

# highmededucation-member Entity-Category

*Anleitung für Service-Provider (SPs)*

## Projekt

Im Rahmen der Arbeitsgruppe Lehre des HiGHmed-Projekts (Website) werden von verschiedenen Institutionen in Deutschland Online-Lernmodule entwickelt.

Ziel ist es, dass Lernende von allen teilnehmenden Institutionen auf die Lehrangebote der anderen Institutionen zugreifen können. Dafür sind die Lernmanagementsysteme (LMS) per Shibboleth an der DFN AAI angebunden, die Partnerstandorte werden über ihre jeweiligen Identity Provider (IdPs) authentifiziert.

In der Regel gibt ein Identity Provider eines Standorts Attribute der Nutzer nur weiter, wenn

1. der Service Provider (SP, das LMS) auch Teil der Föderation ist (DFN AAI)
2. der Nutzer der Freigabe explizit zustimmt
3. konfiguriert ist, dass dieses Attribut auch an den konkreten SP ausgeliefert werden soll.

Um Teil 3 nicht für jeden Service Provider von Institutionen des HiGHmed-Konsortiums einzeln die Konfiguration anpassen zu müssen, wurde ein minimales Set an Attributen zusammengestellt und eine Entity Category eingeführt. Durch eine Entity Category kann eine virtuelle Subföderation gebildet werden, für die z.B. gemeinsame Attributfreigaben realisiert werden können (siehe auch Dokumentation des DFN).

## Notwendige Schritte

Von Seiten der Service-Provider müssen einige Voraussetzungen erfüllt sein.

### Integration in die DFN AAI

Ihr Lernmanagementsystem (LMS) muss in die DFN AAI Föderation aufgenommen werden. Dazu ist das notwendig, dass ihr LMS Shibboleth/SAML2 fähig ist. Dies ist beispielsweise bei ILIAS (<https://lms.highmed.org/Services/AuthShibboleth/README.SHIBBOLETH.t>) oder Moodle (<https://docs.moodle.org/39/de/Shibboleth-Server>) gegeben.

## Datenschutzerklärung / Nutzungsbedingungen

Da Sie personenbezogene Daten der Teilnehmenden verarbeiten, sollten Sie beim ersten Aufruf auf die aktuell gültige Datenschutzerklärung sowie die Nutzungsbedingungen des Systems hinweisen und durch die Teilnehmenden akzeptieren lassen.

## Integration in die HiGHmededucation-Subföderation

Durch die Aufnahme in die HiGHmededucation-Subföderation sollten von den Beteiligten Standorten die entsprechenden Attribute automatisch freigebbar sein (die attribute-filter.xml der IdPs sollte einen entsprechenden Eintrag beinhalten). Dies erfordert bei der ersten Anmeldung trotzdem noch eine entsprechende explizite Freigabe durch den individuellen Nutzer auf Seiten des Identity Providers.

Hinweis: Die freigegebenen Attribute entsprechen denen, die bei der HiGHmed-Lehre Koordinationsabfrage angegeben wurden - diese finden Sie hier.

Falls Ihr Service-Provider zwingend weitere Attribute benötigt, die Sie nicht anhand vorhandener Attribute berechnen können, dann wenden Sie sich bitte an [highmededucation-shibboleth@highmed.org](mailto:highmededucation-shibboleth@highmed.org). Wir werden dann im Zweifel die Infos für IdPs aktualisieren und diese bitten, die weiteren Attribute freizugeben.

Sollte die Einrichtung mit Hilfe des Shibboleth Service Providers erfolgen (Apache mod\_shib), so kann beispielsweise so gefiltert werden, dass Anmeldungen nur von HiGHmededucation-Standorten möglich ist:

```
1      <MetadataProvider type="XML"
2          url="http://www.aai.dfn.de/fileadmin/metadata/dfn-aai-basic-metadata.xml"
3          backingFilePath="dfn-test.xml" reloadInterval="3600"
4          legacyOrgNames="true">
5          <MetadataFilter type="Signature"
6              certificate="/etc/shibboleth/dfn-aai.g2.pem"/>
7          <MetadataFilter type="Whitelist"
8              matcher="EntityAttributes">
9              <saml:Attribute
10                  Name="http://macedir.org/entity-category"
11                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
12                  <saml:AttributeValue>http://aai.dfn.de/category/highmededucat
13              </saml:Attribute>
14          </MetadataFilter>
15      </MetadataProvider>
```

## Aufnahme

Um Ihren Service-Provider zur HiGHmededucation-Föderation hinzuzufügen, schreiben Sie bitte eine Mail an [highmededucation-shibboleth@highmed.org](mailto:highmededucation-shibboleth@highmed.org) unter Angabe der folgenden Aspekte:

- Sie möchten einen Service-Provider zur HiGHmededucation-Föderation hinzufügen
- Die EntityID Ihres SPs
- Die Angabe, ob Sie alle Identity Provider der HiGHmededucation-Föderation akzeptieren (über die Entity Category, siehe Beispiel oben, empfohlen)
- Angabe, ob Datenschutzerklärung / Nutzungsbedingungen bereits vorhanden (sinnvollerweise mit Link darauf oder Kopie im Anhang; Verlinkung von HiGHmed-Seite erfolgt erst, falls diese vorhanden ist, zuvor nur zum internen Testen)

Im Anschluss wird Ihr SP zur Föderation hinzugefügt. Sie sollten in der Verwaltungskontrolle des DFN AAI eine Checkbox sehen, in der Sie die Entity Category freischalten können:

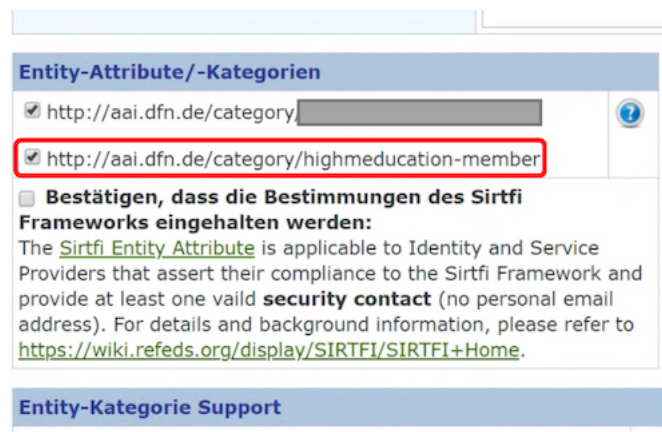


Figure 1: Screenshot 1

Innerhalb von 24 Stunden sollte dieser Eintrag dann verbreitet sein und die IdPs sollten die Attribute entsprechend freigeben. Sie können gerne eine weitere Mail an [highmededucation-shibboleth@highmed.org](mailto:highmededucation-shibboleth@highmed.org) senden, wir werden uns gerne als Testnutzer an Ihrem System anmelden.

## Anhang

Liste der aktuellen IdPs und SPs (Entity Ids)

```
1 https://sso.tu-bs.de
2 https://studip.tu-braunschweig.de
3 https://dfnaai.charite.de/idp/shibboleth
4 https://idp.helmholtz-hzi.de/idp/shibboleth
5 https://idp.hs-hannover.de/idp/shibboleth
6 https://idp.hawk.de/idp/shibboleth
7 https://shibboleth-idp.uni-wuerzburg.de/idp/shibboleth
8 https://shibboleth.mh-hannover.de/idp/shibboleth
9 https://idp.uni-heidelberg.de
10 https://idp.hs-heilbronn.de/idp/shibboleth
11 https://idp.rrz.uni-koeln.de/idp/shibboleth
12 https://zividp.uni-muenster.de/idp/shibboleth
13 https://shibboleth-idp.uni-goettingen.de/uni/shibboleth
14 https://studip-sp.uni-goettingen.de/shibboleth
```

Dieses Dokument wurde zuletzt am 2023-08-29T02:03+00:00 aktualisiert. Die PDF-Fassung dieser Dokumentation finden Sie hier: <https://highmededucation.pages.gwdg.de/metadata/highmed-sp.pdf>.