Neues aus der DFN-AAI

Wolfgang Pempe, DFN-Verein
pempe@dfn.de

67. DFN-Betriebstagung,
26./27. September 2017, Berlin

Neuigkeiten im Überblick

- Zwei **neue Stellen** gemeinsam für DFN-AAI und eduroam ab 1. Oktober und 1. November
- **Shibboleth Consortium:** neues Support-Modell
- **Planungen für die nähere Zukunft:**
  - Unterstützung für **OpenID Connect**
  - Unterstützung für das **Metadata Query** Protocol (MDQ) als Alternative zu statischen und v.a. großen Metadaten-Dateien
  - Neue **Metadatenverwaltung** (SAML + OpenID Connect)
  - **Verlässlichkeitsklassen** nicht mehr (nur) an Metadaten-Dateien koppeln + Interoperabilität mit internationalen Standards, Self-Assessment-Tool
  - Vorbereitung auf **EU-DSGVO** → u.a. GÉANT CoCo

Shibboleth Consortium

- Erhöhung der Mitgliedsbeiträge um 25% (ab 2017)
- Änderung des Support-Modells ab 1. Dezember
  - Support seitens der Entwickler nur noch für (direkte) Mitglieder
    https://wiki.shibboleth.net/confluence/display/consort/Technical+Support+Policy+FAQ
  - Mehrwert für Mitglieder
  - Mehr Zeit für die Shibboleth-Entwickler, sich um die Weiterentwicklung + Pflege der Software zu kümmern
  - shibboleth-users Liste bleibt bestehen, Entwickler werden sich aber nur noch nach eigenem Ermessen beteiligen
- Neu: Development Blog mit monatlichem Update:
  https://wiki.shibboleth.net/confluence/pages/viewrecentblogposts.action?key=DEV
- Supportanfragen bitte an DFN-AAI Hotline

Datenschutz und CoCo Version 2

- EU-DSGVO (GDPR) tritt Mai 2018 in Kraft
- Neue Version des *GÉANT Data Protection Code of Conduct* in Arbeit, aktuelle Version und Materialien: https://wiki.refeds.org/display/CODE/Code+of+Conduct+ver+2.0+project
- Selbstverpflichtung für Service Provider, Entity Category
- Regelt auch Übertragung personenbezogener Daten in Staaten außerhalb der EU/EEA
- Best Practice Empfehlungen im Anhang (Informationspflichten, SP-Security → Sirfti, Sanktionen)
- Endgültige Version soll dem European Data Protection Board vorgelegt werden
- **Unabhängig von CoCo:** Datenschutz-Session bei AAI-Workshop im (Früh-)Sommer 2018?

Föderationsmetadaten via MDQ

- MDQ = Metadata Query Protocol
  https://datatracker.ietf.org/doc/draft-young-md-query/
  https://datatracker.ietf.org/doc/draft-young-md-query-saml/
- Ermöglicht Download signierter Metadaten pro Entity über GET-Requests
- Alternative zu immer voluminöseren Metadaten-Dateien (derzeit 4256 Entities in eduGAIN)
- Unterstützung in aktueller Shibboleth Software
  s.a. https://spaces.internet2.edu/display/perentity/MDQ+Client+Software
- Beta-Version des (Shib-)MDQ-Servers wird seit einiger Zeit von InCommon und UKAMF getestet
- Test-Installation für DFN-AAI: demnächst

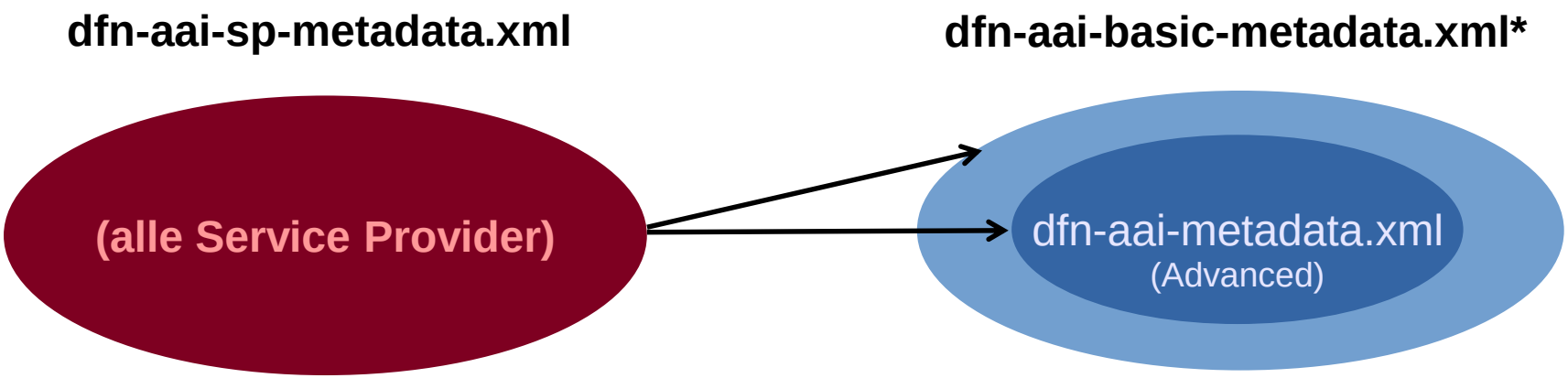
DFN-AAI Verlässlichkeitsklassen

Verlässlichkeits-klasse	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 Vertrauens-instanz 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://wiki.aai.dfn.de/de:degrees_of_reliance

Technische Umsetzung (1)

1. Getrennte Metadatensätze (s. https://wiki.aai.dfn.de/de:metadata)



* enthält **alle** IdP

	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*`

Nachteile des bisherigen Ansatzes

- Eine Verlässlichkeitsklasse / *Level of Assurance* (LoA) pro IdP → Speziallösungen (Attribute Filter Policies) für Identitäten, die nicht den Anforderungen genügen
- Verlässlichkeitsklasse = Kombination unterschiedlicher Kriterien, diese können nicht einzeln von SP adressiert werden
- Umständliches Handling der verschiedenen Metadaten-Dateien, ideal wäre eine Datei mit SP- und eine mit IdP-Metadaten (oder MDQ)

Technische Umsetzung (2)

2. Entity Attributes/Categories

seit Anfang des Jahres verfügbar, bislang nicht aktiv beworben

```
<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>
```

(https://www.aai.dfn.de/fileadmin/metadata/dfn-aai-idp-metadata.xml)

Beispiel für SP-seitigen Filter im AAI-Wiki

Levels of Assurance via SAML

Diverse Möglichkeiten, um LoA-relevante Informationen via SAML zu transportieren:

1. **Getrennte Metadatensätze** (IdP-Gruppen), SP bindet die passenden Metadaten ein (LoA auf Gruppenebene)
2. **Entity Attributes/Categories** (LoA pro IdP)
3. **Authentication Context Class** (LoA pro Identität / Login)
4. **Attribut-basiert** (eduPersonAssurance, multi value), verschiedene Aspekte unabhängig voneinander abbildbar (LoA pro Identität / Login)

Zukunftsmusik …

- Kontrolliertes LoA-Vokabular
- International
- Interoperabel
- Einzelne Kategorien bei Bedarf (← SP) kombinierbar
- …

REFEDS Assurance Framework (1)

- Noch keine offizielle Empfehlung, Konsultationsphase jedoch bereits abgeschlossen
  https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+Assurance+Framework
- Vier orthogonale *Assurance Components*:
  1. Identifier uniqueness
  2. Identity proofing and credential issuance, renewal and replacement
  3. Authentication
  4. Attribute quality and freshness

... sowie vier *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)

Zwei *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 via SAML2 – Beispiele

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 – Beispiele

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>
```

LoA – Nächste Schritte DFN-AAI

- Unterstützung des REFEDS Assurance Frameworks, Dokumentation und Teststellung, siehe einstweilen unter https://wiki.aai.dfn.de/de:common_attributes#a14
- Support für interessierte IdP- und SP-Betreiber
- Mapping Verlässlichkeitsklassen auf Assurance Profiles
- Self-Assessment Tool für die Zuordnung zu Assurance Profiles, Verlässlichkeitsklassen und Entity Attributes, z.B. Sirtfi (https://refeds.org/sirtfi) wird derzeit im Rahmen von GÉANT entwickelt und soll u.a. in der DFN-AAI zum Einsatz kommen

Vielen Dank für Ihre Aufmerksamkeit!

Fragen? Anmerkungen?

Kontakt
Internet: https://www.aai.dfn.de
E-Mail: aai@dfn.de
Telefon: +49 30 884299 9124

AAI-Zertifikate aus der DFN-PKI