



Technische
Universität
Braunschweig

Universitätsbibliothek
Braunschweig



RDMO institutionsübergreifend mit Shibboleth nutzen

Robert Strötgen, TU Braunschweig, Universitätsbibliothek



Warum Shibboleth institutionsübergreifend?

- Single-Sign-On (SSO) für die Nutzer*innen der eigenen Einrichtung
- Anforderung für Verbundprojekte: gemeinsame Arbeit an DMP
- Login mit der Kennung der Heimat-Einrichtung möglich

Grundlagen Shibboleth in RDMO

- Gute Dokumentation (<https://rdmo.readthedocs.io/en/latest/configuration/authentication/shibboleth.html>)
- Was man braucht:
 - Shibboleth-Server-Zertifikat (über DFN-PKI, zusätzlich zu Webserver-Zertifikat)
 - Konfiguration eines Service Providers in der DFN-AAI
 - Aktuelle Shibboleth-Implementierung (libapache2-mod-shib2)
 - Konfiguration in
 - /etc/shibboleth/shibboleth2.xml,
 - /etc/apache2/sites-enabled/001-default-ssl.conf **und** /srv/rdmo/rdmo-app/config/settings/local.py

Shibboleth SP anlegen

```
<Handler type="MetadataGenerator" Location="/Metadata" signing="false">
<mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
  <mdui:DisplayName xml:lang="de">RDMO (TU Braunschweig)</mdui:DisplayName>
  <mdui:DisplayName xml:lang="en">RDMO (TU Braunschweig)</mdui:DisplayName>
  <mdui:Description xml:lang="de">RDMO ist ein Service f&#xFC;r die TU Braunschweig und kooperierende Einrichtungen zur Unterst&#xfc;tzung des Forschungsdatenmanagements - vor allem bei der Erstellung und Weiterentwicklung von Datenmanagementpl&#xE4;nen.</mdui:Description>
...
...
```

Metadatengenerator

URL <https://rdmo.biblio/etc.tu-bs.de/Shibboleth.sso/Metadata> **abfragen**

allgemeine Daten

EntityID 

Shibboleth SP anlegen

Metadatengenerator		
URL	<input type="text" value="https://rdmo.biblio/etc.tu-bs.de/Shibboleth.sso/Metadataservice"/>	<input type="button" value="abfragen"/>
allgemeine Daten		
EntityID	<input type="text" value="https://rdmo.biblio/etc.tu-braunschweig.de/shibboleth"/> CRITICAL Es gibt bereits einen Provider mit dieser EntityId	
Displayname (deutsch)	<input type="text" value="RDMO (TU Braunschweig)"/>	
Displayname (englisch)	<input type="text" value="RDMO (TU Braunschweig)"/>	
Beschreibung (deutsch)	RDMO ist ein Service für die TU Braunschweig und kooperierende Einrichtungen zur Unterstützung des Forschungsdatenmanagements – vor allem bei der Erstellung und Weiterentwicklung von Datenmanagementplänen.	
Beschreibung (englisch)	RDMO offers a tool for TU Braunschweig and cooperating institutions, which supports the research data management process. It guides the user through the creation of a data management plan (dmp).	
Information URL (deutsch)	<input type="text" value="https://rdmo.biblio/etc.tu-braunschweig.de/"/>	
Information URL (englisch)	<input type="text" value="https://rdmo.biblio/etc.tu-braunschweig.de/"/>	

Kleinere Fallstricke

- Shibboleth-Paket in Ubuntu 18.04 LTS funktioniert nicht, daher Update auf Ubuntu 18.10 ff
- Middleware-Paket muss eingebunden werden

```
MIDDLEWARE.insert(  
    MIDDLEWARE.index('django.contrib.auth.middleware.AuthenticationMiddleware') + 1,  
    'shibboleth.middleware.ShibbolethRemoteUserMiddleware'  
)
```

Besonderheiten institutionsübergreifende Authentifizierung

- Benutzername nicht uid, sondern eppn
(eduPersonPrincipalName)

- robstroe **vs.** robstroe@tu-bs.de

- Login über DFN-AAI-Discovery-Service

```
<SSO discoveryProtocol="SAMLDS"
discoveryURL="https://wayf.aai.dfn.de/DFN-AAI-Basic/wayf">
    SAML2
</SSO>
```

- DFN-AAI-Metadaten laden

```
<MetadataProvider type="XML" validate="true"
url="http://www.aai.dfn.de/fileadmin/metadata/dfn-aai-basic-metadata.xml"
backingFilePath="dfn-aai-basic-metadata.xml" maxRefreshDelay="7200">
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="2419200"/>
    <MetadataFilter type="Signature" certificate="/etc/ssl/certs/dfn-aai.g2.pem"
verifyBackup="false"/>
</MetadataProvider>
```

Fallstrick Datenschutz

- Einige IdP sind so konfiguriert, dass sie personenbezogene Daten nur dann übertragen, wenn für den SP besondere Regelungen zum Datenschutz aktiviert sind
- REFEDS Research and Scholarship Entity Category
<https://refeds.org/category/research-and-scholarship>
- GÉANT Data Protection Code of Conduct
<https://geant3plus.archive.geant.net/uri/dataprotection-code-of-conduct/v1>

Shibboleth SP anpassen

Entity-Attribute/-Kategorien	
<input checked="" type="checkbox"/> http://refeds.org/category/research-and-scholarship	
<input checked="" type="checkbox"/> https://refeds.org/sirtfi	
<p><input checked="" type="checkbox"/> REFEDS Research & Scholarship (R&S) Entity-Kategorie beantragen: The REFEDS Research and Scholarship (R&S) Entity Category is applicable to Service Providers that are operated for the purpose of supporting research and scholarship interaction, collaboration or management as an essential component. This Entity Category should not be used for access to licensed content such as e-journals.</p>	
<p><input checked="" type="checkbox"/> Bestätigen, dass die Bestimmungen des Sirtfi Frameworks eingehalten werden: The Sirtfi Entity Attribute is applicable to Identity and Service Providers that assert their compliance to the Sirtfi Framework and provide at least one valid security contact (no personal email address). For details and background information, please refer to https://wiki.refeds.org/display/SIRTFI/SIRTFI+Home.</p>	

Nutzerverwaltung

<input type="checkbox"/>	BENUTZERNAME	E-MAIL-ADRESSE	VORNAME	NACHNAME	MITARBEITER-STATUS
<input type="checkbox"/>	██████████	██████████@tum.de	██████████	██████████	✖
<input type="checkbox"/>	██████████	██████████@tum.de	██████████	██████████	✖
<input type="checkbox"/>	██████████	██████████@tu-bs.de	██████████	██████████	✖
<input type="checkbox"/>	██████████	██████████@tu-bs.de	██████████	██████████	✖

Erfahrungen / Fazit

- Shibboleth mit über DFN-AAI funktioniert
- Datenschutzkonfiguration bedenken
- RDMO an der TU Braunschweig noch im Testbetrieb
- Nachhaltigkeit und Austausch Fragebögen noch zu klären
- Daher aktuell noch wenige Nutzer*innen im Testsystem



Technische
Universität
Braunschweig

Universitätsbibliothek
Braunschweig



Fragen? Erfahrungen? Anregungen?

<https://ub.tu-braunschweig.de/>
r.stroetgen@tu-braunschweig.de