RDB

Hinweise für die Verwendung von SAML zur Anmeldungen bei der RDB (Rechtsdatenbank) der Manz'schen Verlags- und Universitätsbuchhalndlung GmbH.

entityID

Der global eindeutige Name des Services lautet

- `https://cas.manz.at/shibboleth` (für das Produktivsystem), sowie
- `https://tst-cas.manz.at/shibboleth` (für das Testsystem).

Siehe auch Service Providers für den Servicekatalog aller eduID.at-Services, inkl. technischer Daten.

Attribute

Folgende Attribute werden laut Manz zum Funktionieren der Anwendung benötigt:

- **Eine eindeutige Kennung (unique identifier)**:
  - Persistent NameID bzw. eduPersonTargetedID, oder
  - eduPersonPrincipalName, oder
  - Matrikelnummer (d.h. schacPersonalUniqueCode-Attribut nach angegebenem Schema), oder
  - mail (E-Mail-Adresse)
- **eduPersonScopedAffiliation** zur Autorisierung laut Vertrag (siehe unten)
- Optional: eduPersonEntitlement mit dem Wert `https://rdb.manz.at/student/remote-access`

  Nur bei Institutionen, die Sonderregelungen mit Manz betreffend Fernstudierenden o.ä. getroffen haben!
- Optional: eduPersonEntitlement mit dem Wert `https://rdb.manz.at/fellow/remote-access`

  Nur bei Institutionen, die Sonderregelungen mit Manz betreffend Fellows o.ä. getroffen haben!

IP-Adressen

Manchen BenutzerInnengruppen wird laut RDB-Vertrag kein Fernzugriff ("off campus") gestattet. Daher müssen Institutionen nun jene IP-Adressbereiche, die "on campus"-Adressen repräsentieren, an Manz übermitteln, damit Manz zwischen "on campus" und "off campus" Zugriffen unterscheiden kann – soweit eine IP-Adresse darüber Auskunft erteilen kann. (So wird das ja auch bei fast allen anderen Anbietern lizensierter e-Resourcen gehandhabt, wie e-Journals oder Datenbanken, dort allerdings zum Zweck des noch einfacheren Zugangs "on campus", gänzlich ohne Anmeldung, nicht zum gänzlichen Aussperren.)
Solange für eine Institution keine solchen Adressen bei Manz vorliegen, werden potentiell alle RDB-Zugriffe scheitern!

Autorisierung und Zugriffsregeln

IP-Adress-unabhängig zugriffsberechtigt sind alle "MitarbeiterInnen", ausgedrückt über folgende SAML Attribute bzw- Attributwerte:

- `eduPersonScopedAffiliation: staff@…` oder/und `faculty@…` oder/und `employee@…`

"Studierende" nur vom institutionellen Datennetz aus (an Manz gemeldete IP-Adressbereiche, "on-campus"):

- `eduPersonScopedAffiliation: student@…`

Bei Institutionen, die mit Manz entsprechende Ausnahmeregelungen vereinbart haben (z.B. für Fernstudierende, die sich nicht/nur selten am Campus aufhalten), sind RDB-Zugriffe auch IP-Adress-unabhängig möglich, sofern auch das hier dokumentierte Entitlement geschickt wird:

- `eduPersonScopedAffiliation: student@…`
- `eduPersonEntitlement: https://rdb.manz.at/student/remote-access`

Bei Institutionen, die mit Manz entsprechende Ausnahmeregelungen vereinbart haben (z.B. für ProjektmitarbeiterInnen, die nicht formal zum Personal gehören, aber dennoch zugriffsberechtigt sind), sind RDB-Zugriffe auch IP-Adress-unabhängig möglich, sofern auch das hier dokumentierte Entitlement geschickt wird. Zusätzlich muß zum einfachen Erkennen der Institution das Attribut schacHomeOrganization übermittelt werden, mit dem Wert, der eigenen "attribute scope" (also wie in eduPersonScopedAffiliation, siehe https://eduid.at/entities/idp für eine Liste aller scopes aller IDPs in eduID.at).

- `eduPersonEntitlement: https://rdb.manz.at/fellow/remote-access`
- `schacHomeOrganization: <eigene-dns-domain-wie-in-scoped-affiliations>`

Alle anderen Affiliation- oder Entitlement-Werte (oder Kombinationen derselben) sind nicht zugriffsberechtigt.
(Fehler in dieser Dokumentation vorbehalten.)

Beispiel attribute-filter.xml für die Shibboleth IDP v3 Software

Sofern die entsprechenden Daten (über Konfiguration in `/opt/shibboleth-idp/conf/attribute-resolver.xml`) bereits prinzipiell im IDP verfügbar sind, können sie im `attribute-filter.xml` nach Bedarf freigegebenen werden.

Unter der benötigten `eduPersonScopedAffiliation` ist im untenstehenden Beispiel noch eine eindeutige Kennung zu konfigurieren, etwa durch Auskommentieren der gewünschten `AttributeRule`: Bei Verfügbarkeit empfiehlt sich eine `persistentId` bzw. `eduPersonTargetedID`, anderenfalls evtl. ein eduPersonPrincipalName-Attribut. Ist beides im eigenen IDP nicht vorhanden – was nicht gut wäre, da möglichst alle eduID.at IDPs diese liefern können sollen – könnte für Studierende auf die Matrikelnummer als speziell konstruiertes SAML-Attribut zurückgegriffen werden, wobei dann evtl *zusätzlich* noch ein anderes Attribut für MitarbeiterInnen freigegegben werden müsste (die evtl. ihrem Mitarbeiterkonto keine Matrikelnummer zugeordnet haben werden). Ist das alles nicht vorhanden, kann evtl. die E-Mail-Adresse als Kennung "missbraucht" werden, die in allen IDPs vorhanden sein sollte.

Das ganz unten erwähnte eduPersonEntitlement sollte nur von Institutionen verwendet werden, die mit Manz entsprechende Ausnahmeregeln vereinbart haben.

```
<AttributeFilterPolicy id="RDB-Manz">
    <PolicyRequirementRule xsi:type="OR">
        <Rule xsi:type="Requester" value="https://cas.manz.at/shibboleth" />
        <Rule xsi:type="Requester" value="https://tst-cas.manz.at/shibboleth" />
    </PolicyRequirementRule>

    <!-- nur jene affiliation-werte weitergeben, die autorisierte personengruppen indentifizieren -->
    <AttributeRule attributeID="eduPersonScopedAffiliation">
        <PermitValueRule xsi:type="OR">
            <Rule xsi:type="Value" value="faculty" ignoreCase="true" />
            <Rule xsi:type="Value" value="student" ignoreCase="true" />
            <Rule xsi:type="Value" value="staff" ignoreCase="true" />
            <Rule xsi:type="Value" value="employee" ignoreCase="true" />
        </PermitValueRule>
    </AttributeRule>

    <!-- eindeutige kennung: nach lokaler verfuegbarkeit "ein-/entkommentieren" -->
    <!--
    <AttributeRule attributeID="eduPersonTargetedID" permitAny="true" />
    <AttributeRule attributeID="eduPersonPrincipalName" permitAny="true" />
    <AttributeRule attributeID="matrikel" permitAny="true" />
    <AttributeRule attributeID="mail" permitAny="true" />
    -->

    <!-- NUR bei zusatzvereinbarungen mit Manz bezueglich studentischen RDB-fernzugriffen (z.B. Linzer
Rechtsstudien) -->
    <!--
    <AttributeRule attributeID="eduPersonEntitlement">
        <PermitValueRule xsi:type="Value" value="https://rdb.manz.at/student/remote-access" />
    </AttributeRule>
    -->

    <!-- NUR bei zusatzvereinbarungen mit Manz bezueglich RDB-fernzugriffen "externer MitarbeiterInnen/fellows"
-->
    <!--
    <AttributeRule attributeID="eduPersonEntitlement">
        <PermitValueRule xsi:type="Value" value="https://rdb.manz.at/fellow/remote-access" />
    </AttributeRule>
    <AttributeRule attributeID="schacHomeOrganization" permitAny="true" />
    -->
</AttributeFilterPolicy>
```