deutsches forschungsnetz

REFEDS Assurance Framework

ZKI Arbeitskreis IAM | 21. und 22. September 2022

Wolfgang Pempe (pempe@dfn.de)

Verlässlichkeitsklassen → REFEDS Assurance Framework

- Februar 2022
  - Workshops zur Umsetzung REFEDS Assurance Framework und MFA
- Mai 2022
  - Abschaffung der Trennung der Metadatensätze nach Verlässlichkeit; Unterscheidung Basic vs. Advanced nach wie vor über Entity Attribute möglich
- Ende Dezember 2022
  - Einstellung Support für die alten Verlässlichkeitsklassen in der Metadatenverwaltung

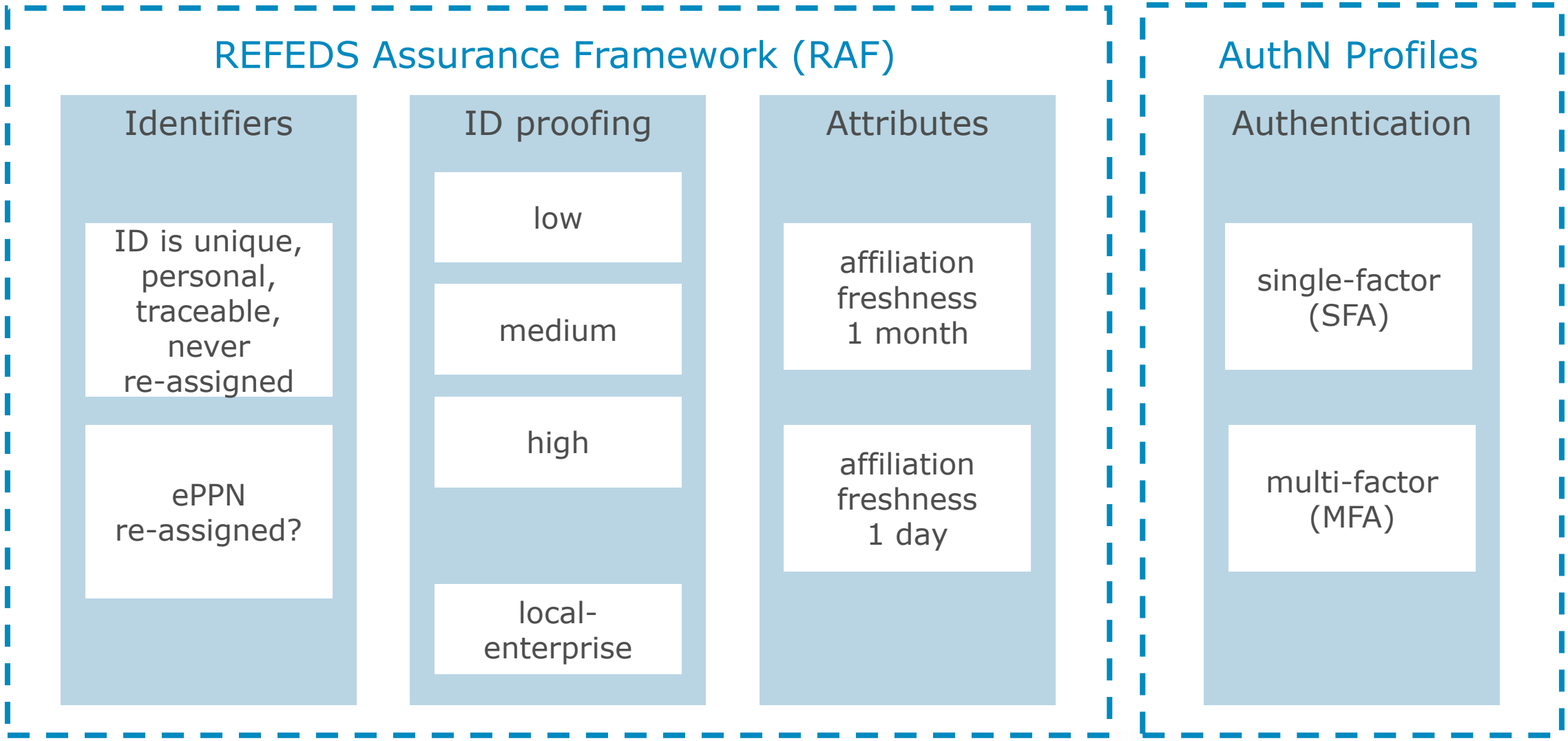
REFEDS Assurance Framework (1)

- Zentrale Eigenschaften des Frameworks
  - Verlässlichkeit *kann* pro Identität angegeben werden
  - Aspekte der Verlässlichkeit werden unabhängig voneinander adressiert
  - Internationaler Standard, kontrolliertes Vokabular
  - Identity Proofing: u.a. eIDAS Durchführungsverordnung als Bezugsgröße
- Ergänzt wird das Framework durch zwei Authentifizierungsprofile zur REFEDS Assurance Suite
  - Single-Factor Authentication Profile: https://refeds.org/profile/sfa
  - Multi-Factor Authentication Profile: https://refeds.org/profile/mfa
- Siehe unter https://refeds.org/assurance

REFEDS Assurance Framework (2)

- Verlässlichkeit wird über drei einzeln adressierbare Komponenten modelliert
  - Eindeutigkeit und Art des Identifikators (identifier uniqueness)
  - Qualität der Identitätsfeststellung (identity assurance)
  - Qualität und Aktualität der Attributwerte (attribute assurance).
- Zur Beschreibung der drei Komponenten existiert ein kontrolliertes Vokabular
- Die entsprechenden Angaben werden über das Attribut eduPersonAssurance übertragen
- Service Provider können sich die für den jeweiligen Dienst relevanten Angaben „herauspicken“
  - Daneben existieren aber auch zwei Profile, die Kombinationen abbilden

REFEDS Assurance Suite



Konformitätskriterien

- Identity Provider müssen grundsätzlich vier Konformitätskriterien erfüllen
  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
- Aktuelle Einschätzung: für die allermeisten der teilnehmenden Einrichtungen kein Problem
- Erfüllung der Kriterien zukünftig Voraussetzung für Teilnahme an DFN-AAI

Identifier uniqueness (1)

Attributwert	https://refeds.org/assurance**/ID/unique**
Bedingungen	1. The user identifier represents a single natural person 2. The CSP can contact the person to whom the identifier is issued 3. The user identifier is never re-assigned 4. The user identifier is eduPersonUniqueId, SAML 2.0 persistent name identifier, subject-id or pairwise-id or OpenID Connect sub (public or pairwise)

- Alle 4 Bedingungen müssen erfüllt sein
- CSP = Credential Service Provider
  üblicherweise die Heimateinrichtung (IdM- und IdP-Betreiber)

Identifier uniqueness (2)

Falls eduPersonPrincipalName als Identifier zum Einsatz kommt:

Attributwert	https://refeds.org/assurance**/ID/eppn-unique-no-reassign**
Bedingungen	eduPersonPrincipalName value has the Unique 1-3 properties

Attributwert	https://refeds.org/assurance**/ID/eppn-unique-reassign-1y**
Bedingungen	eduPersonPrincipalName value has the Unique 1 and 2 property but may be re-assigned after a hiatus period of 1 year or longer

- Falls die Bedingungen nicht erfüllt sind: keine Angabe machen

Identity proofing etc. (1)

- Identity proofing and credential issuance, renewal and replacement
- Drei Bezugssysteme
  - Interoperable Global Trust Federation (IGTF):
    IGTF Profiles of Authentication Assurance Version 1.0 (aktuell: Version 1.1)
  - Kantara Initiative: Kantara Identity Assurance Framework. KIAF-1420 Operational -63r2 Service Assessment Criteria (OP_SAC), Version 1.0
    Link zu Version 1.1: https://kantarainitiative.org/download/7663
  - eIDAS Durchführungsverordnung zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel […]
- Vgl. Comparison Guide to Identity Assurance Mappings for Infrastructures

Identity proofing etc. (2)

Attributwert	https://refeds.org/assurance**/IAP/low**
Bedingungen	[siehe Spezifikation] – Prozesse müssen dokumentiert sein; Rückführbarkeit
Beispiel	self-asserted identity together with verified e-mail address

Attributwert	https://refeds.org/assurance**/IAP/medium**
Bedingungen	z.B. eIDAS ‚niedrig' gemäß Abs. 2.1.2 (Identitätsnachweis und -überprüfung), 2.2.2 (Ausstellung, Auslieferung und Aktivierung), 2.2.4 (Verlängerung und Ersetzung): Beweismittel erforderlich „es kann davon ausgegangen werden, dass…", „eine verlässliche Quelle…"
Beispiel	the person has sent a copy of their government issued photo-ID to the CSP and the CSP has had a remote live video conversation with them

Identity proofing etc. (3)

Attributwert	https://refeds.org/assurance**/IAP/high**
Bedingungen	z.B. eIDAS ‚substanziell' gemäß Abs. 2.1.2 (Identitätsnachweis und -überprüfung), 2.2.2 (Ausstellung, Auslieferung und Aktivierung), 2.2.4 (Verlängerung und Ersetzung)
Beispiel	the person has presented an identity document that is checked to be genuine and represent the claimed identity and steps have been taken to minimise the risk of a lost, stolen, suspended, revoked or expired document, following sections 2.1.2, 2.2.2 and 2.2.4 of eIDAS assurance level substantial

- Fazit: RAF kann ein höheres Vertrauensniveau adressieren, als die Verlässlichkeitsklassen: ‚Advanced' entspricht allenfalls /IAP/medium

Identity proofing etc. (4)

Attributwert	https://refeds.org/assurance**/IAP/local-enterprise**
Bedingungen	The identity proofing and credential issuance, renewal and replacement are done in a way that qualifies (or would qualify) the user to access the Home Organisation's internal administrative systems
Beispiele	Systems that deal with • money (e.g. travel expense management systems or invoice circulation systems) • employment-related personal data (e.g. employee self-service interfaces provided by the Human Resources systems) • student information (e.g. administrative access to the student information system)

Attribute quality and freshness

Attributwert	https://refeds.org/assurance**/ATP/ePA-1m**
Bedingungen	eduPersonAffiliation, eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes (if populated and released to the RP) reflect user's departure within 31 days time

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

„‘A Departure‘ takes place when the organisation decides that the user doesn't have a continuing basis for the affiliation value and therefore loses their organisational role and privileges"

Weitere Hinweise

- Belegung des Attributs eduPersonAssurance mit Werten
  - Erfüllung der Konformitätskriterien wird mit dem ‚Prefix' deklariert:
    `https://refeds.org/assurance`
  - Bei /IAP/medium und /IAP/high müssen die jeweils niedrigeren Stufen mit übertragen werden. Analog ist bei /ATP/ePA-1d zu verfahren, hier muss /ATP/ePA-1m mit angegeben werden, also z.B.
    `https://refeds.org/assurance/IAP/low`
    `https://refeds.org/assurance/IAP/medium`
    `https://refeds.org/assurance/ATP/ePA-1m`
    `https://refeds.org/assurance/ATP/ePA-1d`
- Dokumentation mit Konfigurationsbeispielen für Shib IdP und SP im Wiki:
  https://doku.tid.dfn.de/de:aai:assurance

Ausblick auf RAF 2.0

- Keine externen Referenzsysteme mehr, sondern direkte Empfehlungen bzw. Richtlinien
- ../IAP/low
  - The user is a Person with a self-asserted identity.
- ../IAP/medium*
  - The user is a known Person with a reasonably validated identity.
- ../IAP/high*
  - The user is a Person with a validated and verified identity.

* The trusted source shall be appropriate and authoritative in the CSP’s context

Vielen Dank! Haben Sie noch Fragen?

- Kontakt
  - Wolfgang Pempe

    Teamleiter DFN-AAI
    E-Mail: pempe@dfn.de
    Telefon: +49 30 884299-380
    Fax: +49 30 884299-370

    Anschrift:
    DFN-Verein, Geschäftsstelle
    Alexanderplatz1
    10178 Berlin

REFEDS

- REFEDS = **R**esearch and **E**ducation **Fed**eration**s**
- Diskussionsforum und Interessensvertretung:
  „is to be the voice that articulates the mutual needs of research and education identity federations worldwide.“ (https://refeds.org)
- Gehostet von GÉANT
- Diverse Arbeitsgruppen
  - Darunter auch die Assurance Working Group
  - Spezifikationen für die sog. REFEDS Assurance Suite bereits 2017 und 2018 erstellt: REFEDS Assurance Framework zzgl. Authentication Profiles

Wie geht es weiter?

- Nach über zehn Jahren Betriebserfahrung
  - Verfahren ist zu statisch - eine Verlässlichkeitsklasse pro IdP → Speziallösungen für Identitäten, die nicht den Anforderungen genügen
  - Verlässlichkeitsklasse = Kombination unterschiedlicher Kriterien, diese können nicht separat von SP adressiert werden
  - Insellösung – die Klassen sind DFN-AAI-spezifisch und werden international nicht verstanden (→ eduGAIN)
- Gestaltung Verlässlichkeit für die kommenden Jahre
  - IdM-Merkmale als Attribute übermitteln → REFEDS Assurance Framework: flexibel, Verlässlichkeit kann pro Identität angegeben werden
  - Bestandteil der AAIplus-Initiative