

highmededucation-member Entity-Category

Anleitung für IdP-Betreiber

Diese Dokumentation soll eine kurze Einführung über das Projekt sowie über die notwendigen Schritte geben.

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

Schritt 1: Berechtigung

Sie sollten prüfen, ob Ihr IdP bereits die Berechtigung hat, sich als Teil der Subföderation auszugeben. Die berechtigten EntityIds befinden sich am Ende dieser Anleitung. Falls dies der Fall ist, dann können Sie mit Schritt 2 fortfahren, ansonsten schreiben Sie bitte eine kurze Mail an highmededucation-shibboleth@highmed.org.

Schritt 2: Verwaltungswebsite

Sie sollten aktivieren, dass sich Ihr IdP als Teil der HiGHmed-Subföderation ausgibt.

Dafür können Sie auf der Verwaltungswebsite des DFN AAI eine entsprechende Checkbox setzen.

Dazu wählen Sie dort Ihren IdP aus und setzen die entsprechende Checkbox (siehe Screenshot):

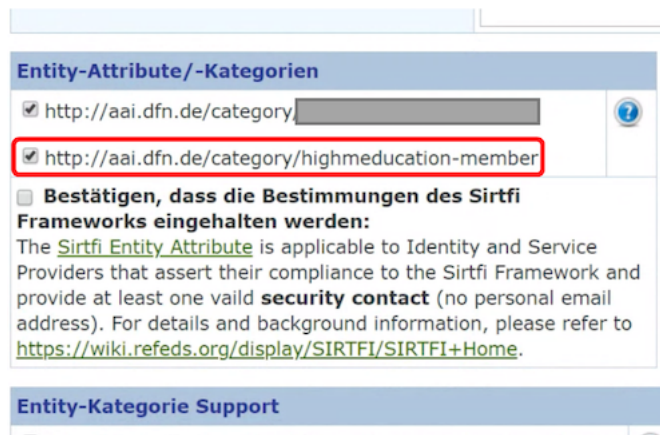


Figure 1: Screenshot 1

Schritt 3: Attributfreigabe

Im Anschluss sollten das Set von Attributen an die Teilnehmer der HiGHmededucation-Subföderation freigegeben werden.

Dies wird im folgenden Anhand einer Beispielkonfiguration von Shibboleth 3.4 dargestellt.

Die Konfiguration kann folgendermaßen gedeutet werden: Falls für ein Service Provider die Entity-Category mit dem Wert “highmededucation-member” vorhanden ist, dann wird es erlaubt, die Werte von mail, sn, givenName, ... freizugeben.

Im folgenden Beispiel ist die Benennung der attributeIDs werden nach der Konvention des DFN AAI vorgenommen (siehe hier) und muss evtl. an die eigene Konfiguration angepasst werden.

Ergänzung der `attribute-filter.xml`-Konfigurationsdatei:

```
1 <!-- HiGHmed Lehre - Freigabe an Entity Category -->
```

```

2 <AttributeFilterPolicy id="releaseAttributesToHighmededucation">
3   <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
4     attributeName="http://macedir.org/entity-category"
5     attributeValue="http://aai.dfn.de/category/highmededucation-member"/>
6   <AttributeRule attributeID="eduPersonEntitlement">
7     <PermitValueRule xsi:type="ValueRegex"
8       regex="http://highmed\.org/entitlement/.*$"/>
9   </AttributeRule>
10  <AttributeRule attributeID="persistent-id" permitAny="true"/>
11  <AttributeRule attributeID="eduPersonPrincipalName"
12    permitAny="true"/>
13  <AttributeRule attributeID="mail" permitAny="true"/>
14  <AttributeRule attributeID="surname" permitAny="true"/>
15  <AttributeRule attributeID="givenName" permitAny="true"/>
16 </AttributeFilterPolicy>

```

Schritt 4: Entitlement

Ihre Institution soll einschränken können, welche Angehörigen die HiGHmed-Service-Provider nutzen dürfen. Dafür wurde das Entitlement <http://highmed.org/entitlement/education> eingeführt, das den berechtigten Angehörigen verliehen werden soll. Der Standortverantwortliche (von HiGHmed-Seite) sollte Ihnen diese Information mitgeteilt haben.

Nach Anpassen der Konfiguration sollte die Konfiguration des IdPs entsprechend neu geladen werden.

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.pdf>.