deutsches forschungsnetz

OpenID Connect Federation

80. DFN-Betriebstagung | 19. März 2024

Wolfgang Pempe (pempe@dfn.de)

Der Kontext:

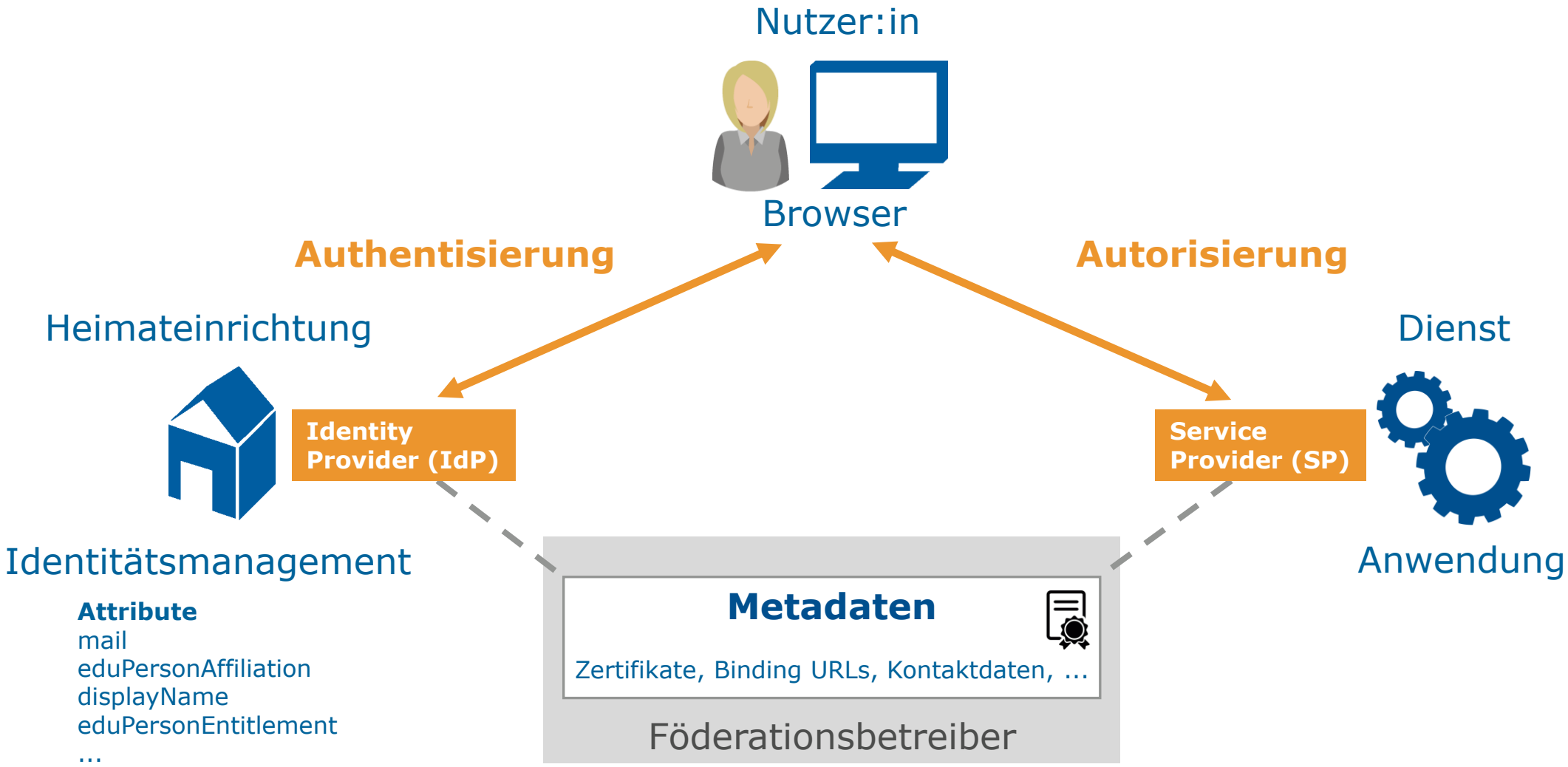
AAI, föderierte Identitäten, Web-SSO

Quelle: Classical Numismatic Group, Inc. http://www.cngcoins.com, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=510430

Föderation

- Föderiertes Identitätsmanagement erfordert zentrale Instanz: Föderationsbetreiber
  - definiert die organisatorischen, technischen und rechtlichen Rahmenbedingungen und stellt deren Einhaltung sicher
  - etabliert auf diese Weise das Vertrauensverhältnis innerhalb der Föderation
  - „Trusted Third Party“
- DFN-Verein ist Betreiber der einrichtungsübergreifenden Föderation DFN-AAI
  - Zielgruppe: Hochschulen und Forschungseinrichtungen
  - hält Dienstvereinbarungen mit über 430 Einrichtungen aus der Wissenschaft
  - hält über 200 Dienstvereinbarungen mit Dienstanbietern außerhalb der Wissenschaft
- Konzept der Föderation erlaubt Hierarchien (Interföderation eduGAIN, Subföderationen)

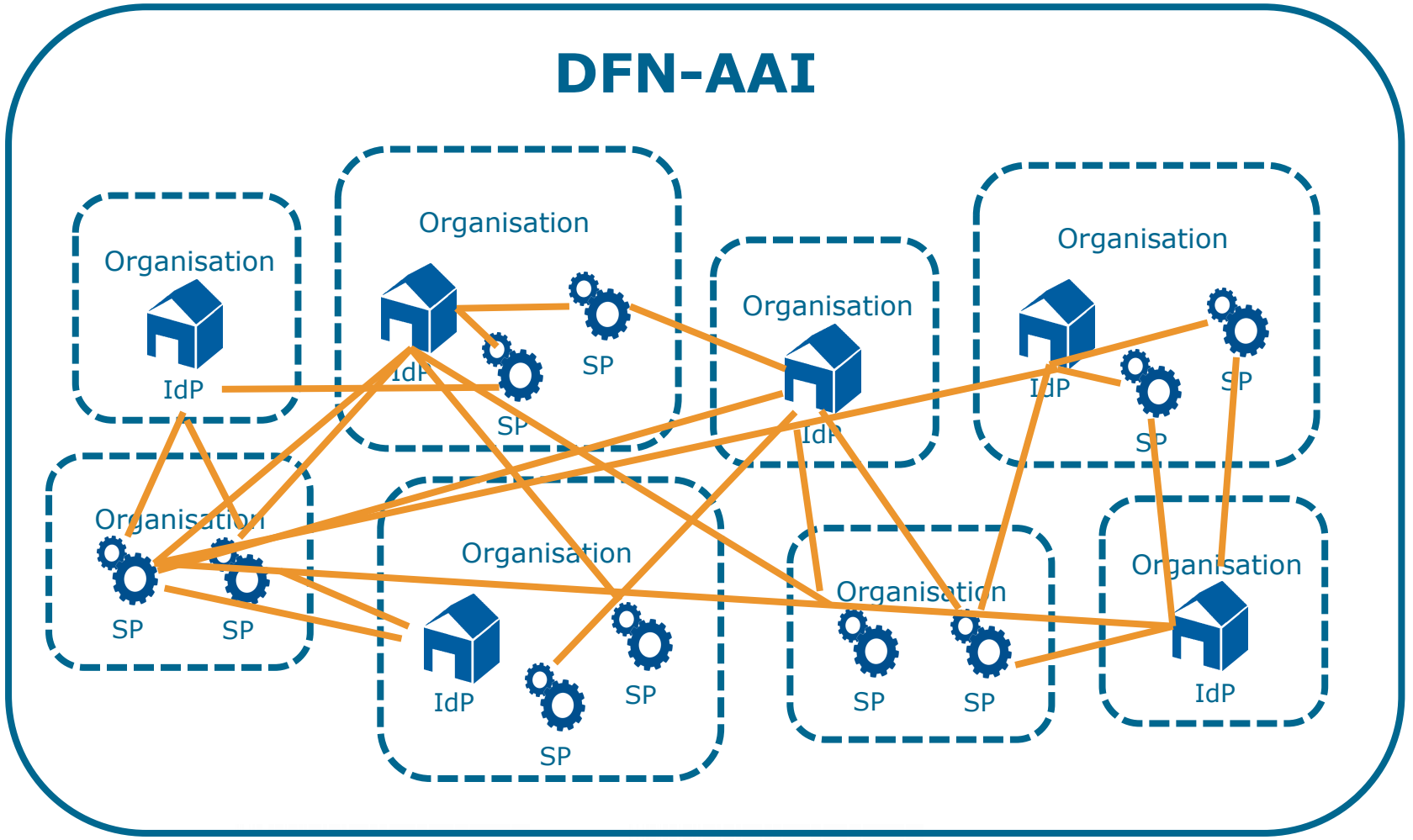
Wie funktioniert eine Föderation?



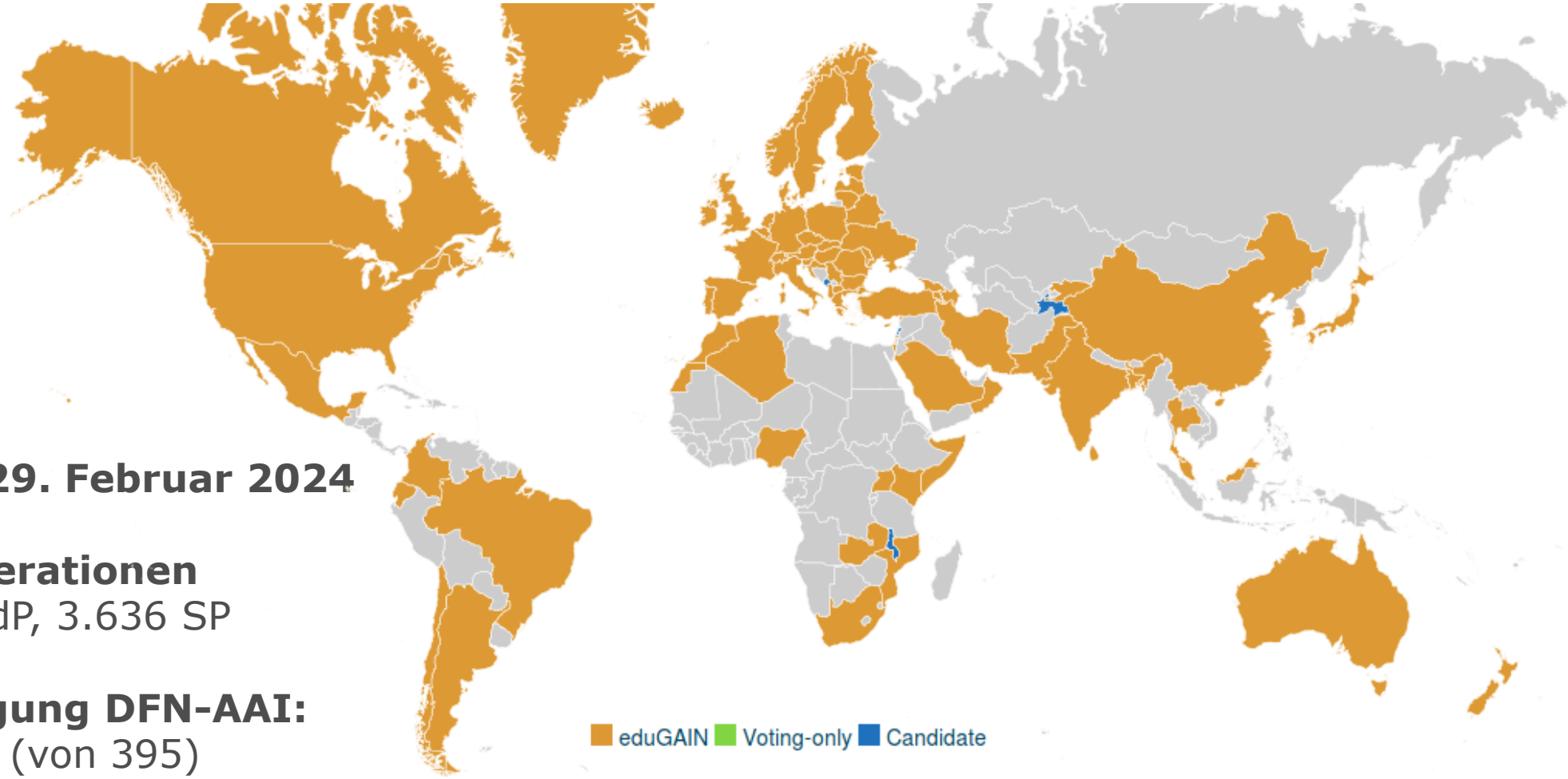
Beispiel DFN-AAI

- **Föderationsbetreiber**
  DFN-Verein
- **Vertrauen**
  Verträge mit allen Teilnehmern, Policies, Levels of Assurance
- **Technik**
  Metadatenverwaltung und –Signierung

Aktuell ~395 aktiv teilnehmende Einrichtungen und 830 Dienste (zzgl. ~1600 lokale SP)



eduGAIN – beteiligte Föderationen



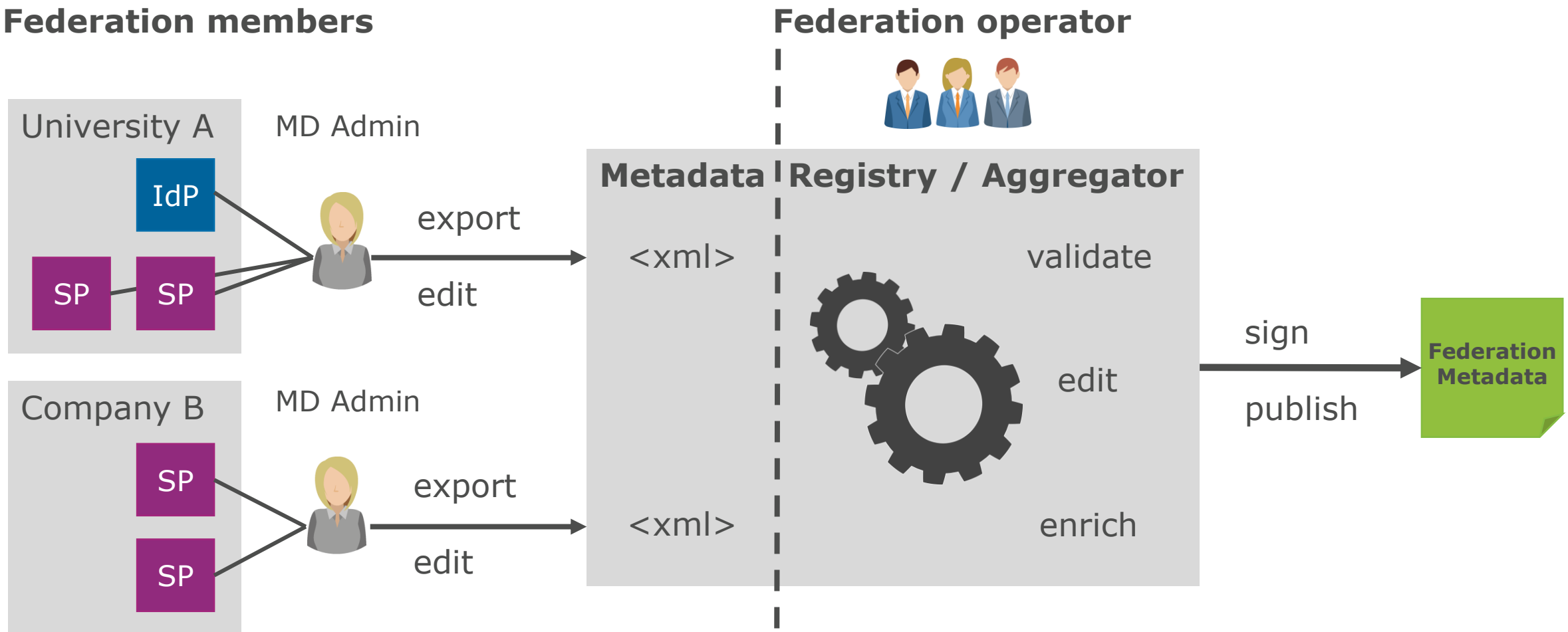
Stand 29. Februar 2024

79 Föderationen
5.551 IdP, 3.636 SP

Beteiligung DFN-AAI:
350 IdP (von 395)
167 SP (von 833)

https://technical.edugain.org

Metadata Aggregation and Management



SAML Metadaten

- Standardisiertes XML-Format
- Enthalten alle Informationen, die für eine Kommunikation zwischen den beteiligten Entities (IdPs, SPs, Attribute Authorities) benötigt werden
- Verfügbar in aggregierter Form (Dateien) oder einzeln via Metadata Query (MDQ)
- Eindeutiger Identifier: Entity ID (Datentyp: anyURI),
  z.B. https://idp.fraunhofer.de/idp/shibboleth
- Einführung und Überblick unter
  https://groups.oasis-open.org/higherlogic/ws/public/document?document_id=51890
- Das Konzept der Föderationsmetadaten macht n:n-Beziehungen skalier- und handhabbar. Kann als eine Art Konfigurationsmanagement verstanden werden.

Föderationen der DFN-AAI

- DFN-AAI („Hauptföderation“) + eduGAIN (optional)
- DFN-AAI-Test
- Lokale Metadaten/Föderationen für ~205 teilnehmende Einrichtungen mit insges. ~1600 SPs
- Spezialföderationen (edu-ID, NFDI, NHR)

- Metadaten werden stündlich neu generiert, signiert und publiziert

OIDC - OpenID Connect

OpenID Connect (OIDC)

- „A simple identity layer on top of the OAuth 2.0 protocol”
- Standard wurde im Februar 2014 verabschiedet
- OIDC und OAuth2 basieren auf REST/JSON + JWT (JSON Web Token), nicht auf Web Browser beschränkt (→ mobile Endgeräte, Apps)
- Infos, Spezifikationen, Software etc. unter http://openid.net/connect/
- Schulungsmaterialien im Wiki: https://doku.tid.dfn.de/de:aai:training
- OIDC Core deckt nur bilaterale Szenarien ab
  - Keine Möglichkeit, multilaterale Föderationen skalierbar zu modellieren

Terminologie im Vergleich (Auswahl)

OpenID Connect	SAML
Open ID Provider (OP)	Identity Provider
Relying Party (RP) / Client	Service Provider
Claim	Attribut
Scope = Gruppe bestimmter Claims	-
-	Scope = Kennung der Heimateinrichtung
Authentication Request	Authentication Request
Client Id, Issuer Identifier, (Entity Identifier*)	Entity ID
…	…

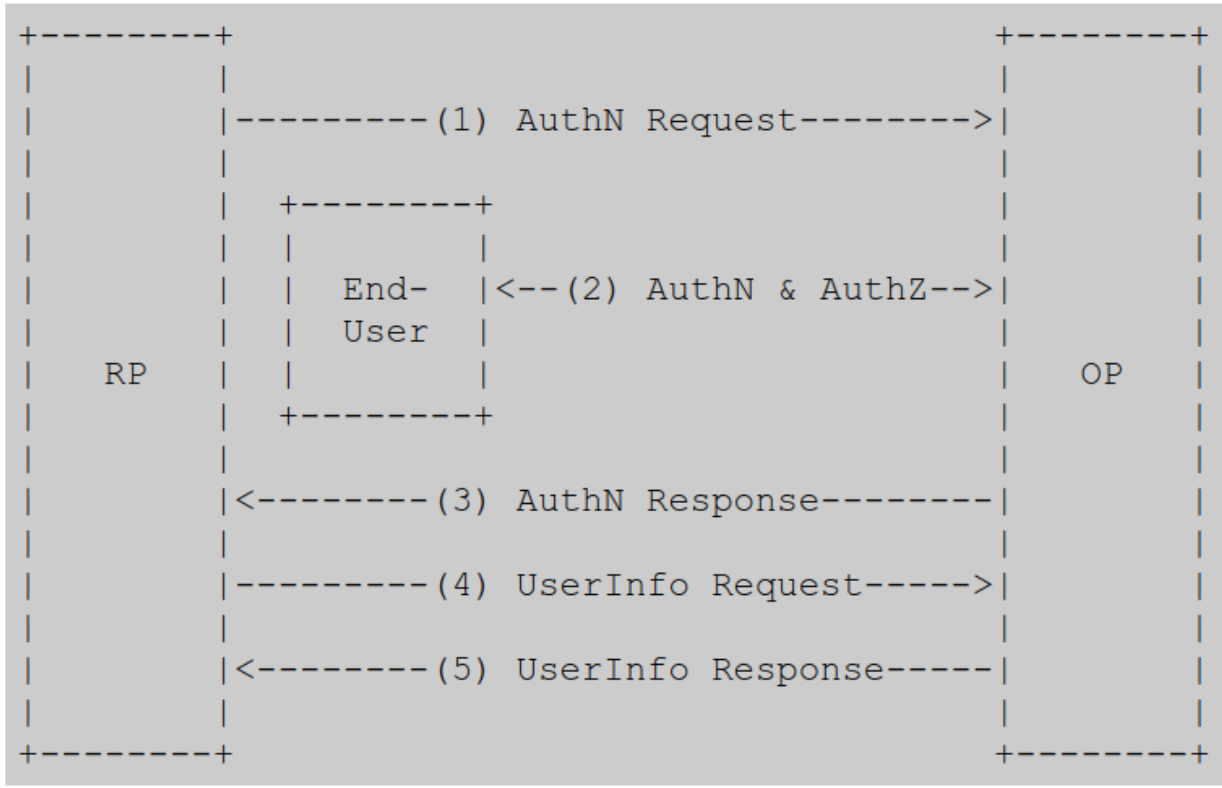
* OpenID Federation

- Details unter

  http://openid.net/specs/openid-connect-core-1_0.html#Terminology

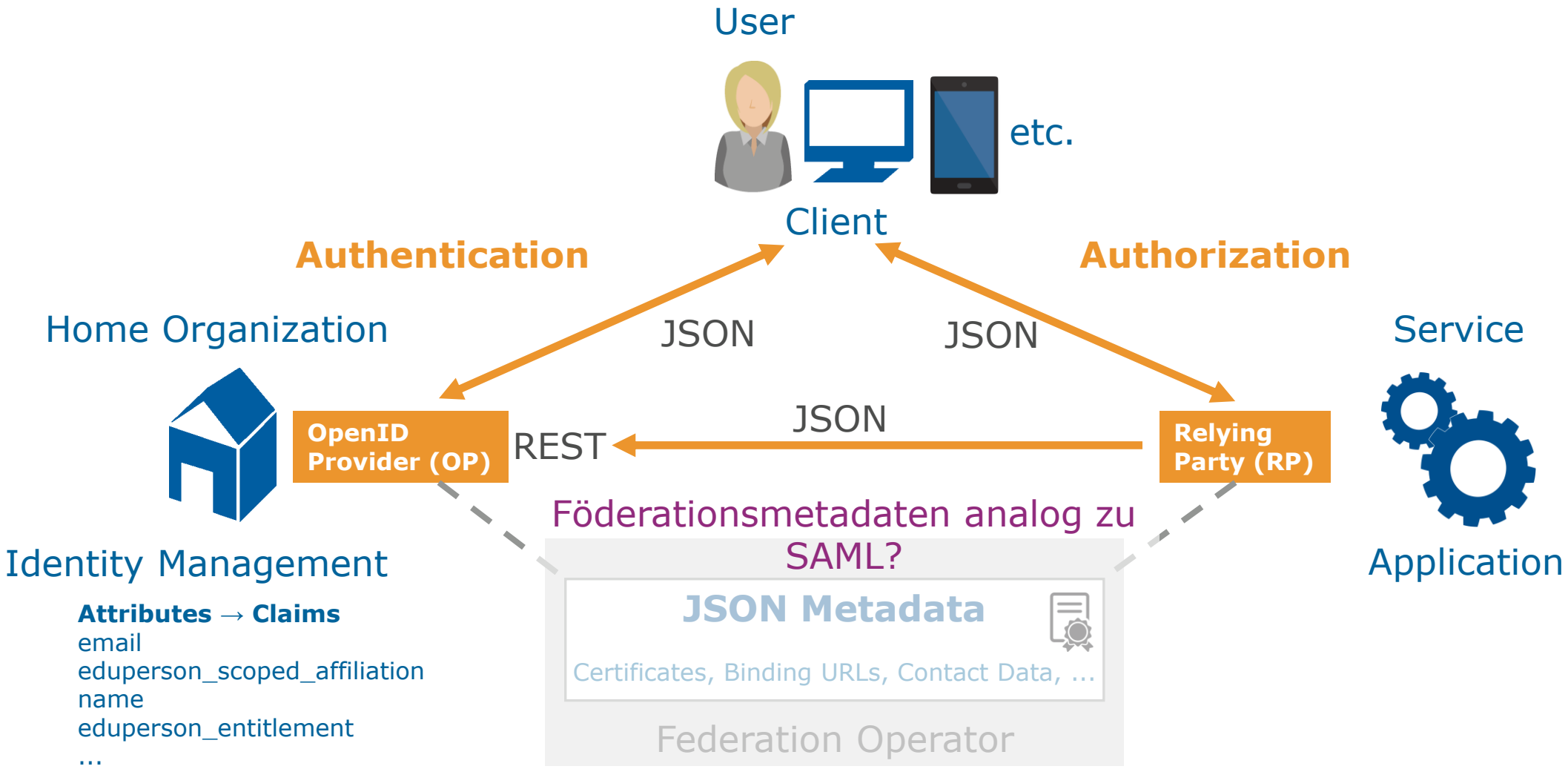
Authentifizierungs-Flow ähnlich SAML

1. The RP (Client) sends a request to the OpenID Provider (OP).
2. The OP authenticates the End-User and obtains authorization.
3. The OP responds with an ID Token and usually an Access Token.
4. The RP can send a request with the Access Token to the UserInfo Endpoint.
5. The UserInfo Endpoint returns Claims about the End-User.



Quelle: https://openid.net/specs/openid-connect-core-1_0.html

Föderation mit OpenID Connect (OIDC)?



Status OpenID Federation

- Seit 2017 in Arbeit, aktuelle Entwurfsfassung #33
- Ursprünglich „OpenID Connect Federation“
- Grundprinzip: Chain of Trust
  - PKI-ähnliches Prinzip: Signaturhierarchien, d.h. jedes Glied der Kette von der jeweils darüber liegenden Entity signiert
  - Ausnahme: Oberstes Glied Trust Anchor selbst-signiert, ähnlich Root-CA
  - Ein RP/OP muss die benötigten Informationen/Metadaten von allen beteiligten Endpunkten abfragen, validieren und schlussendlich zusammenführen
  - Keine Aggregate von Föderationsmetadaten, statt dessen MDQ-basiert
  - Neuer Endpunkt: `/.well-known/openid-federation`

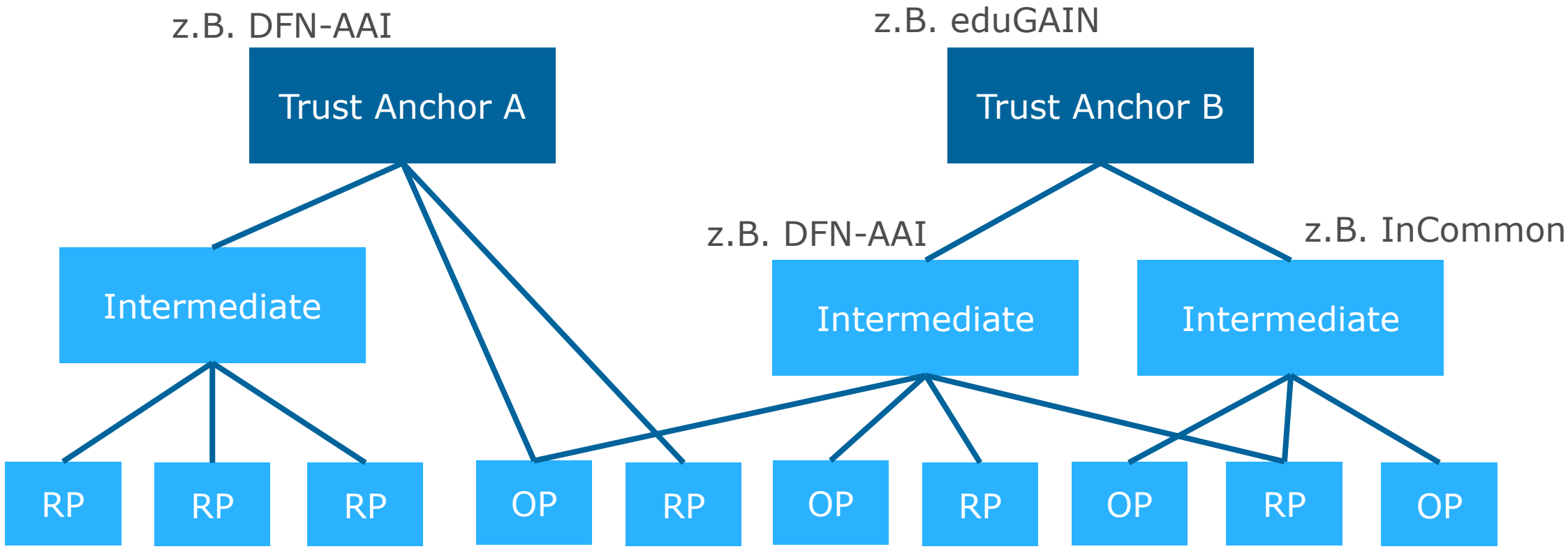
Trust Chain

Drei Typen von Entities

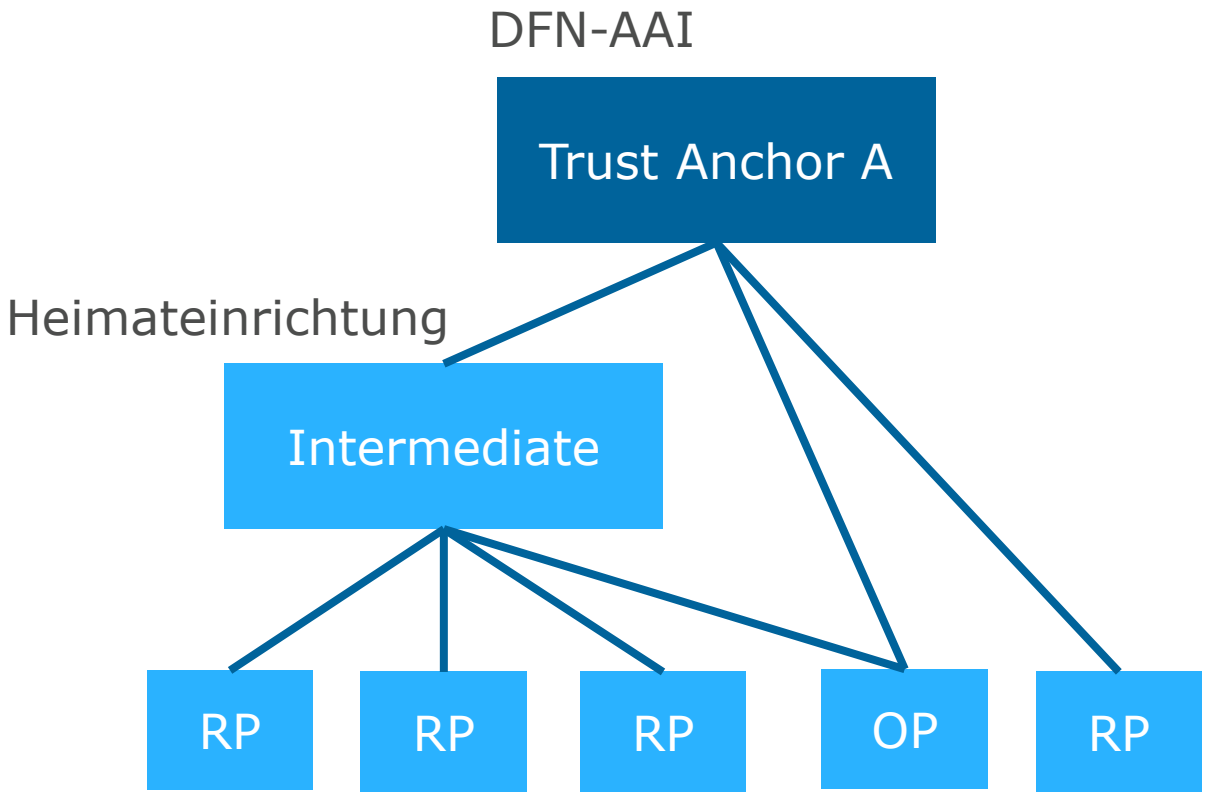
- Trust Anchor
  - Vergleichbar Root CA, Föderationsbetreiber und/oder eduGAIN
- Intermediate
  - z.B. Föderationsbetreiber unterhalb eduGAIN
- Leaf
  - OpenID Provider, Relying Party

Identifiziert über Entity Identifier, der als Basis für `/.well-known` Endpunkte dient -> muss also „funktionierender“ URL sein

Trust Chain – Beispiel Föderationen



Trust Chain – Beispiel lokale Metadaten



Entity Statement

- Signiertes JWT (JSON Web Token) -> JWS (JSON Web Signature)
- Selbst-signiert: Entity Configuration, verfügbar über `/.well-known/openid-federation`
- Von der jeweils darüber liegenden Entity signiert: Subordinate Statement
- Inhalt (Auswahl):
  - `jwks` - eigenes öffentliches Schlüsselmaterial als JWKS (JSON Web Key Set)
  - `metadata` – Angaben zur Entity selbst, z.B. Typ, Kontaktdaten, Endpunkte
    - `federation_fetch_endpoint` – siehe nächste Folie
  - `metadata_policies` – Übergreifende Regeln von „oben" (nicht in Entity Config.), müssen gesammelt und nach festgelegten Regeln zusammengeführt werden
  - `trust_marks` – entspricht ungefähr Entity Attributen in SAML (signed JWT)
  - `authority_hints` – übergeordnete Entities, die Subordinate Statement liefern

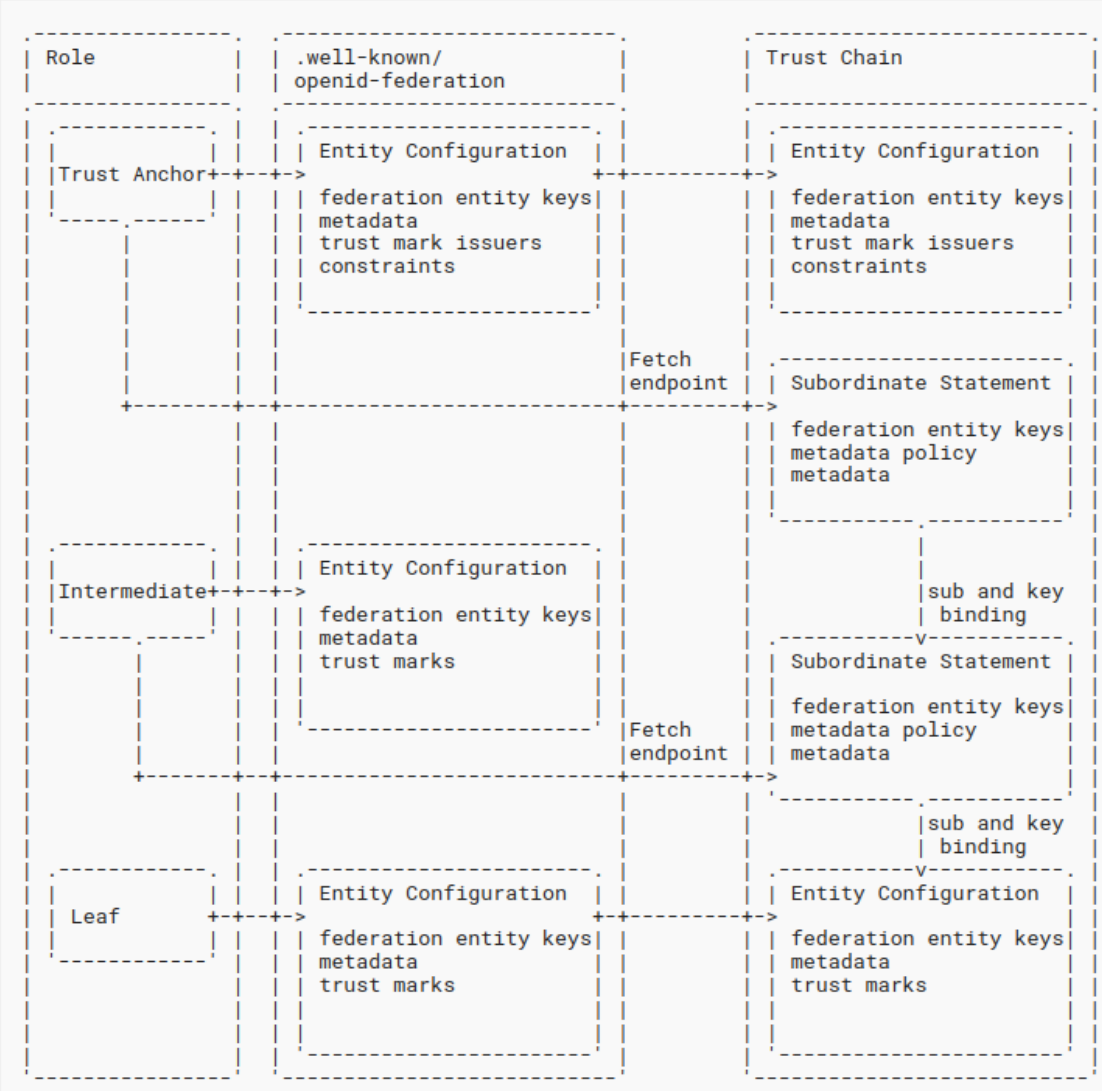
Federation Endpoints

- Modellieren eine Art Metadata-Query-API
- Sind Bestandteil der Entity Configuration von Nicht-Leaf-Entities
- Liefern unter anderem Subordinate Statement
- Auswahl:

Parameter / claim	Endpunkt-Funktion
federation_fetch_endpoint	Entity/Subordinate Statement zu einer Entity
federation_resolve_endpoint	Validiert Trust Chain, Trust Marks etc. und Metadaten zu einer Entity
federation_list_endpoint	Liste von Subordinates
federation_trust_mark_status_endpoint	Gültigkeit von Trust Marks einer Entity (nur Trust Mark Issuers)
federation_historical_keys	Ehemals verwendetes Schlüsselmaterial

OpenID Federation – Trust Chain

Federation Entities

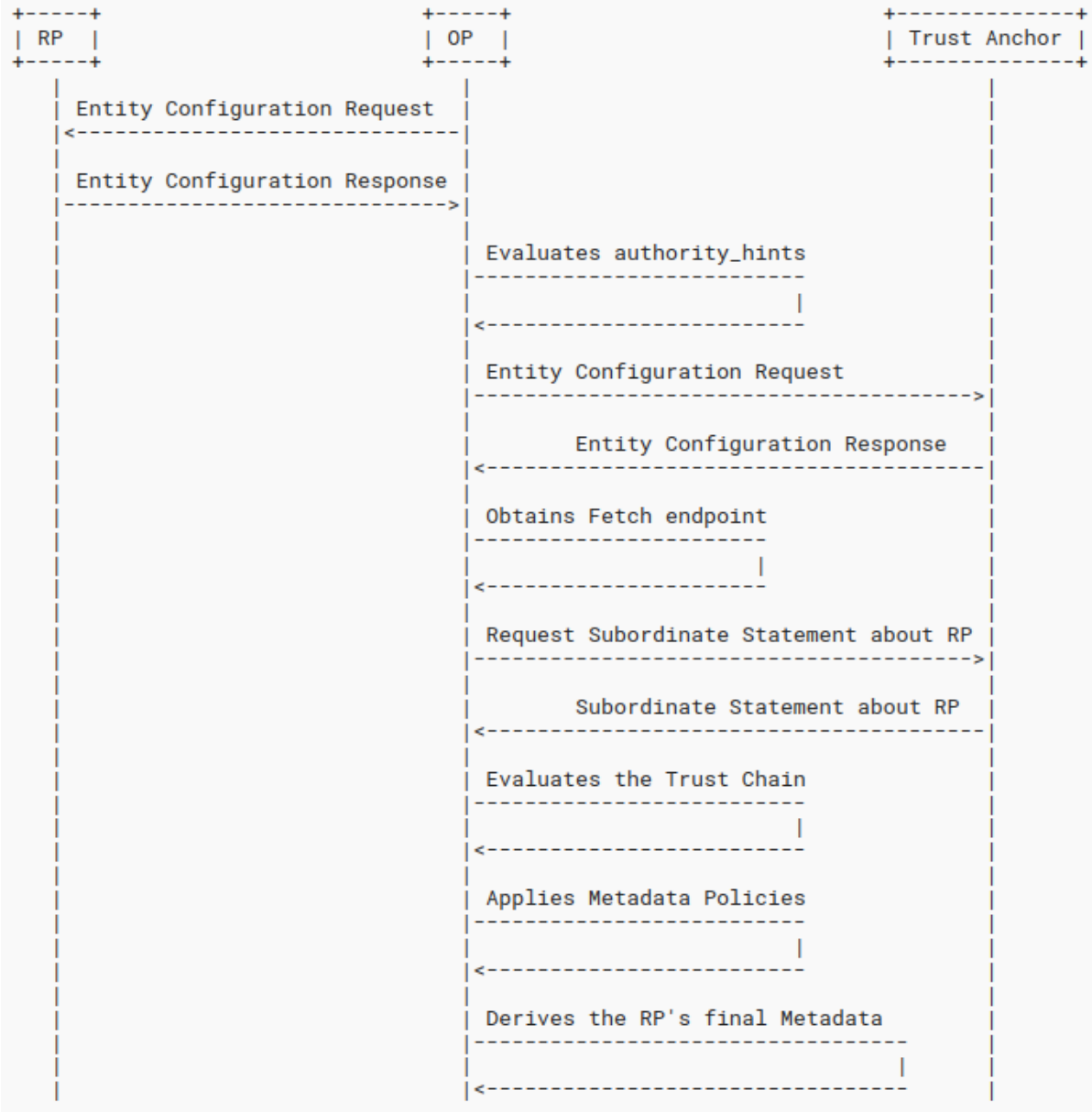


Metadata

https://openid.net/specs/openid-federation-1_0.html#name-trust-chain

Trust Chain Validation (OP)

1. OP MUST have RP's Entity Identifier and a list of Entity Identifiers of Trust Anchors and their public signing keys.
2. OP will first have to fetch sufficient Entity Statements to establish at least one chain of trust from the RP to one or more of the Trust Anchors.
3. Then the OP MUST validate the Trust Chains independently.
4. If there are multiple valid Trust Chains and if the application demands it, the OP MUST choose one to use.

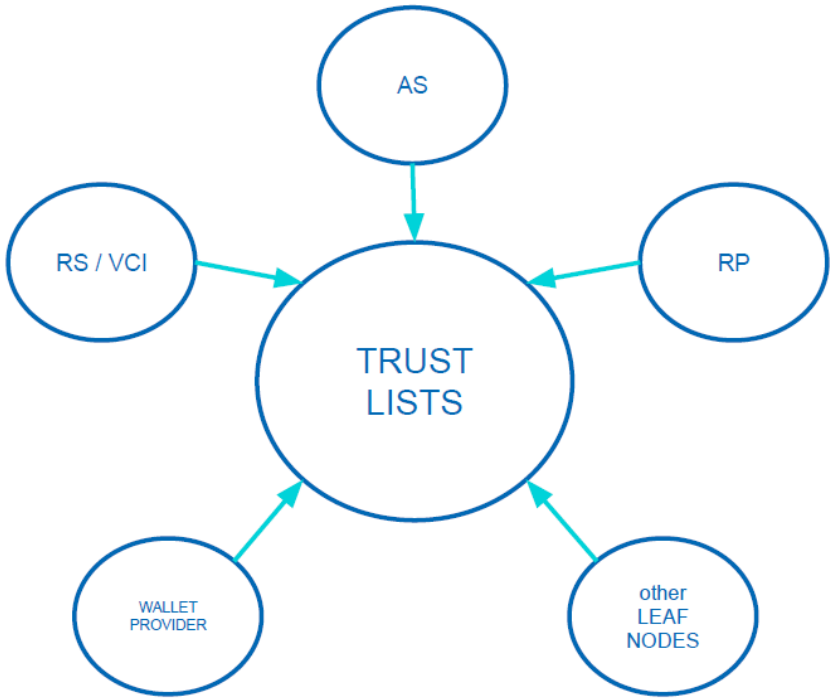


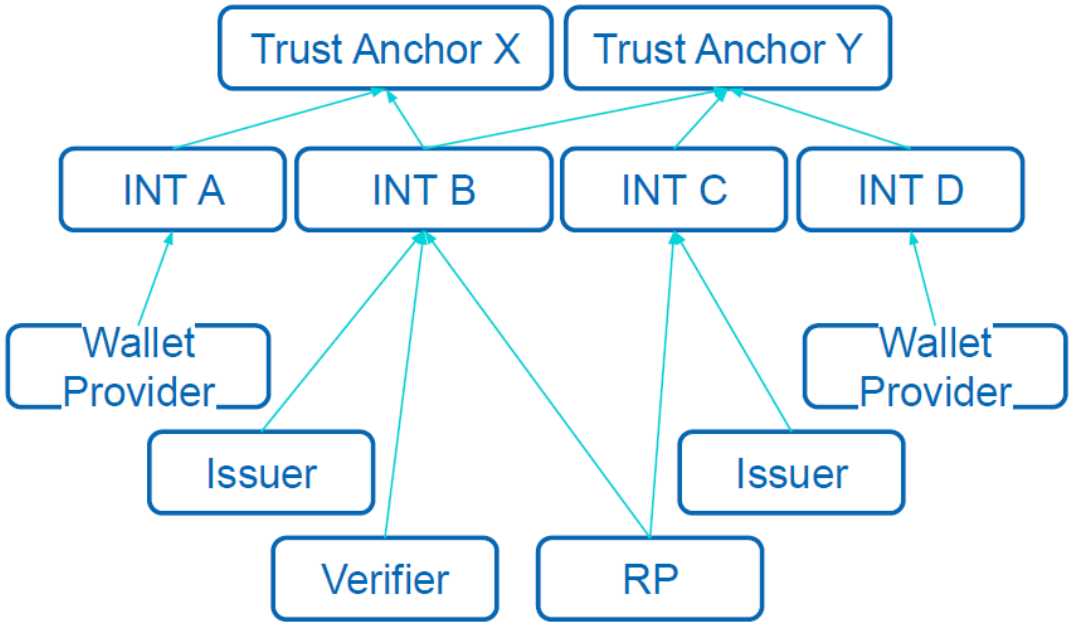
https://openid.net/specs/openid-federation-1_0.html#name-fetching-entity-statements-

OpenID Federation nicht nur für OIDC

THE TOPOLOGIES OF TRUST INFRASTRUCTURES

Flat vs. Decentralized and Hierarchical





Quelle: Guiseppe De Marco, 18th FIM4R Workshop, 30.1.2024 Copenhagen

TODO: Standardisierung der Claims

- Standardisierung von OIDC-claims für den Bereich Forschung und Bildung ist noch nicht abgeschlossen
  - eduPerson, SCHAC, voPerson etc. auch für OIDC
  - Kein urn:oid, sondern Registrierung bei IANA
  - Spezifikation von Scopes

- Best Practice Empfehlungen der AARC Community sind in Arbeit
  - https://aarc-community.org/guidelines/#upcoming (AARC-G028)
  - Research and Education Profile for OpenID Connect

TODO: Föderation DFN-AAI

- Hoffen, dass Spezifikation bald verabschiedet wird…
- Aufbau Testbed
  - Signaturservice -> Metadatenverwaltung
  - Web Services
    - Publikation von Entity Statements
    - Federation Endpoints (fetch, resolve, list, etc.)
  - Definition der technischen Metadata Policies
- Testpartner für Intermediates
  - lokale Metadaten
  - ???

Vielen Dank! Fragen? Kommentare?

- Kontakt
  - Wolfgang Pempe, Teamleiter DFN-AAI

    E-Mail: pempe@dfn.de
    Tel.: +49-30-884299-308
    Fax: +49-30-884299-370

    Adresse:
    DFN-Verein, Geschäftsstelle
    Alexanderplatz 1
    D-10178 Berlin

Ressourcen zu OpenID Federation

- Spezifikation
  - https://openid.net/specs/openid-federation-1_0.html
- Präsentationen zum letzten Stand
  - 18th FIM4R Workshop - https://indico.cern.ch/event/1325302/
  - https://indico.cern.ch/event/1325302/contributions/5720543/attachments/2790181/4866593/OpenID_Federation_1.0_for_18th_FIM4R_Workshop_at_TIIME_2024.pdf
  - https://indico.cern.ch/event/1325302/contributions/5753884/attachments/2790679/4866600/eduGAIN%20OpenID%20Federation%20POC%20-%20FIM4R%20Copenhagen%20TIIME.pdf