

Allgemeine Nutzungsbedingungen für die Nutzung der „IDM.nrw-CAAI“

Diese Nutzungsbedingungen gelten zwischen der RWTH Aachen, vertreten durch den Kanzler, Templergraben 55, 52062 Aachen und den Nutzenden der „Attribute Authority“.

Die Community-Verwaltung ermöglicht es, die Mitgliedschaften von Personen zu Communities und Gruppen zu verwalten und deren Community- bzw. Gruppenzugehörigkeiten an Dienste weiterzugeben, so dass die Mitglieder einer Community oder Gruppe diesen Dienst gemeinsam nutzen können. Die Community-Verwaltung besteht aus zwei Komponenten. Die eine Komponente ist die Attribute Authority, in der die Communities und die ihnen untergeordneten Gruppen verwaltet werden. Die zweite Komponente ist ein Proxy. Wenn sich ein User einen Service authentifizieren möchte, ruft der Proxy die Daten des Users bei dessen Heimateinrichtung und etwaige Community-/Gruppenzugehörigkeiten bei der Attribute Authority ab und gibt diese Daten an den Service weiter.

§ 1 Definitionen

Attribute Authority: Eine Attribute Authority ist ein Verzeichnis oder eine Datenbank, die Attribute (z. B. Gruppenzugehörigkeiten, Rollen) zu einer Identität hinzufügt, verwaltet und sicherstellt, um sie für die Attributbasierte Zugriffskontrolle (ABAC) bereitzustellen.

Admin: Innerhalb der Attribute Authority gibt es verschiedene Arten von Admins mit abgestuften Berechtigungen. Der Super-Admin, welcher der Geschäftsstelle IDM.nrw vorbehalten ist, kann Communities anlegen sowie löschen und (weitere) Community-Admins benennen. Innerhalb einer Community kann ein Community-Admin die Mitglieder der Community und Gruppen (Untereinheiten einer Community) verwalten. Er kann also Mitglieder hinzufügen und entfernen, Gruppen anlegen, diese auch wieder löschen und

Mitglieder der Community zu Gruppen hinzufügen und auch wieder aus der Gruppe entfernen. Die Verwaltung einer Gruppe kann an einen oder mehrere Gruppen-Admins delegiert werden. Diese können lediglich die Mitglieder der Gruppe verwalten, für die sie als Gruppen-Admin eingesetzt sind. Zu den Admin-Rechten gehört notwendigerweise die Berechtigung, die Daten der Mitglieder der Community oder der Gruppe einsehen zu können. Der Super-Admin hat Leserechte in allen Communities, um den Support zu ermöglichen.

Mitglieder: Mitglieder sind im Kontext der Attribute Authority User, die einer Community oder einer Gruppe angehören. Auch die oben skizzierten Community- und Gruppen-Admins sind Mitglieder der jeweiligen Community bzw. Gruppen, verfügen darüber hinaus aber noch über die entsprechenden Admin-Rechte.

Community: Im Kontext der Community-Verwaltung von IDM.nrw ist eine Community eine Gemeinschaft oder ein Verbund von Personen, die (i.d.R., aber nicht notwendigerweise) hochschulübergreifend zusammenarbeiten, also z.B. die Mitglieder eines Forschungsprojekts. In der Attribute Authority entspricht jede Community einem Mandanten. Das führt dazu, dass die Nutzer, Gruppen- bzw. Rollenmitgliedschaften, sowie Berechtigungen im Datenmodell zwischen den Communities komplett getrennt sind. (Verschiedene Mandanten – wie in diesem Fall die Communities – befinden sich zwar physisch im selben System und nutzen technisch die gemeinsame Infrastruktur, aber sie sind derart voneinander unabhängig, dass sie keinen Einblick in die Daten der anderen Mandanten haben.)

Gruppe: Eine Gruppe ist eine Untereinheit einer Community. Nur Mitglieder einer Community können Mitglied in einer ihr untergeordneten Gruppe werden, aber nicht jedes Mitglied einer Community ist automatisch auch Mitglied der Gruppen einer Community. Eine Community kann beliebig viele Gruppen als Untereinheiten haben.

User: User bzw. Nutzende sind Personen, die die Berechtigung zum Zugriff auf und zur Nutzung von Diensten erhalten haben.

Service: Ein Service oder ein Dienst ist jedes System oder jede Anwendung der Informations- und Kommunikationstechnologie, auf das bzw. die Nutzenden der Infrastruktur zugreifen können.

Heimatinrichtung: Auch Home Organization oder HO. Hierbei handelt es sich in der Regel um die den Nutzenden zugehörige Hochschule.

Service Provider (SP): Ein Service Provider ist eine Website, Anwendung oder Plattform, die Nutzenden Dienste anbietet.

Identity Provider (IdP): Ein Identity Provider ist ein System, das Identitätsinformationen für Nutzende erstellt, pflegt und verwaltet und gleichzeitig Authentifizierungsfunktionen für Dienste und SP-IdP-Proxys innerhalb der Infrastruktur bereitstellt.

Proxy: Der Proxy als Komponente der Community-Verwaltung ist ein Service Provider to Identity Provider Proxy (SP-IdP-Proxy) der zwischen Diensten und IdPs vermittelt und dabei Daten aus der Attribute Authority in den Datenaustausch zwischen IdPs und SPs einspeist.

NRW-Subföderation: Die NRW-Subföderation ist eine Föderation von IdPs und SPs innerhalb der DFN-AAI. Die Zugehörigkeit zu Subföderation wird über die Metadaten kommuniziert und die Mitglieder der Subföderation geben sich wechselseitig bestimmte Attribute automatisch frei.

§ 2 Nutzungsberechtigung

Nutzungsberechtigt sind alle Personen, deren Heimateinrichtungen Mitglied in der DFN-AAI und in der NRW-Subföderation sind. In begründeten Fällen kann von der zweiten Bedingung abgewichen werden. Der Anschluss von IdPs und SPs, die nicht Mitglied in der NRW-Subföderation sind, bedarf der individuellen Prüfung. Nutzungsberechtigte Personen müssen sich mittels SSO authentifizieren können und ihre Heimateinrichtung muss die angeforderten Attribute übermitteln.

§ 3 Zugang

Die Verwaltung der eigenen Mitgliedschaften in der Attribute Authority (oder im Falle von Admins die Verwaltung der Communities) erfolgt

browserbasiert. Das Frontend der Attribute Authority wird über eine Web-oberfläche aufgerufen. Der Login erfolgt via SSO. Dabei werden die Nutzendenaten vom IdP der Heimateinrichtung abgerufen. Nach dem Login wählt der User entweder eine Community, in der er bereits Mitglied ist oder tritt einer offenen Community bei oder fragt die Mitgliedschaft bei einer genehmigungspflichtigen Community an.

§ 4 Admin-Rechte & Pflichten

Jede Community braucht einen eigenen Admin. Dieser Admin ist berechtigt, die jeweilige Community zu verwalten und Untergruppen einzustellen. Sie haben außerdem die Berechtigung Mitglieder beitreten zu lassen, einzuladen und auch wieder aus der Community zu entfernen. Ebenfalls sind sie berechtigt weitere Community-Admins und Gruppenadmins zu benennen.

Der Admin ist verpflichtet, über alle ihm bekanntwerdenden personenbezogenen Daten Stillschweigen zu wahren. Er darf diese personenbezogenen Daten weder herausgeben noch anderen Dritten, die keine entsprechenden Admin-Berechtigungen haben, in irgendeiner Art und Weise zugänglich machen.

§ 5 Community

Es wird zwischen 3 verschiedenen Community Typen unterschieden:

1. Offene (open) Community: Den offenen Communities können alle in der Attribute Authority registrierten Nutzenden beitreten. Bei der Registrierung/Anmeldung werden die offenen Communities angezeigt.
2. Genehmigungspflichtige (requestable) Community: Auch die genehmigungspflichtigen Communities werden allen Nutzenden im Zuge der Registrierung oder Anmeldung angezeigt. Die Nutzenden können jedoch nicht direkt beitreten, sondern müssen eine Beitrittsanfrage stellen. Die Anfrage wird von den entsprechenden Community-Admins bearbeitet und entweder positiv oder negativ beschieden.

3. Geschlossene (closed) Community: Geschlossene Communities werden den registrierten Nutzenden nur angezeigt, wenn sie bereits Mitglied der jeweiligen Community sind. Ein Beitritt ist nur über Einladung durch entsprechende Community Admins möglich. Die Einladung wird per E-Mail mit einem TAN-Link versendet. Die Empfänger müssen dann mittels des TAN-Links aktiv beitreten.

§ 6 Haftung

Die Haftung ist unbeschränkt bei Vorsatz oder grober Fahrlässigkeit für die Verletzung von Leben, Leib oder Gesundheit.

Bei leicht fahrlässiger Verletzung einer Pflicht, die wesentlich für die Erreichung des Vertragszwecks ist (Kardinalpflicht), ist die Haftung der Höhe nach begrenzt auf den Schaden, der nach der Art des fraglichen Geschäfts vorhersehbar und typisch ist.

Die RWTH haftet nicht für missbräuchlichen Zugriff.

Die vorstehende Haftungsbeschränkung gilt auch für die persönliche Haftung der Mitarbeitenden, Vertreter*innen und Organe der RWTH.

§ 7 Sonstiges

1. Änderungen und Ergänzungen dieses Vertrages einschließlich dieses Paragraphen bedürfen der Schriftform, soweit nichts anderes bestimmt ist. Mündliche Nebenabreden bestehen nicht.
2. Allgemeine Geschäftsbedingungen der Nutzenden finden keine Anwendung.
3. Auf diesen Vertrag ist das deutsche Recht anzuwenden.
4. Erfüllungsort ist Aachen. Ausschließlicher Gerichtsstand ist Aachen, sofern jede Partei Kaufmann oder juristische Person des öffentlichen Rechts ist oder keinen allgemeinen Gerichtsstand in Deutschland hat.

5. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein, berührt dies die Gültigkeit der übrigen Bestimmungen nicht. Die Vertragsparteien werden sich bemühen, anstelle der unwirksamen Bestimmung eine wirksame zu finden, die dem wirtschaftlichen Bedeutungsgehalt der unwirksamen Bestimmung am ehesten nahekommt.