What can DFN-AAI provide?

Wolfgang Pempe, DFN-Verein
pempe@dfn.de

LSDMA Technical Forum / HDF AAI Kickoff
29./30. August 2017, KIT

What is DFN-AAI (1)

- **AAI** =
  Authentication and **A**uthorization **I**nfrastructure
- Underlying technology: **SAML-based Web-SSO**
- [emerging: OpenID Connect – different underlying standards, same basic principles]
- **SAML** = **S**ecurity **A**ssertion **M**arkup **L**anguage
  https://wiki.oasis-open.org/security
- **Web-SSO** = Web **S**ingle **S**ign-**O**n
  - Authenticate once for 1..n services
  - No service-specific credentials, login exclusively takes place at the Login Service (Identity Provider) of the user's Home Organization ("Privacy Preserving")

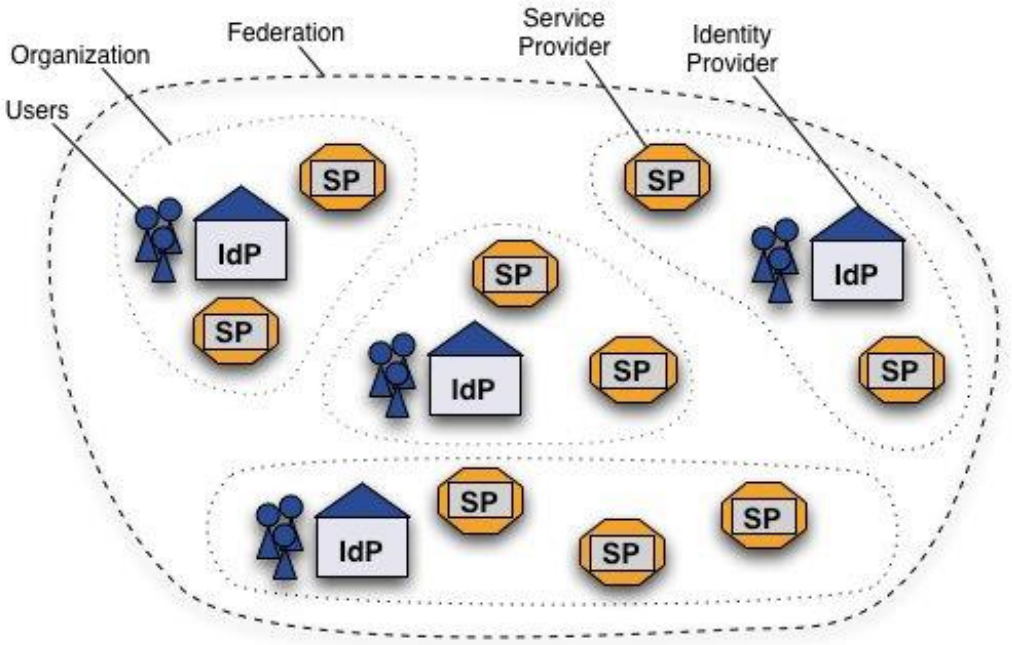
What is DFN-AAI (2)

- An **AAI** can be operated **locally** (e.g. on campus level) or **cross-institutional**, connecting multiple Home Organizations and Service Providers
- In the latter case, a central instance as **AAI operator** is needed who ensures compliance with the legal and technical framework, a trusted third party establishing mutual trust
- This kind of AAI is called **“Identity Federation”**
- **DFN-AAI** is the **Identity Federation** operated by DFN, the German NREN

What is it all about?

- Access to **services** via
  - Web-SSO
  - (Non-Web-SSO)
- Technical: **Metadata**
- Organizational: **Trust** (policies, contracts)
- **Collaboration:** locally, cross-institutional, **inter-federation (eduGAIN)**
- **Data protection** and **data minimization**, user credentials (usually username + password) are not released to any service
- **Attributes** for authorization and personalization

Federation and Metadata



(Reference: http://www.switch.ch/aai/about/federation/)

- DFN-AAI:
  - Contracts with all participants
  - (SAML) Metadata: technical backbone of a federation
  - MD are validated, updated and signed every hour
  - Certificate checks and monitoring

Numbers and Facts

- Federation Services (list incomplete)
  - Central Discovery Services (WAYF)
  - Metadata Administration Tool
  - Local Federations (usually campus-level)
  - Virtual Sub-Federations via project-/community-specific Entity Categories (e.g. bwIDM, VHB)
- DFN-AAI is 3rd or 4th biggest federation world wide
- Current numbers (2017-08-01):
  - 240 IdP, 381 SP
  - 88 local (campus-level) federations with 697 SPs (managed via DFN infrastructure and tools)
  - Connected to 36 other federations via eduGAIN

DFN-AAI: Services + User Groups

2007 → 2017

„Content Provider“ (Publishers, Databases) – Springer, Elsevier, etc.

Distribution of licensed software – Microsoft Dreamspark, Kivuto, etc.

E-Learning – Moodle, Bildungsportal Sachsen, VHB, etc.

Storage and communication services – Gigamove, WebConf…

State services – bwIDM, SaxID, Nds-AAI, …

E-Research – CLARIN, DARIAH, ELIXIR …

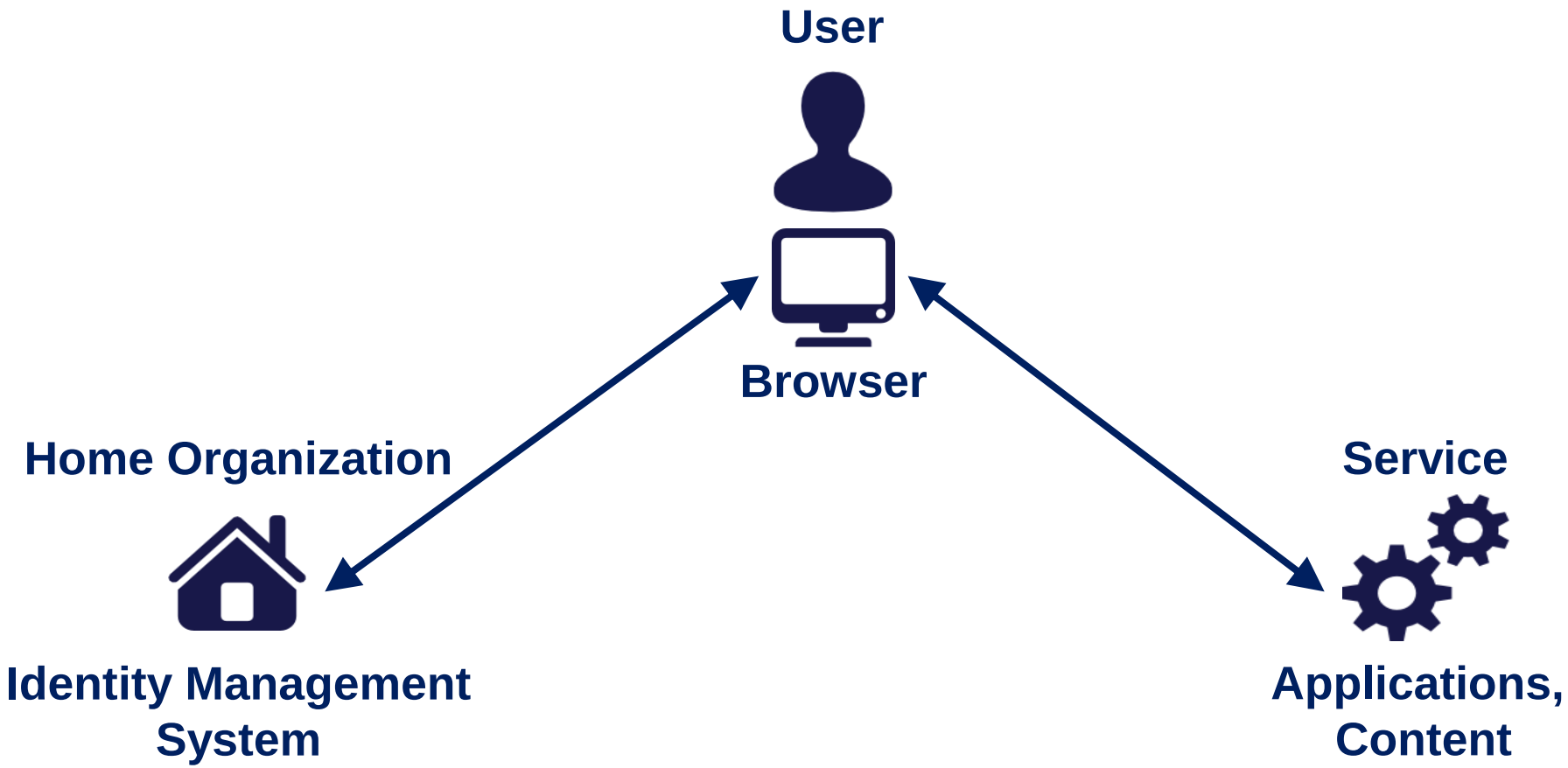
International research communities (→ eduGAIN)

Libraries, library users

Students, teaching staff

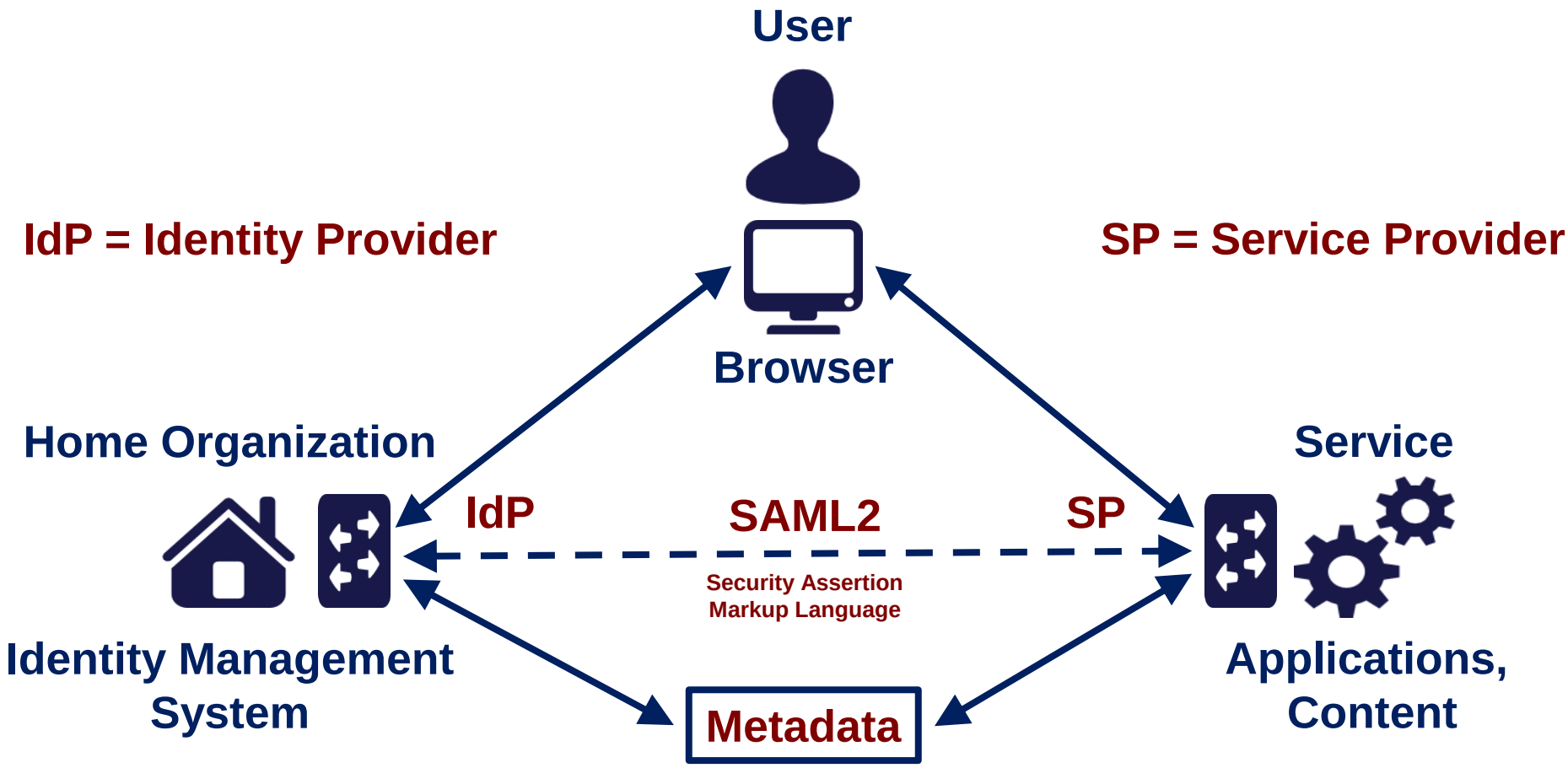
Academic staff, researchers

How does it work? (1)



Icons: http://www.visualpharm.com

How does it work? (2)



Icons: http://www.visualpharm.com

SP → IdP: AuthnRequest

- User tries to access a protected resource
- SP sends AuthnRequest to IdP (HTTP-Redirect)

```
<samlp:AuthnRequest
   AssertionConsumerServiceURL="https://loa-check.aai.dfn.de/Shibboleth.sso/SAML2/POST"
   Destination="https://testidp2.aai.dfn.de/idp/profile/SAML2/Redirect/SSO"
   ID="_ee4f0a227fb1b51f130395afe5d4688d"
   IssueInstant="2017-08-26T21:48:23Z"
   ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
   Version="2.0" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
   <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://loa-check.aai.dfn.de/shibboleth</saml:Issuer>
   <samlp:NameIDPolicy AllowCreate="1"/>
   <samlp:RequestedAuthnContext>
      <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef>
   </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

NameID Policy

Authentication Context

- User is being redirected to login page of IdP (AuthN)
- IdP issues its response to the SP … (next slide)

IdP → SP: SAML Assertion

DFN Deutsches Forschungsnetz

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="_d73b4433c963d393dec6990d59c16b6f"
  IssueInstant="2017-08-26T21:48:35.056Z" Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Issuer>https://testidp2.aai.dfn.de/idp/shibboleth</saml2:Issuer>
  <saml2:Subject>
    <saml2:NameID
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
      NameQualifier="https://testidp2.aai.dfn.de/idp/shibboleth"
      SPNameQualifier="https://loa-check.aai.dfn.de/shibboleth" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">8WLoMAAo9QFH7LmTA2GeqY1X90s=</saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml2:SubjectConfirmationData Address="194.95.228.13"
        InResponseTo="_ee4f0a227fb1b51f130395afe5d4688d"
        NotOnOrAfter="2017-08-26T21:53:35.070Z" Recipient="https://loa-check.aai.dfn.de/Shibboleth.sso/SAML2/POST"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2017-08-26T21:48:35.056Z" NotOnOrAfter="2017-08-26T21:53:35.056Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>https://loa-check.aai.dfn.de/shibboleth</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2017-08-26T21:48:34.747Z" SessionIndex="_e27034dd21a0cddfca0c88e340c6a3c6">
    <saml2:SubjectLocality Address="194.95.228.13"/>
    <saml2:AuthnContext>
      <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
    <saml2:Attribute FriendlyName="mail"
      Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml2:AttributeValue>aai@dfn.de</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="eduPersonScopedAffiliation"
      Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml2:AttributeValue>affiliate@testscope.aai.dfn.de</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="eduPersonPrincipalName"
      Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml2:AttributeValue>2fa-test@testscope.aai.dfn.de</saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>
```

NameID - Identification

Authentication Context

Attributes
- **Authorization**
- **Personalization / Identification**

DFN Levels of Assurance (1)

- Requirements on Identity Management (reliability of identities) at Home Organizations
- DFN-AAI started in 2007 with a policy approx. equivalent to today's 'Advanced'
- Not all HOs were able to meet those requirements
- As of 2009: Two so-called **Degrees of Reliance** ('Verlässlichkeitsklassen'): 'Advanced' and 'Basic'
- Technical approach: Two metadata aggregates
  - SP consume either the 'Advanced' or the 'Basic' aggregate
- New (2017): LoA expressed via Entity Attribute

DFN Levels of Assurance (2)

Degree of Reliance	Identification	Authentication (IdP of Home Org.)	Data Management + Processes for Maintaining Identities
Undefined / Test	any procedure	any procedure	any procedure
Basic	via response from a unique address (e.g. email, phone number, postal address)	authentication via unique digital address	keep user data correct and bring it up-to-date within **3 months**
Advanced	users must present themselves **in person with an official ID**, the enrolment and recruitment procedures established by the universities are considered as equivalent	authentication by means of a personal account with **user ID and password** or with a **digital certificate** which has been issued under sufficiently secure and trustworthy directives	keep user data correct and bring it up-to-date within **2 weeks**

Cf. https://wiki.aai.dfn.de/en:degrees_of_reliance

The AARC LoA Approach

Recommendations on minimal assurance level relevant for low-risk research use cases

https://aarc-project.eu/wp-content/uploads/2015/11/MNA31-Minimum-LoA-level.pdf

1. The accounts in the Home Organisations must each belong to a known individual person [DFN]
2. Persistent user identifiers (i.e., no re-assignment of user identifiers) [DFN, recommendation]
3. Documented identity vetting procedures (not necessarily face-to-face)
4. Password authentication (with some good practices)
5. Departing user's eduPersonAffiliation must change promptly (i.e. within one month) [DFN]
6. Self-assessment (supported with specific guidelines)

No known implementations yet!

REFEDS Assurance Framework (1)

- Not an official recommendation yet, but consultation is closed
  https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+Assurance+Framework
- Four orthogonal assurance components:
  1. Identifier uniqueness
  2. Identity proofing and credential issuance, renewal and replacement
  3. Authentication
  4. Attribute quality and freshness

... plus four conformance criteria …

REFEDS Assurance Framework (2)

Conformance Criteria:

1. The Identity Provider is operated with organizational-level authority
2. The Identity Provider is trusted enough to 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 site technical, admin, and security contacts, MDUI information

REFEDS Assurance Framework (3)

DFN Deutsches Forschungsnetz

Two Assurance Profiles:

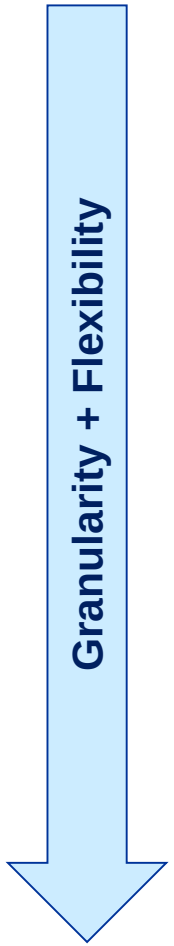
- Cappucino (lower)
- Espresso (higher)

Value	Cappuccino	Espresso
$PREFIX$/ID/unique	X	X
$PREFIX$/ID/no-eppn-reassign		
$PREFIX$/ID/eppn-reassign-1yr		
$PREFIX$/IAP/local-enterprise	X	X
$PREFIX$/IAP/assumed	X	X
$PREFIX$/IAP/verified		X
$PREFIX$/AAP/good-entropy	X	
https://refeds.org/profile/mfa		X
$PREFIX$/ATP/ePA-1m	X	X

LoA Information via SAML2

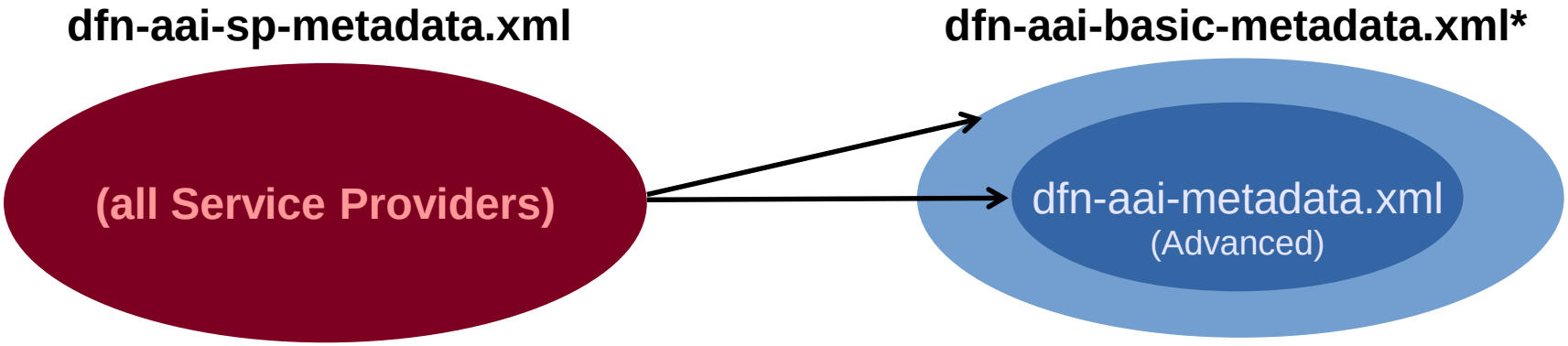
There are several ways to transport LoA-relevant information via SAML2:

1. **Different metadata sets** (IdP groups), SP has to consume the appropriate metadata set (LoA on group level)
2. **Entity Attributes/Categories** (LoA per IdP)
3. **Authentication Context Class** (LoA per identity / login)
4. **Attribute-based** (eduPersonAssurance, multi value, more than one aspect can be covered → Vectors of Trust approach) (LoA per identity / login)



LoA via SAML2 – Examples

1. Different metadata sets (cf. https://wiki.aai.dfn.de/en:metadata)



* contains **all** IdPs

2. Entity Attributes/Categories

```
<EntityDescriptor entityID="https://idp.scc.kit.edu/idp/shibboleth">
 <Extensions>
  <mdrpi:RegistrationInfo registrationAuthority="https://www.aai.dfn.de" registrationInstant="2010-03-15T10:30:11Z">
   <mdrpi:RegistrationPolicy xml:lang="en">https://www.aai.dfn.de/en/join/</mdrpi:RegistrationPolicy>
   <mdrpi:RegistrationPolicy xml:lang="de">https://www.aai.dfn.de/teilnahme/</mdrpi:RegistrationPolicy>
  </mdrpi:RegistrationInfo>
  <mdattr:EntityAttributes>
   <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:assurance-certification" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue>https://refeds.org/sirtfi</saml:AttributeValue>
   </saml:Attribute>
   <saml:Attribute Name="http://macedir.org/entity-category" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue>http://aai.dfn.de/category/bwidm-member</saml:AttributeValue>
   </saml:Attribute>
   <saml:Attribute Name="http://aai.dfn.de/loa/degree-of-reliance" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue>advanced</saml:AttributeValue>
   </saml:Attribute>
  </mdattr:EntityAttributes>
```

LoA via SAML2 – Examples

3. Authentication Context Class

```
<samlp:AuthnRequest
   AssertionConsumerServiceURL="https://loa-check.aai.dfn.de/Shibboleth.sso/SAML2/POST"
   Destination="https://testidp2.aai.dfn.de/idp/profile/SAML2/Redirect/SSO"
   ID="_ee4f0a227fb1b51f130395afe5d4688d"
   IssueInstant="2017-08-26T21:48:23Z"
   ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
   Version="2.0" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
   <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://loa-check.aai.dfn.de/shibboleth</saml:Issuer>
   <samlp:NameIDPolicy AllowCreate="1"/>
   <samlp:RequestedAuthnContext>
      <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://refeds.org/profile/mfa
</saml:AuthnContextClassRef>
   </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

LoA via SAML2 – Examples

4. Attributes: eduPersonAssurance

(cf. http://macedir.org/specs/eduperson/#eduPersonAssurance)

```
<saml2:AuthnStatement AuthnInstant="2017-08-26T21:48:34.747Z" SessionIndex="_e27034dd21a0cddfca0c88e340c6a3c6">
  <saml2:SubjectLocality Address="194.95.228.13"/>
  <saml2:AuthnContext>
    <saml2:AuthnContextClassRef>https://refeds.org/profile/mfa</saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
</saml2:AuthnStatement>
<saml2:AttributeStatement>
  <saml2:Attribute
    FriendlyName="eduPersonAssurance"
    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.11" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml2:AttributeValue>http://aai.dfn.de/loa/ID/unique</saml2:AttributeValue>
    <saml2:AttributeValue>https://refeds.org/profile/mfa</saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

Next Steps DFN-AAI

- Adopt the REFEDS Assurance Framework
  https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+Assurance+Framework
- Mapping of REFEDS assurance components to DFN's Degrees of Reliance (backwards compatibility)
- Encourage and support IdP and SP operators in implementing LoA-support based on Authentication Context Classes and eduPersonAssurance attribute
- Requires community engagement and (ideally) some use cases, i.e. really popular services that implement LoA-based authorization

LoA aspects / components

Component	DFN-AAI Degree of Reliance[1]	REFEDS Assurance Framework[2]	IGTF LoAA[3]
Identity	Identification (IA/RA)	Identifier uniqueness, identity proofing, credential issuance, renewal + replacement	Identity validation, identifier assignment, credential strength
Authentication	Authentication, acceptable credentials	Authentication context, MFA	
Attributes, user data	IDM, maintenance and attribute freshness	Attribute quality and freshness	Credential validity, management of assigned credentials
Operational practice and other aspects	[Sirtfi] [Federation policies and tools]	Conformance criteria (operations, trust, security, metadata)	(other) operational requirements, site security, publication, audits, etc.

1 https://wiki.aai.dfn.de/en:degrees_of_reliance
2 https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+Assurance+Framework
3 https://www.igtf.net/ap/authn-assurance/igtf-authn-assurance-1.1.pdf

Thoughts on Attribute Release

- Research & Scholarship Entity Category not suitable for environments where trust and higher LoAs are crucial
- Better use a community-/project-specific Entity Category that is under control of the community
  (whitelist hooked up with DFN-AAI metadata registry)
- SPs are able to generate an EC-based IdP whitelist
- IdPs can trigger attribute release based on that EC
- Examples: (cf. https://wiki.aai.dfn.de/de:entity_attributes#entity_categories)
  http://aai.dfn.de/category/bwidm-member
  http://clarin.eu/category/clarin-member
  http://aai.dfn.de/category/ndsidm-member
  http://aai.dfn.de/category/vhb-member
  http://aai.dfn.de/category/rarp-member
- Perhaps also: **`http://aai.dfn.de/category/hdf-member`** ?

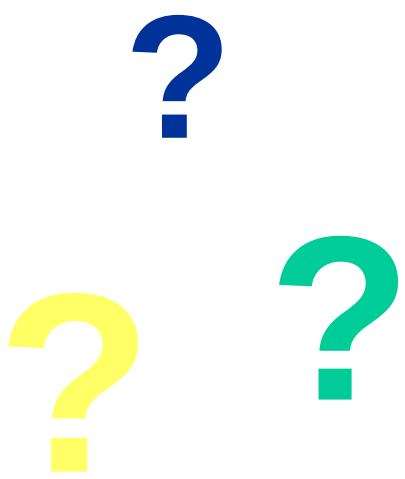
Next Steps for HDF AAI?

- Could the REFEDS Assurance Framework meet all the needs of HDF?
- If SAML-based AAI is an option, would it be necessary to implement support for IGTF-compliant values for Authentication Context Classes and/or the eduPersonAssurance attribute?
- What about OpenID Connect?
  http://openid.net/connect/
  (NB: almost the same mechanisms as in SAML, JSON instead of XML)
- What could DFN-AAI help with?

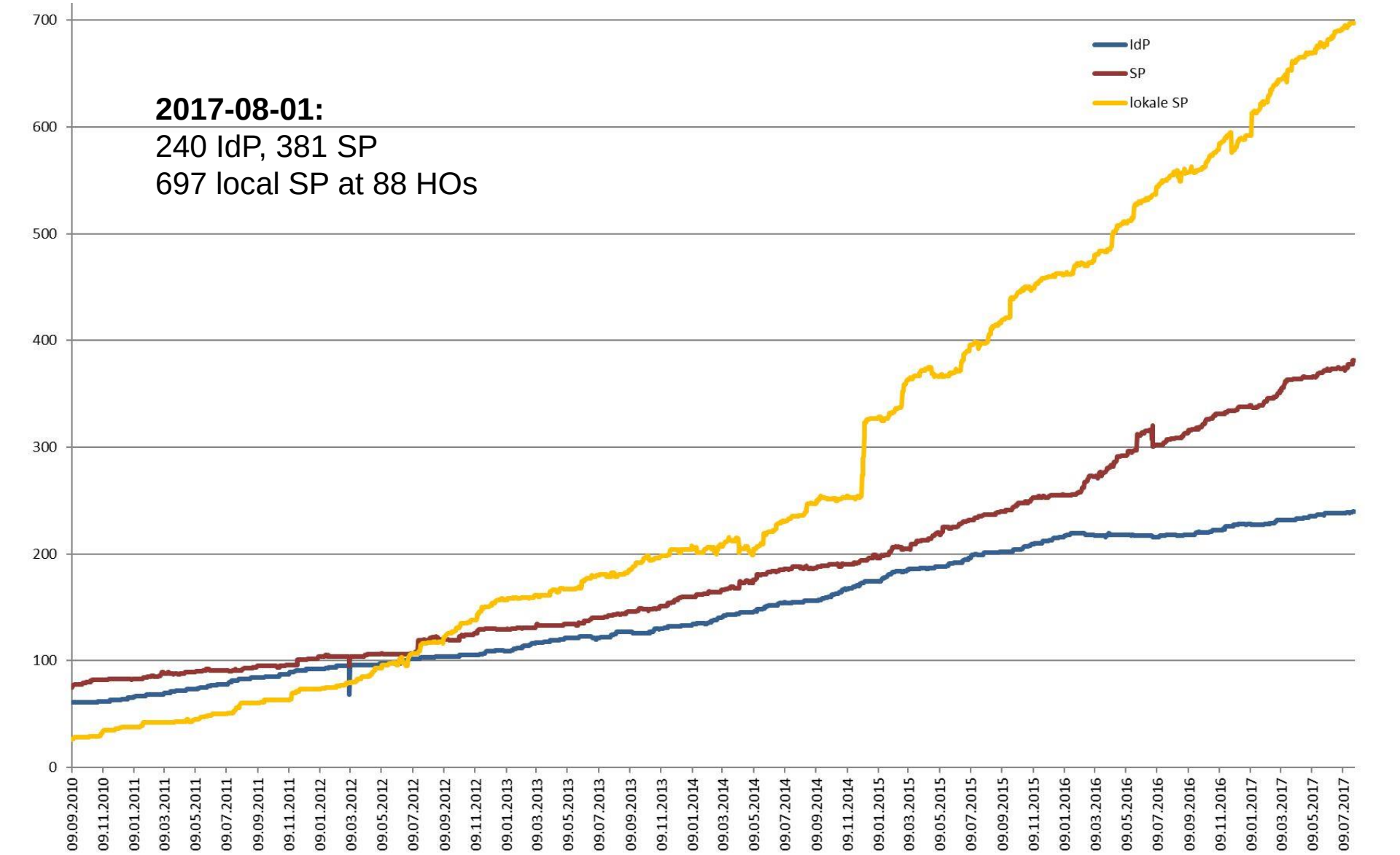
Thanks for your attention!

DFN Deutsches Forschungsnetz

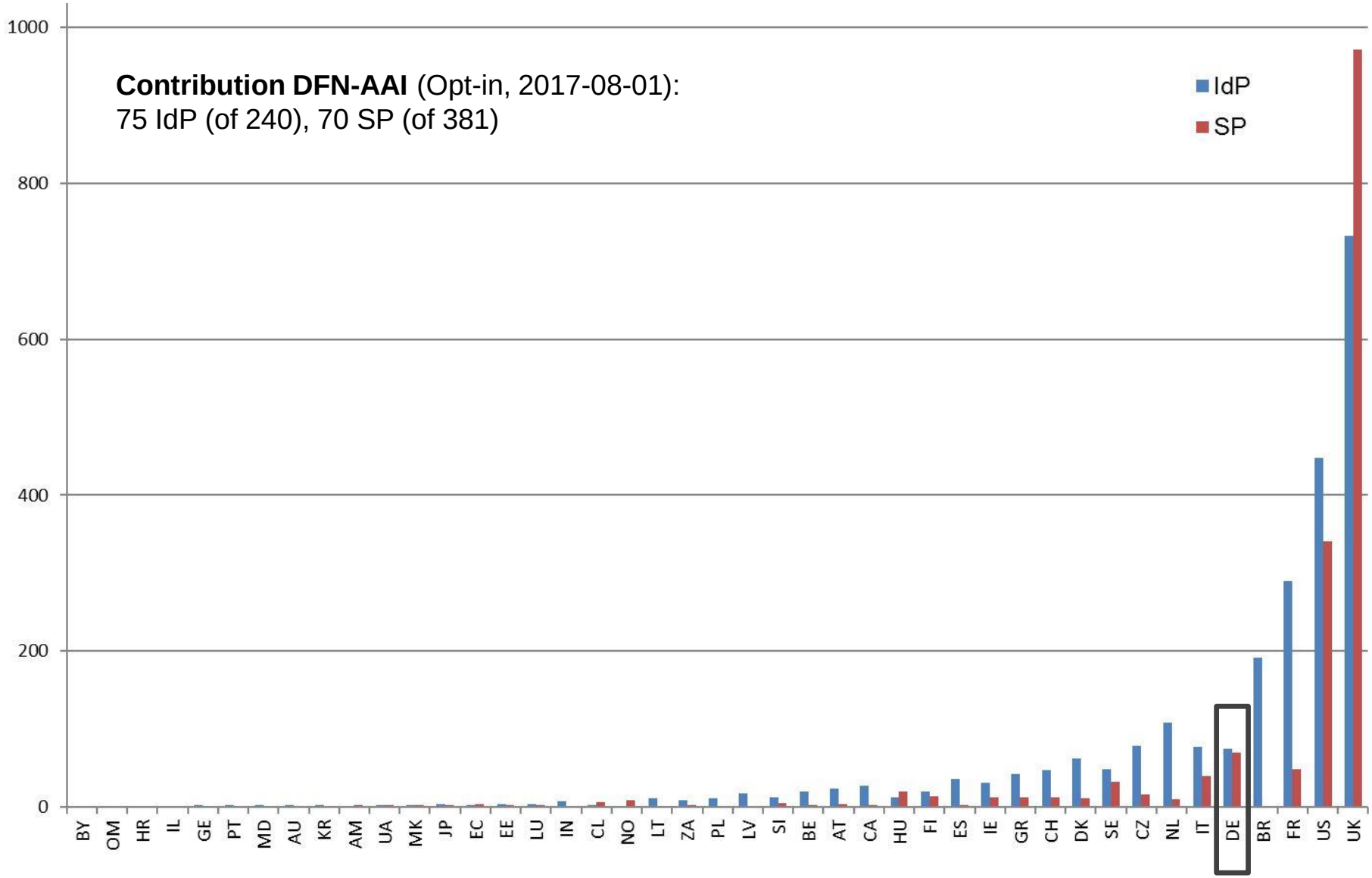
Any questions, comments, suggestions?



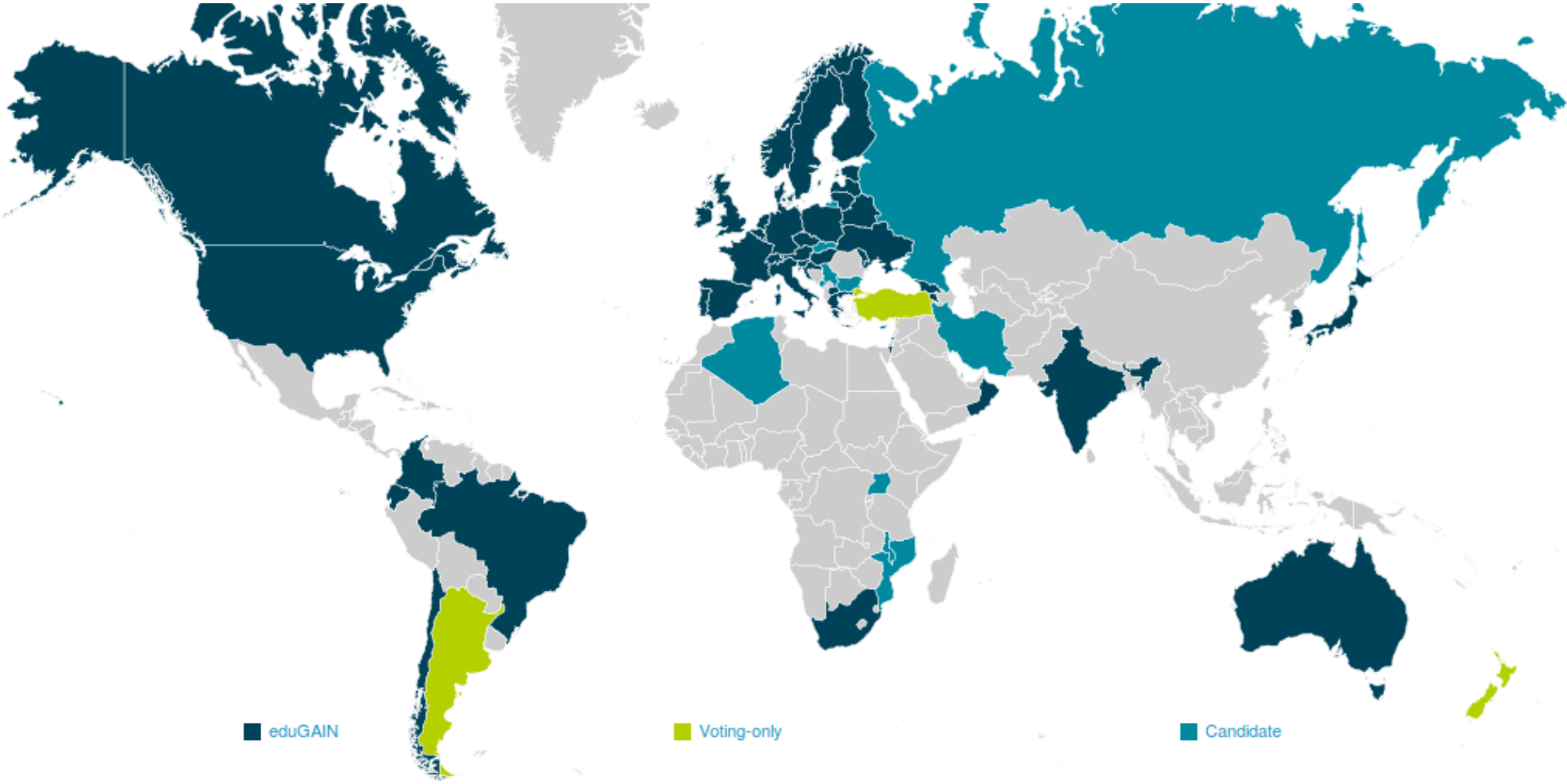
IdP and SP since 2010



eduGAIN


Contribution DFN-AAI (Opt-in, 2017-08-01):
75 IdP (of 240), 70 SP (of 381)
IdP
SP
1000
800
600
400
200
0
BY OM HR IL GE PT MD AU KR AM UA MK JP EC EE LU IN CL NO LT ZA PL LV SI BE AT CA HU FI ES IE GR CH DK SE CZ NL IT DE BR FR US UK

eduGAIN



eduGAIN: Participating Federations (Reference: https://technical.edugain.org/status)