Metadaten und SAML2

IdP Workshop, Teil 2

Andreas Borm , Doreen Liebenau

Metadaten als „Rückgrat der Föderation“

- Abbildung des Vertrauensverhältnisses zwischen den teiln. Organisationen
- DFN gibt stündlich signierte Metadaten heraus: Wer nimmt an AAI teil, unter welchen Adressen, mit welchen Zertifikaten?
- IdP / SP: Informationsabgleich der Informationen der Gegenseite mit den Föderationsmetadaten
- Abbruch der Kommunikation bei Nichtübereinstimmung

Metadaten bei der SAML-basierten Kommunikation(1)

- Auszug aus Metadaten am Beispiel des DFN-IdP https://idp.dfn.de/idp/shibboleth

```
<EntityDescriptor entityID="https://idp.dfn.de/idp/shibboleth">…
<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">…

<KeyDescriptor use="signing">
<ds:KeyInfo>
…
<ds:X509SubjectName>CN=idp.dfn.de</ds:X509SubjectName>
<ds:X509Certificate>
      MIIE8DCCAtigAwIBAgIUQ8ZM3aGQMOLuXsR5viqX9yE2MFowDQYJKoZIhvcNAQEL…                …
</ds:X509Certificate>
..
</KeyDescriptor>

<ArtifactResolutionService Binding=”…"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" … Location="https://idp.dfn.de/idp/profile/SAML2/POST/SSO"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST- … Location="https://idp.dfn.de/idp/profile/SAML2/POST-
SimpleSign/SSO"/>
<SingleSignOnService …
</IDPSSODescriptor>
<ContactPerson contactType="technical">
<GivenName>DFN OS Team</GivenName>
<EmailAddress>mailto:os@dfn.de</EmailAddress>
</ContactPerson>

</EntityDescriptor >
```

Entity ID

- enthalten alle für die Kommunikation benötigten Informationen
- eindeutiger Identifier: entity ID
- Datentyp: anyURI (Bsp: https://idp.dfn.de/idp/shibboleth)
- Entity ID muss nicht auf Web-Ressource verweisen bzw. dem Hostname der Entity entsprechen
- Einrichtung sollte Rechte an der Domain besitzen
- zur Einführung: SAML V.20 Metadata Guide von Oasis

Metadaten – typunabhängige Elemente

- Wurzelelement: <EntityDescriptor entityID="https://entity-xyz.de">
- Informationen für User Interfaces: <UIInfo>
- Zertifikate: <KeyDescriptor>
- Benötigte / unterstützte Name Identifier: <NameIDFormat>
- Kontaktdaten: <Organization>, <ContactPerson> (Typ: technical, administrative, support, security)

Metadaten – IdP / AA

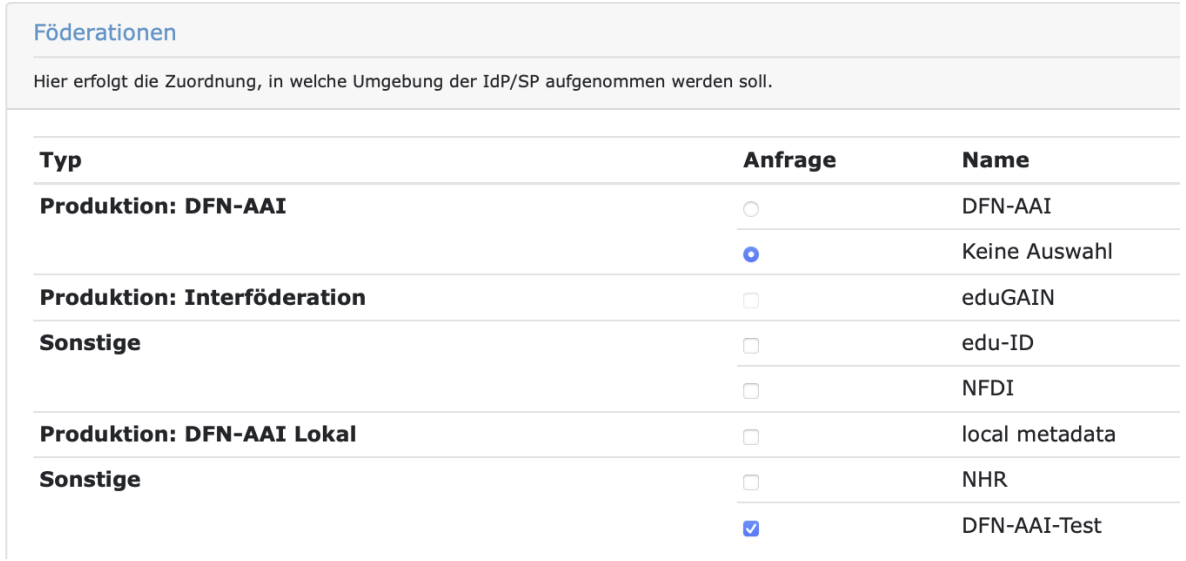
- IdP Single Sign-On Descriptor (nur IdP): <IDPSSODescriptor>
- „Scope“ (Geltungsbereich / Name der Einrichtung):
  - <saml1md:Scope regexp=“false“>**dfn.de**</saml1md:Scope>
- Bindings für SSO und SLO: <SingleSignOnService>, <SingleLogoutService>
- weitere optionale Elemente, z.B. Bindings für Attribute Queries <AttributeService> oder Attribute Authority Descriptor <AttributeAuthorityDescriptor>

Metadaten – SP

- SP Single Sign-On Descriptor: <SPSSODescriptor>
- Bindings für Entgegennahme von Assertions: <AssertionConsumerService>
- Bindings für SLO: <SingleLogoutService>
- Deklaration der vom SP benötigten Attribute: <AttributeConsumingService>

Nutzungsmöglichkeiten von Metadaten

- auf nationaler Ebene (z.B. DFN-AAI)
- „virtuelle Subföderationen“ (z.B. Bundesländer, Forschungsprojekte)
- auf lokaler Ebene (innerhalb einer Einrichtung)
- auf internationaler Ebene / Interföderation (eduGAIN)



Föderation(en) und Metadaten in der DFN-AAI

- Organisatorisch ist die DFN-AAI *eine* Identity Federation.
- Wir stellen aber *mehrere* Metadatensätze zur Verfügung:

	IdP / AA	SP
DFN-AAI-Test	dfn-aai-test-metadata.xml	
DFN-AAI	dfn-aai-sp-metadata.xml	dfn-aai-idp-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*

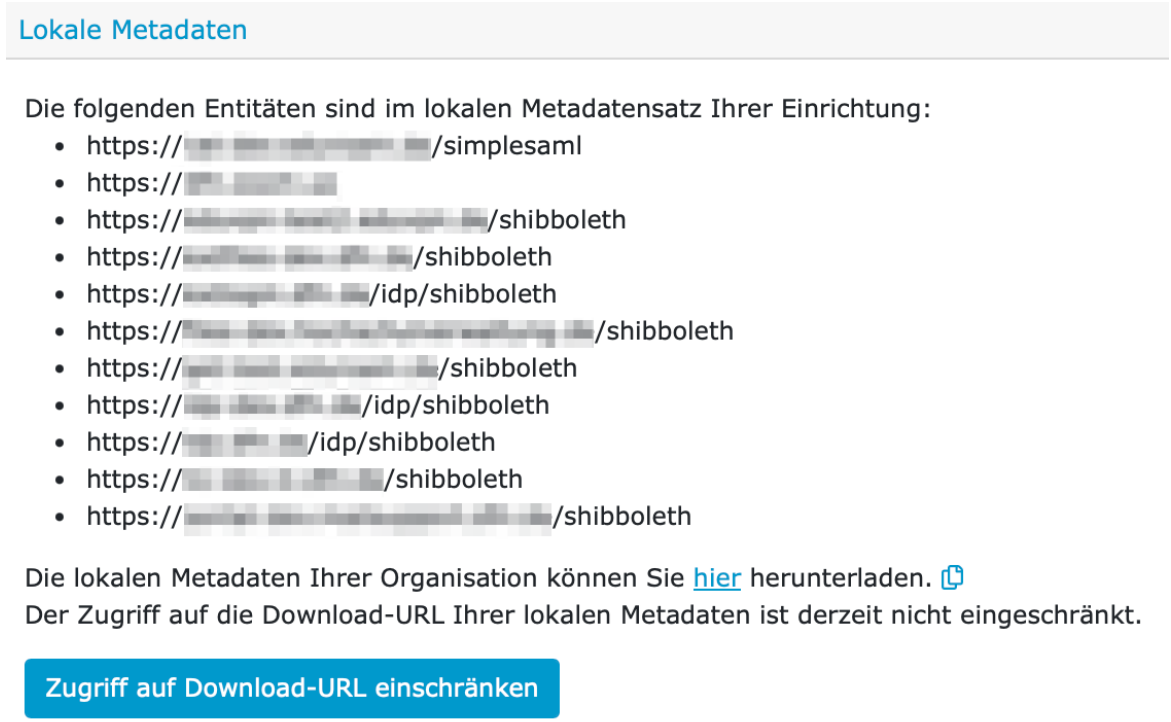
* einrichtungsspezifische Nummer statt „999“

Lokale Metadaten (= lokale Mini-Föderation)

- für Einrichtungen mit vielen lokalen/internen SPs
- einrichtungsspezifischer Metadatensatz mit IdP und internen SPs
- Auch lokale Metadatensätze werden stündlich generiert und signiert.
- bei Bedarf Zugriff nur für bestimmte IP-Bereiche
- Validierung, automatische Zertifikatsprüfungen
- Dokumentation

Konfiguration lokaler Metadaten

- Mit Aufnahme des ersten SP in die lokalen Metadaten wird der Datensatz generiert
- Metadatenverwaltung

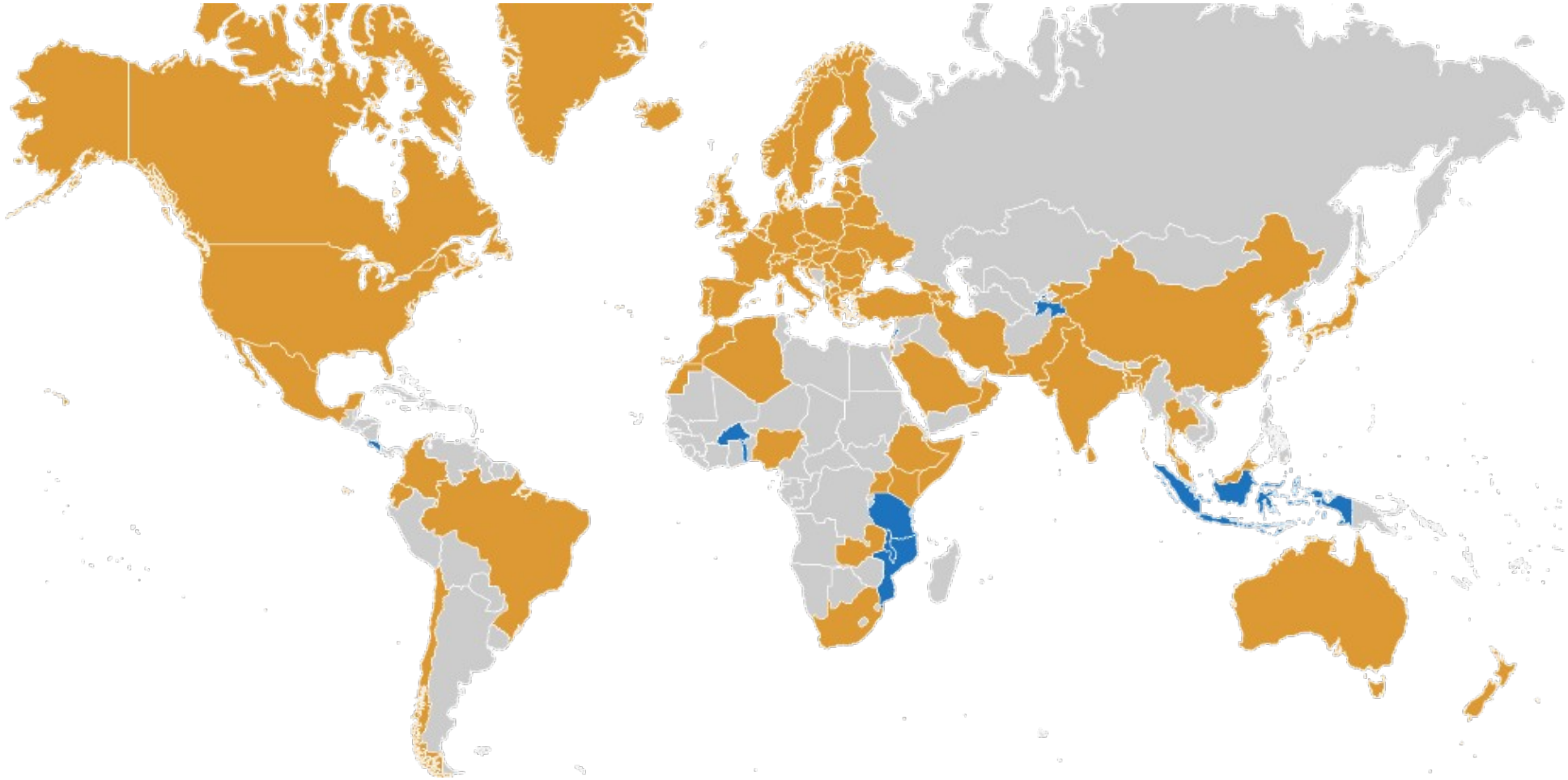


Einführung in eduGAIN

eduGAIN

- föderationsübergreifende AAI / Interföderation
- Use case: Anmeldung bei SP in anderem Land / anderer Föderation
- Betrieben von GÉANT, produktiv seit 2011
- Aggregation der Metadaten aller teilnehmenden Föderationen durch eduGAIN/GÉANT („Upstream Metadata“)
- Verteilung dieser Metadaten innerhalb der eigenen Föderation durch einzelne Föderationsbetreiber („Downstream Metadata“)

eduGAIN – beteiligte Föderationen



EduGAIN – Beteiligung in der DFN-AAI

- Teilnahme an eduGAIN ist in der DFN-AAI Opt-in
- 88% der IdPs (360/409)
- 17% der SPs (168/941)

(Stand: 22.11.2024)

EduGAIN

- Teilnehmende Föderationen https://technical.edugain.org/status
- Entities Database https://technical.edugain.org/entities
- Connectivity Check https://technical.edugain.org/eccs/