
- Can this user ID be later reassigned to some other person?
- Is their information, e.g. name or status, accurate or could it have changed?
- How was the user authentication done?



Credit to Mikael Linden

What is Assurance?

- The degree of confidence that a digital credential really belongs to the expected entity/user
- Multiple important aspects
  - Reliable identifiers (do they change, are they unique)
  - Identity Proofing (was an ID check done? how?)
  - Attributes (are they accurate? expected freshness?)
  - Authentication (was Two Factor Authentication (2FA) used?)
- Service Providers may choose to trust users based on the assurance information issued by their Identity Provider

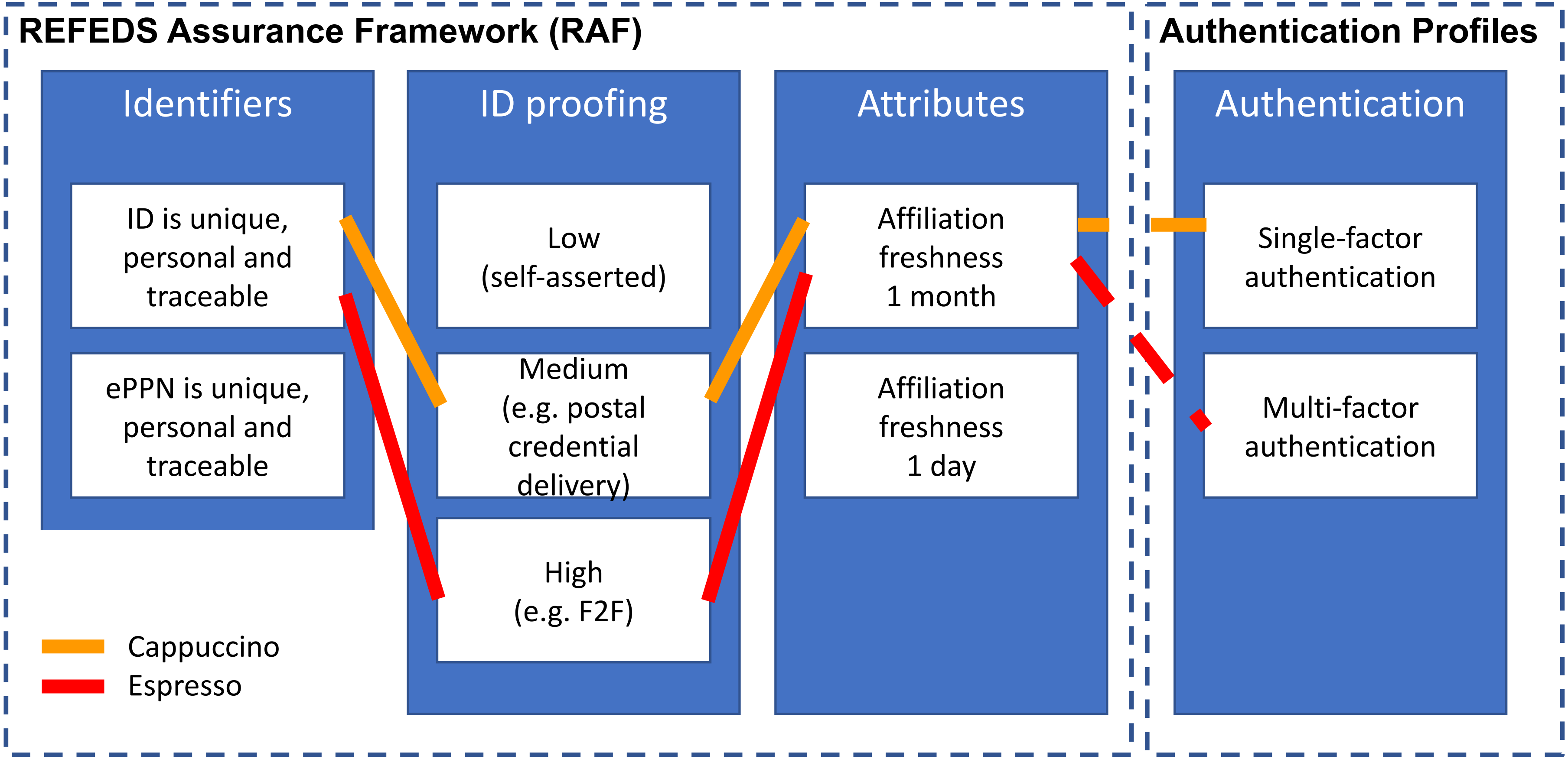
Current Work around Assurance

- Likely that some research communities may start **requiring** a certain level of assurance for their authenticating users
- Several assurance **profiles** (that define levels of trustworthiness) exist e.g. REFEDS, IGTF, InCommon, Kantara
  - So far very few Identity Providers support these profiles, they are missing driving use cases
- Research Communities may be able to influence the **uptake** of such profiles by combining our voices (concretely a short whitepaper authored by the FIM4R community)

REFEDS Assurance Suite in a nutshell

- Consisting of **three individual specifications**:
  - REFEDS Assurance Framework (RAF), ver 1.0, published 2018
  - REFEDS Single Factor Authentication Profile (SFA), ver 1.0, 2018
  - REFEDS Multi Factor Authentication Profile (MFA), ver 1.0, 2017
- Component-based approach
- Two identity assurance profiles: Espresso (high assurance) and Cappuccino (moderate assurance)

REFEDS Assurance Suite Big Picture



REFEDS Assurance Framework (RAF)

Identifiers

- ID is unique, personal and traceable
- ePPN is unique, personal and traceable

ID proofing

- Low (self-asserted)
- Medium (e.g. postal credential delivery)
- High (e.g. F2F)

Attributes

- Affiliation freshness 1 month
- Affiliation freshness 1 day

Authentication Profiles

Authentication

- Single-factor authentication
- Multi-factor authentication

🟧 Cappuccino

🟥 Espresso

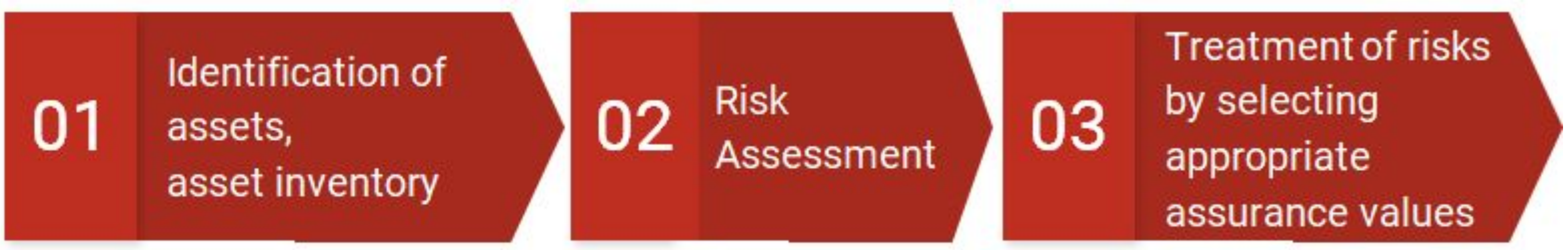
Assurance Challenge

- Identity Provider Challenge: How to implement assurance requirements?
- Service Provider Challenge: Which values should be requested? Risk exposure?

→ Both will be addressed in the Paper Preprint "Making Identity Assurance and Authentication Strength Work for Federated Infrastructures"

SP-side: Select REFEDS Assurance Values

- Determining the appropriate assurance level is all about risk management
- In an ideal world: three-fold approach



01 Identification of assets, asset inventory

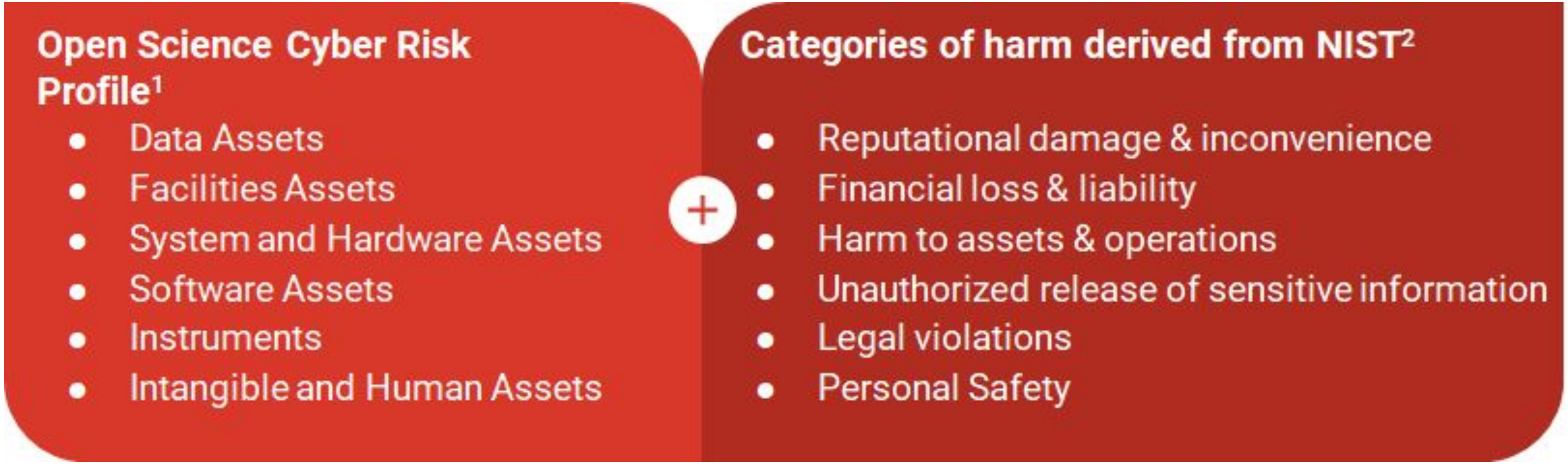
02 Risk Assessment

03 Treatment of risks by selecting appropriate assurance values

SP-side: Select REFEDS Assurance Values (cont.)

- In case formal asset & risk management processes are not in place:
  - Start self-assessing service(s) that rely on external assurance
  - If applicable, consider grouping of services
  - Focus on services in production
  - For R&E services, use medium as reference level for both identity and authentication assurance, increase or decrease if needed

SP-side: Select REFEDS Assurance Values (cont.)



Open Science Cyber Risk Profile[1]

- Data Assets
- Facilities Assets
- System and Hardware Assets
- Software Assets
- Instruments
- Intangible and Human Assets

+

Categories of harm derived from NIST[2]

- Reputational damage & inconvenience
- Financial loss & liability
- Harm to assets & operations
- Unauthorized release of sensitive information
- Legal violations
- Personal Safety

1: http://trustedci.github.io/OSCRP/OSCRP.html

2: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

General Recommendations for adopting REFEDS Assurance Suite

- Identity Provider side:
  - It may make sense to introduce assurance components gradually (e.g. role based, starting with affiliation=staff)
  - Don’t use/introduce authentication factors considered as insecure (e.g. SMS)
- Service Provider side:
  - Don’t ask for more assurance than you need, consider how much you really need to control your users
  - OSCRP assets & NIST categories of harm may serve as starting point

Conclusion

- Read our Paper Preprint for more detailed information
- Work in progress, we plan to share further use cases, experiences and guidance
- Concept of ‘families of related services’

Any Questions?