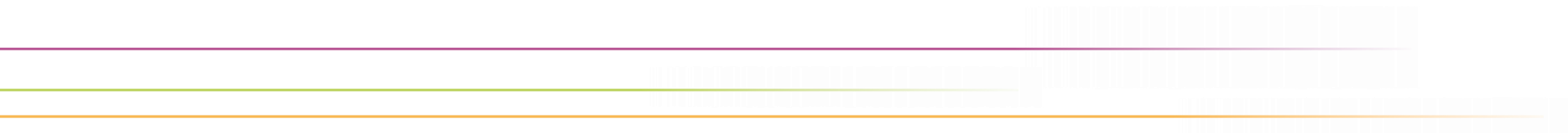


DEN  
deutsches forschungsnetz

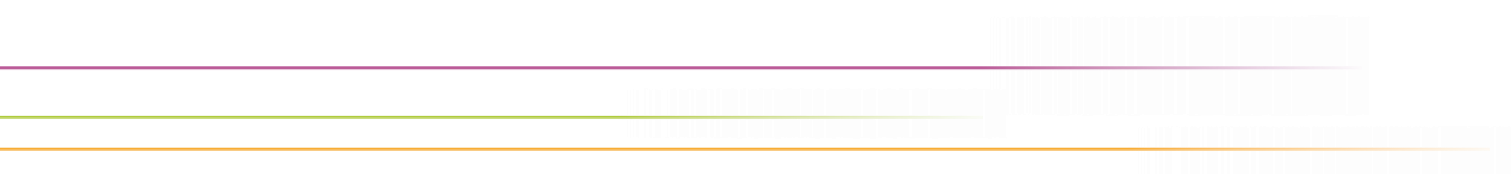




# REFEDS Assurance Suite

DFN-AAI Workshop Februar 2022 | 7. Februar 2022

Wolfgang Pempe ([pempe@dfn.de](mailto:pempe@dfn.de))



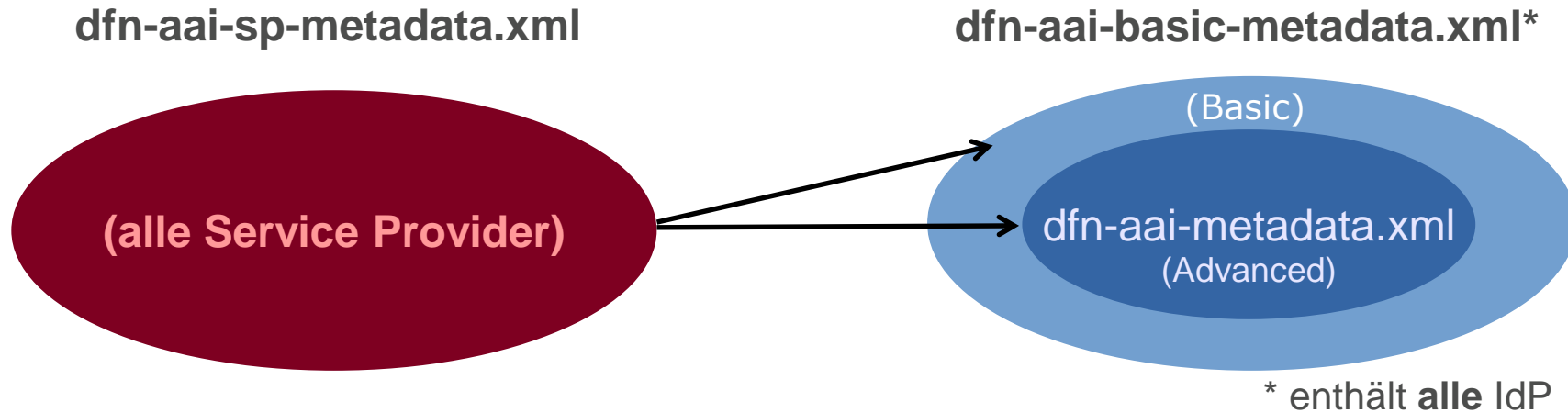
- ▶ REFEDS = **R**esearch and **E**ducation **F**ederations
- ▶ Diskussionsforum und Interessensvertretung:  
„is to be the voice that articulates the mutual needs of research and education identity federations worldwide.“ (<https://refeds.org>)
- ▶ Gehostet von GÉANT
- ▶ Diverse Arbeitsgruppen
  - ▶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

# Verlässlichkeitsklassen in der DFN-AAI

Verlässlichkeitsklasse	Identifizierung durch Heimateinrichtung	Verfahren zum Ausweis einer Identität	Datenhaltung und Prozesse zur Pflege der Identitäten
n.a. / Test	Verfahren freigestellt	Verfahren freigestellt	Verfahren freigestellt
Basic	Rückantwort von eindeutiger Adresse (E-Mail, Tel.-Nr., Postanschrift, etc.)	Anhand eindeutig zuzuordnender digitalen Adresse	Verpflichtung bzgl. Aktualität innerhalb von 3 Monaten
Advanced	pers. Vorsprechen gegenüber Vertrauensinstanz unter Vorlage amtlicher Dokumente (alternativ: Post-Ident, eID/nPA). Die an den Hochschulen etablierten Einschreibungs- und Einstellungsprozesse werden als gleichwertig akzeptiert	pers. Account bzw. digitales Zertifikat (sichere Vergaberichtlinie)	Verpflichtung bzgl. Aktualität innerhalb von 2 Wochen

Vgl. [https://doku.tid.dfn.de/de:degrees\\_of\\_reliance](https://doku.tid.dfn.de/de:degrees_of_reliance)

# Umsetzung (1) getrennte Metadatensätze



	IdP / AA	SP
Advanced	dfn-aai-sp-metadata.xml	dfn-aai-metadata.xml
Basic	dfn-aai-sp-metadata.xml	-
Advanced + Basic	-	dfn-aai-basic-metadata.xml
eduGAIN	dfn-aai-edugain+sp-metadata.xml	dfn-aai-edugain+idp-metadata.xml
Lokale Metadaten	dfn-aai-local-999-metadata.xml*	dfn-aai-local-999-metadata.xml*

<https://doku.tid.dfn.de/de:production>

\* „999“ wird durch einrichtungs-spezifische Nummer ersetzt

# Umsetzung (2) Entity Attribute

## Identity Provider

```
<mdattr:EntityAttributes>  
  <saml:Attribute Name="http://aai.dfn.de/loa/degree-of-reliance"  
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-uri">  
    <saml:AttributeValue>basic</saml:AttributeValue>  
  </saml:Attribute>  
</mdattr:EntityAttributes>
```

## Service Provider

```
<mdattr:EntityAttributes>  
  <saml:Attribute Name="http://aai.dfn.de/require-loa/degree-of-reliance"  
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-uri">  
    <saml:AttributeValue>basic</saml:AttributeValue>  
  </saml:Attribute>  
</mdattr:EntityAttributes>
```

Siehe auch unter [https://doku.tid.dfn.de/de:entity\\_attributes](https://doku.tid.dfn.de/de:entity_attributes)

## 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

# 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>



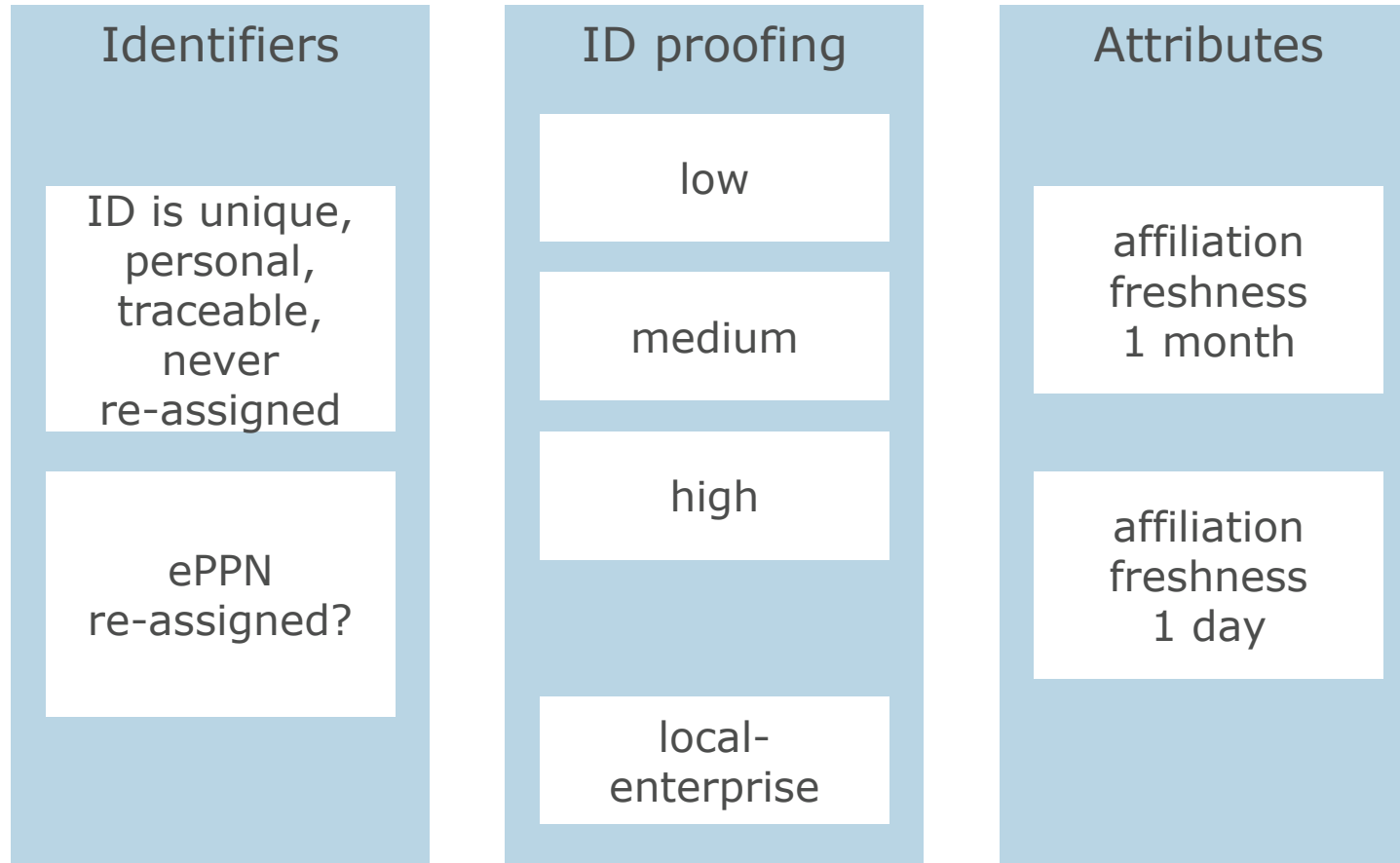
## REFEDS Assurance Framework (2)

- ▶ 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

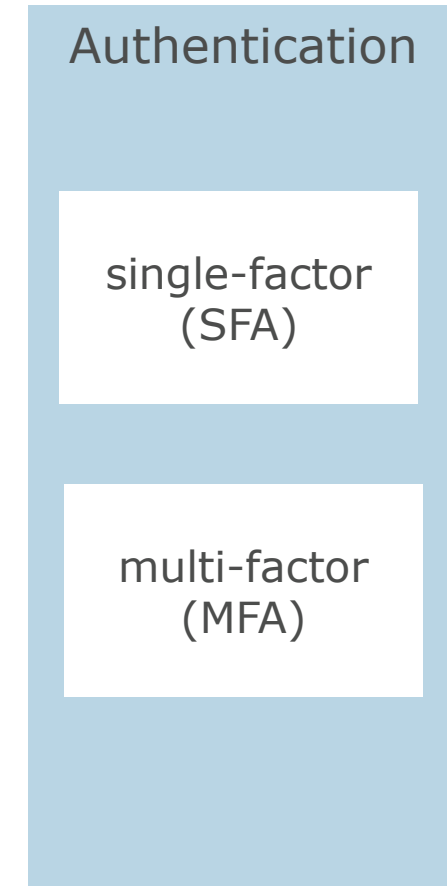
# REFEDS Assurance Suite

DFN

## REFEDS Assurance Framework (RAF)



## AuthN Profiles



# 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	<a href="https://refeds.org/assurance/ID/unique">https://refeds.org/assurance/ID/unique</a>
Bedingungen	<ol style="list-style-type: none"><li>1. The user identifier represents a single natural person</li><li>2. The CSP can contact the person to whom the identifier is issued</li><li>3. The user identifier is never re-assigned</li><li>4. The user identifier is eduPersonUniqueId, SAML 2.0 persistent name identifier, subject-id or pairwise-id or OpenID Connect sub (public or pairwise)</li></ol>

- ▶ 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	<a href="https://refeds.org/assurance/ID/eppn-unique-no-reassign">https://refeds.org/assurance/ID/eppn-unique-no-reassign</a>
Bedingungen	eduPersonPrincipalName value has the Unique 1-3 properties

Attributwert	<a href="https://refeds.org/assurance/ID/eppn-unique-reassign-1y">https://refeds.org/assurance/ID/eppn-unique-reassign-1y</a>
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	<a href="https://refeds.org/assurance/IAP/low">https://refeds.org/assurance/<b>IAP/low</b></a>
Bedingungen	[siehe Spezifikation] – Prozesse müssen dokumentiert sein; Rückführbarkeit
Beispiel	self-asserted identity together with verified e-mail address

Attributwert	<a href="https://refeds.org/assurance/IAP/medium">https://refeds.org/assurance/<b>IAP/medium</b></a>
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	<a href="https://refeds.org/assurance/IAP/high">https://refeds.org/assurance/<b>IAP/high</b></a>
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	<a href="https://refeds.org/assurance/IAP/local-enterprise">https://refeds.org/assurance/<b>IAP/local-enterprise</b></a>
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 <ul style="list-style-type: none"><li>• money (e.g. travel expense management systems or invoice circulation systems)</li><li>• employment-related personal data (e.g. employee self-service interfaces provided by the Human Resources systems)</li><li>• student information (e.g. administrative access to the student information system)</li></ul>

# Attribute quality and freshness

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

Attributwert	<a href="https://refeds.org/assurance/ATP/ePA-1d">https://refeds.org/assurance/ATP/ePA-1d</a>
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>

## Assurance Profiles

- ▶ Cappuccino for low-risk research use cases  
(\$PREFIX\$/profile/cappuccino)
- ▶ Espresso for use cases requiring verified identity  
(\$PREFIX\$/profile/espresso)
- ▶ Aktuell sind (mir!) keine Anwendungsfälle bekannt...

Value	Cappuccino	Espresso
\$PREFIX\$	X	X
\$PREFIX\$/ID/unique	X	X
\$PREFIX\$/ID/eppn-unique-no-reassign		
\$PREFIX\$/ID/eppn-unique-reassign-1y		
\$PREFIX\$/IAP/low	X	X
\$PREFIX\$/IAP/medium	X	X
\$PREFIX\$/IAP/high		X
\$PREFIX\$/IAP/local-enterprise		
\$PREFIX\$/ATP/ePA-1m	X (*)	X (*)
\$PREFIX\$/ATP/ePA-1d		

# Die Modelle im Vergleich

REFEDS Assurance Suite	DFN-AAI Verlässlichkeitsklassen
RAF identifier uniqueness	Keine direkte Entsprechung
RAF identity proofing and credential issuance, renewal and replacement	Verfahren zur Identifizierung durch die nutzende Einrichtung
RAF attribute quality and freshness	Datenhaltung und Prozesse zur Pflege der Identitäten
single-factor / multi-factor authentication profile	Verfahren zum Ausweis einer Identität

# Roadmap

## ▶ Februar 2022

- ▶ Workshops zur Umsetzung Assurance Framework und MFA

## ▶ Ende März 2022

- ▶ Abschaffung der Trennung der Metadatenätze 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 Authentication Profiles

- ▶ Spezifikation und Identifier:
  - ▶ <https://refeds.org/profile/sfa>
  - ▶ <https://refeds.org/profile/mfa>
- ▶ Transport über `AuthnContextClassRef` in SAML Assertion (OIDC: `acr claim`)
- ▶ Dokumentation im AAI-Wiki folgt demnächst
- ▶ Service Provider, die SFA-/MFA-Profil verlangen:
  - ▶ SFA: ???
  - ▶ MFA: National Institutes of Health (NIH): angekündigt, bei einem SP umgesetzt  
<https://spaces.at.internet2.edu/display/federation/get-nih-ready>

- ▶ Minimalanforderungen für den Einsatz von Authentifizierungs-Verfahren
  - ▶ Memorized Secret
  - ▶ OTP-Device
  - ▶ Out-of-Band Device
  - ▶ Look-Up Secret
  - ▶ Cryptographic Device/Software
  
- ▶ Weitere Anforderungen bezüglich der Kriterien
  - ▶ Schutz vor Brute-Force Attacken
  - ▶ Absicherung des Transports von Authentication Secrets
  - ▶ Tausch und Erneuerung von Authentication Secrets



► Anforderungen:

1. The authentication of the user's current session used a combination of at least two of the four distinct types of factors defined in [ITU-T X.1254](#): something you **know**, something you **have**, something you **are**, something you **do**)
2. The factors used are independent, in that access to one factor does not by itself grant access to other factors
3. 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

► Ausführliche FAQ mit Beispielen für SP- und IdP-Betreiber:

<https://wiki.refeds.org/display/PRO/MFA+Profile+FAQ>

# Praktische Hinweise

- ▶ Shibboleth Identity Provider
  - ▶ Mehr dazu morgen, 8.2.2022, Vorträge von David Hübner und Steffen Hofmann
  - ▶ <https://doku.tid.dfn.de/de:aai:events:ws2022>
- ▶ Shibboleth Service Provider
  - ▶ Anleitung im Shibboleth Wiki: [Requiring Multi-Factor Authentication](#)
  - ▶ Einige Gedanken hierzu auf den kommenden Folien...

# Shibboleth SP und MFA

- ▶ Autorisierung im Apache Webserver

```
require authnContextClassRef https://refeds.org/profile/mfa
```

- ▶ REFEDS MFA anfordern, AuthnContextClassRef im AuthnRequest

- ▶ Webserver Konfiguration

```
ShibRequestSetting authnContextClassRef https://refeds.org/profile/mfa
```

- ▶ Parameter in <ApplicationDefaults> in /etc/shibboleth2.xml

```
<ApplicationDefaults ...
```

```
authnContextClassRef="https://refeds.org/profile/mfa" ...>
```

- ▶ Login Handler (/Shibboleth.sso/Login): URL Parameter

```
authnContextClassRef=https%3a%2f%2frefeds.org%2fprofile%2fmfa
```

# Shibboleth SP – Error Handling (1)

- ▶ Wie damit umgehen, wenn der IdP keinen entsprechenden Authentication Context “liefert”?
- ▶ Shibboleth Wiki (Seite [Requiring Multi-Factor Authentication](#)):
  - ▶ Angepasste Error-Seite, die die IdP-seitigen Fehlermeldungen als URL-Parameter auswertet
- ▶ Nachteil: SP muss auf alle Fehler des IdP reagieren...



## **opensaml::FatalProfileException**

The system encountered an error at Sun Feb 6 17:03:26 2022

To report this problem, please contact the site administrator at [hotline@aai.dfn.de](mailto:hotline@aai.dfn.de).

Please include the following message in any email:

**opensaml::FatalProfileException at (https://sp-dev.aai.dfn.de/Shibboleth.sso/SAML2/POST)**

SAML response reported an IdP error.

Error from identity provider:

**Status:** urn:oasis:names:tc:SAML:2.0:status:Requester

**Sub-Status:** urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext

**Message:** An error occurred.

## Shibboleth SP – Error Handling (2)

- ▶ Alternative: Session Hook Mechanismus mit AttributeChecker Handler  
<https://wiki.geant.org/display/eduGAIN/How+to+configure+Shibboleth+SP+attribute+checker>
- ▶ Autorisierung durch SP selber (kein `require` Parameter im Webserver)
- ▶ Zunächst alternative `authnContextClassRef` anbieten, z.B.

```
<ApplicationDefaults ...  
  authnContextClassRef="https://refeds.org/profile/mfa  
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"  
  authnContextComparison="maximum"  
  sessionHook="/Shibboleth.sso/AttrChecker" ...>
```

## Shibboleth SP – Error Handling (3)

- ▶ Attribute Checker Handler konfigurieren

```
<Handler type="AttributeChecker" Location="/AttrChecker"  
  template="attrChecker.html" flushSession="true">  
  <Rule require="authnContextClassRef">https://refeds.org/profile/mfa</Rule>  
</Handler>
```

(bestehende Rules ggf.entsprechend erweitern)

- ▶ Auf attrChecker.html dann entsprechende Informationen liefern und ggf. Step-up Authentication triggern

# Shibboleth SP – Error Handling (4)

Ganz simples Beispiel:



**We're sorry, but you cannot access this service.**

This service requires Multi-Factor Authentication, which the Identity Provider (DFN Test-IdP 1) doesn't seem to support. Please contact your home organisation's helpdesk (here: <mailto:hotline@aai.dfn.de>)

For more information about this service, including what user information is required for access, please visit [our information page](#).

# Vielen Dank! Haben Sie noch Fragen?

DFN

## ► Kontakt

### ► Wolfgang Pempe

Teamleiter DFN-AAI

E-Mail: [pempe@dfn.de](mailto:pempe@dfn.de)

Telefon: +49 30 884299-380

Fax: +49 30 884299-370

Anschrift:

DFN-Verein, Geschäftsstelle

Alexanderplatz1

10178 Berlin

