Dokument	bwIDM Federation Access Policy
Version	1.0
Letzte Änderung	31.07.2013
Status	FINAL

Inhalt

1 Glossar 2
2 Einleitung 2
3 Organisation der Föderation 4
3.1 Gremien 4
3.1.1 Strategisches Gremium 4
3.1.2 Operatives Gremium 4
4 Mitgliedschaft 4
4.1 Mitgliedschaftsvoraussetzungen 4
4.2 Bewerbungsprozess 4
4.3 Austritt aus der Föderation 5
4.4 Ausschluss aus der Föderation 5
4.5 Folgen eines Austritts 5
4.6 Auflösung der Föderation 5
5 Regeln der DFN-AAI Advanced 5
6 Gebühren 6
7 Verpflichtungen der Föderation 6
8 Verpflichtungen der Mitglieder 6
9 Verpflichtungen eines Identity Providers 7
10 Verpflichtungen eines Service Providers 7
11 Haftung und Datenschutz 8
12 Änderungen 8
13 Sonstiges 8

1 Glossar

Begriff	Beschreibung
Identity Provider (IdP)	Provider, der die Identitätsinformationen seiner Endbenutzer verwaltet.
Service Provider (SP)	Provider, der den anderen Mitgliedern der Föderation Dienste zur Verfügung stellt.
Deutsches Forschungsnetz (DFN)	Kommunikationsnetz für Wissenschaft und Forschung in Deutschland. Betrieben vom Verein zur Förderung eines deutschen Forschungsnetzes (DFN-Verein)
DFN Authentifikations- und Autorisierungs-Infrastruktur (DFN-AAI)	Authentifikations- und Autorisierungs-Infrastruktur, welche durch den DFN-Verein betrieben wird.
Endnutzer	Eine einem Identity Provider angehörige Identität einer Mitgliedseinrichtung der Föderation
Mitglied	Identity oder Service Provider einer Organisation (Einrichtung), die durch das Unterschreiben der Mitgliedschaftsvereinbarung zum Mitglied der bwIDM-Föderation geworden ist.
Verlässlichkeitsklasse „Advanced“	Untergruppierung der Mitglieder der DFN-AAI auf Grund des Schutzbedürfnisses von Ressourcen bzw. Einhaltung dieses Schutzbedürfnisses. Siehe auch https://www.aai.dfn.de/der-dienst/verlaesslichkeitsklassen/
Organisation	Eine Hochschule oder eine wissenschaftliche Einrichtung im Geschäftsbereich des Ministeriums für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK)
Strategisches Gremium	Siehe Abschnitt 3.1.1 Strategisches Gremium
Operatives Gremium	Siehe Abschnitt 3.1.2 Operatives Gremium

2 Einleitung

Die Hochschulen des Landes Baden-Württemberg stellen eine große und stetig steigende Anzahl von IT-Diensten und IT-Ressourcen für ihre Nutzer bereit. Die IT-Dienste tragen wesentlich zur Qualität und Attraktivität der baden-württembergischen Hochschulen bei. Etliche Dienstleistungen wurden und werden dabei mit Förderung durch das Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK) aufgebaut mit der Maßgabe, diese auch hochschulübergreifend zur Verfügung zu stellen. Das bedeutet, dass es nicht ausreicht, nur Mitgliedern und Angehörigen der eigenen Hochschule entsprechende Zugangsmöglichkeiten einzuräumen sondern auch denjenigen anderer Hochschulen Baden-Württembergs. Die Verwendung von Diensten für standortfremde Nutzer ist allerdings häufig nur mit größerem Aufwand und wenig komfortabel möglich: Nutzer müssen dazu oftmals für jeden Dienst und jede Ressource eigene Zugänge beantragen, was zeitintensiv und fehleranfällig ist, da die Vergabeprozeduren von den lokalen Gegebenheiten abhängen und der damit verbundene Aufwand eine hohe Hürde für den Nutzer bedeutet.

Deshalb wurde mit Unterstützung des Ministeriums für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK) ein gemeinsames föderatives Identitätsmanagement für die baden-württembergischen Hochschulen (bwIDM) konzipiert und umgesetzt.

Die Aufgabe der bwIDM-Föderation besteht darin, auf den Ebenen der Authentifikation und Autorisation Grundlagen für eine standortübergreifende Dienste-Erbringung und deren ortsunabhängige Nutzung zu schaffen und damit eine Steigerung der nationalen und internationalen Konkurrenzfähigkeit und Sichtbarkeit der baden-württembergischen Hochschulen zu unterstützen.

Die bwIDM-Föderation ermöglicht einen nahtlosen Zugriff auf über das Land verteilt angebotene Ressourcen und Dienste mit den auch lokal verwendeten Zugangsmöglichkeiten: ein Nutzer kann mit seiner üblichen Hochschulkennung aus seiner gewohnten Umgebung heraus auf die Dienste und Ressourcen anderer Hochschulen zugreifen, so als wären diese Ressourcen physisch vor Ort.

Die vorliegende Federation Access Policy (FAP) beschreibt die Föderation, indem sie Prozeduren und Regeln festlegt, die den teilnehmenden Organisationen ermöglichen, die bereitgestellten Föderationstechnologien anzubieten und/oder ihren Nutzern zur Verwendung bereit zu stellen. Sie ist Hauptbestandteil eines Policy Frameworks der bwIDM-Föderation und regelt die Zusammenarbeit zwischen den drei Hauptbeteiligten: Föderationsbetreiber, Service Providern und Identity Providern. Die FAP wird ergänzt von folgenden Policies:

Service Access Policy (SAP): In der Service Access Policy stellt der Service Provider dar, welche personenbezogenen Attribute er zur Authentifizierung und Autorisierung sowie ggf. für die Erbringung des Service benötigt (siehe Verpflichtungen eines Service Providers). Dazu bezieht er sich entweder auf die im Kernsatz spezifizierten Attribute oder stellt für weitere Attribute eine eigene Spezifikation zur Verfügung.

Service Provider Policy (SPP): In der Service Provider Policy erklärt der Service Provider, für welche Zwecke er die benötigten personenbezogenen Attribute verwendet und verarbeitet (siehe Verpflichtungen eines Service Providers). Die Service Provider Policy ist optional.

Service Acceptable Use Policy (SAUP): In der Service Acceptable Use Policy kann der Service Provider darstellen, wie der Dienst von Endbenutzern verwendet werden darf. Sie ist ebenfalls optional.

3 Organisation der Föderation

3.1 Gremien

Die Organisation der bwIDM-Föderation wird von zwei Gremien wahrgenommen: das strategische Gremium und das operative Gremium.

3.1.1 Strategisches Gremium

Das strategische Gremium wird vom MWK benannt. Es muss den Querschnitt der Mitglieder abbilden und somit die Zusammensetzung der Mitglieder möglichst repräsentativ vertreten.

Das strategische Gremium kümmert sich um die strategische Ausrichtung der Föderation. Dazu gehören die langfristige Strategie der Föderation, die Gestaltung der hier formulierten Policy, die Zusammenarbeit mit anderen Föderationen und die Weiterentwicklung der vorhandenen föderativen Services.

Das strategische Gremium wird während der Projektlaufzeit durch den Arbeitskreis der Leiter der wissenschaftlichen Rechenzentren Baden-Württembergs (ALWR) repräsentiert.

3.1.2 Operatives Gremium

Das operative Gremium wird vom strategischen Gremium eingesetzt.

Das operative Gremium erfüllt die anfallenden technischen, operationalen und sicherheitsrelevanten Aufgaben für die Föderation. Dazu gehören insbesondere die jeweiligen Aufgaben, die unter dem Abschnitt „Verpflichtungen der Föderation“ aufgeführt werden.

Das operative Gremium wird während der Projektlaufzeit durch das bwIDM-Partnerforum repräsentiert.

4 Mitgliedschaft

Um einen Identity Provider oder einen Service Provider innerhalb der bwIDM-Föderation betreiben zu können, muss die betreffende Organisation (Einrichtung) Mitglied in der bwIDM-Föderation sein.

4.1 Mitgliedschaftsvoraussetzungen

Um Mitglied in der bwIDM-Föderation zu werden, muss die Organisation eine Hochschule oder eine wissenschaftliche Einrichtung im Geschäftsbereich des Ministeriums für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK) sein (z.B. Universitäten, Hochschulen oder Landesbibliotheken).

Da die bwIDM-Föderation auf der Authentifizierungs- und Autorisierungs-Infrastruktur (AAI) des Deutschen Forschungsnetzwerkes (DFN) aufbaut, ist zusätzlich eine Mitgliedschaft in der DFN-AAI notwendig, in der die Verlässlichkeitsklasse „Advanced“ zwingend festzulegen ist. Für Identity Provider ist somit der Abschluss einer Dienstvereinbarung mit dem DFN bezüglich der DFN AAI notwendig. Service Provider müssen einen DFN-AAI Serviceprovider-Vertrag mit dem DFN abschließen. Organisationen, die sowohl als Identity Provider als auch als Service Provider an der Föderation teilnehmen möchten, benötigen beide Verträge.

4.2 Bewerbungsprozess

Die sich bewerbende Organisation muss sich mit dem zur Verfügung gestellten Aufnahmeantrag bei der Föderation bewerben. Dabei ist eine Bestätigung über die Mitgliedschaft in der DFN-AAI

Advanced zu erbringen. Das operative Gremium der Föderation entscheidet anhand der Bewerbungsunterlagen, ob der Bewerber die Voraussetzungen für eine Aufnahme erfüllt und gibt eine Empfehlung an das strategische Gremium der Föderation ab. Letzteres entscheidet daraufhin, ob der Bewerber aufgenommen wird. Das Ergebnis wird dem Bewerber schriftlich mitgeteilt. Bei Eingang eines positiven Bescheids zum Aufnahmeantrag ist die sich bewerbende Organisation in die Föderation aufgenommen.

4.3 Austritt aus der Föderation

Die Mitgliedschaft ist auf unbegrenzte Zeit gültig. Die Mitgliedschaft kann mit der Frist von einem Monat an jedem Kalendertag gekündigt werden.

Die Mitglieder besitzen ein Sonderkündigungsrecht, sollte die Föderation Entgelte einführen oder sich im Verzug befinden. Die Föderation befindet sich im Verzug, wenn sie ihren Verpflichtungen auch nicht innerhalb eines Monats nach einer ausreichenden Karenzzeit nachkommt.

4.4 Ausschluss aus der Föderation

Ein Mitglied kann aus der Föderation ausgeschlossen werden, wenn es den in dieser Policy definierten Regeln nicht folgt beziehungsweise den vereinbarten Pflichten nicht nachkommt.

Sollte das operative Gremium der Föderation von einem solchen Fehlverhalten des Mitglieds Kenntnis erhalten, kann das operative Gremium eine Mahnung aussprechen. Sollte dieser Mahnung innerhalb der vorgegeben Zeit nicht nachgegangen werden und der Grund für die Mahnung weiterhin bestehen, kann das strategische Gremium die Mitgliedschaft fristlos aufheben.

Wird die Mitgliedschaft des Mitglieds in der DFN-AAI Advanced beendet, führt dies ebenfalls zum sofortigen Ausschluss aus der bwIDM-Föderation. Eine Kündigung der Mitgliedschaft in der DFN-AAI oder der Verlust der Verlässlichkeitsklasse„Advanced“ sind dem operativen Gremium durch das Mitglied unverzüglich mitzuteilen.

4.5 Folgen eines Austritts

Ein Austritt oder Ausschluss aus der Föderation hat den sofortigen Verlust des Anspruchs, die föderative bwIDM-Infrastruktur nutzen zu können, zur Folge. Alle von der Föderation erhaltenen Dokumente, Informationen und Tools sind unverzüglich zurückzugeben. Die Föderation wird unter den verbleibenden Mitgliedern fortgeführt.

4.6 Auflösung der Föderation

Die Föderation kann durch das strategische Gremium aufgelöst werden, sollten ihr weniger als zwei Mitglieder angehören.

5 Regeln der DFN-AAI Advanced

Für Identity Provider gelten die in der Dienstvereinbarung mit dem DFN-Verein und der Verlässlichkeitsklasse „Advanced“ definierten Regeln auch für die bwIDM-Föderation entsprechend.

Für Service Provider gelten die im Anbietervertrag definierten Regeln des DFN-Vereins auch für die bwIDM-Föderation entsprechend.

Die im Rahmenvertrag mit dem DFN-Verein festgelegten Regeln gelten für alle Mitglieder der bwIDM-Föderation entsprechend.

Soweit die oben genannten Dokumente mit dem DFN vereinbart wurden, gelten diese Dokumente für die Föderation und ihre Mitglieder entsprechend und sind wesentlicher Teil dieser FAP. Die in der FAP definierten Regeln sind Spezialisierungen der Regeln aus oben genannten Dokumenten, sie ergänzen diese und gehen bei Widerspruch vor.

6 Gebühren

Für die Nutzung der bwIDM-Föderation fallen keine zusätzlichen Gebühren an. Die durch die verpflichtende Mitgliedschaft in der DFN-AAI anfallenden zusätzlichen Gebühren und Entgelte bleiben davon unberührt.

Die Abrechnung von entgeltlichen Diensten fällt nicht in den Zuständigkeitsbereich der bwIDM-Föderation und unterliegt gegebenenfalls bilateralen Abkommen zwischen den einzelnen Mitgliedern.

7 Verpflichtungen der Föderation

Die Föderation stellt technische Kompetenzen im Rahmen des operationalen Gremiums bereit. Dazu gehört die Unterstützung bei der Einrichtung der für die bwIDM benötigten Infrastruktur, eine Support-Anlaufstelle als Eskalationsmöglichkeit für den Support der Mitglieder und die für die Föderation benötigten Tools.

Die Föderation verwaltet die föderativen Metadaten in Zusammenarbeit mit dem DFN-Verein und stellt diese zur Verfügung.

Die Föderation strebt eine hohe Verfügbarkeit der von ihr angebotenen Dienste an (best-effort). Dennoch kann der Dienst durch notwendige Wartungen oder Störungen unterbrochen werden. Die Föderation informiert die Mitglieder frühestmöglich über anstehende Wartungsarbeiten oder eingetretene Störungen. Weder die bwIDM-Föderation noch ihre Gremien/Organe übernehmen für den störungsfreien Betrieb der von der Föderation angebotenen Dienste, Unterstützungsdienste, die Bereitstellung von Tools, die Verwaltung von föderativen Metadaten und sonstiger föderativer Leistungen eine Gewähr.

Ausfälle, die durch die zugrundeliegende Struktur der DFN-AAI begründet sind, fallen nicht in den Verantwortungsbereich der bwIDM-Föderation. Die Haftung der bwIDM-Föderation und ihrer Gremien, Organe und Erfüllungsgehilfen ist auf Vorsatz und grobe Fahrlässigkeit beschränkt. Die Haftung für Folgeschäden ist ausgeschlossen.

8 Verpflichtungen der Mitglieder

Jedes Mitglied muss die für seine Teilnahme an der Föderation benötigten Technologien und Lizenzen für seine komplette Mitgliedschaftsdauer bereitstellen.

Jedes Föderationsmitglied nennt jeweils mindestens eine Kontaktperson für:

- Sicherheitsvorfälle,

- den Support der Endbenutzer,
- die technische Anbindung an die Föderation.

Im Falle einer missbräuchlichen Nutzung eines Dienstes durch einen Endbenutzer sind die einzelnen Föderationsmitglieder zur Zusammenarbeit untereinander verpflichtet. Die Föderationsmitglieder verpflichten sich die zur Aufklärung benötigten Informationen auszutauschen. Der Identity Provider kann einen Endbenutzer gegebenenfalls sperren.

Die für die Föderation eingesetzten Softwarekomponenten sind immer auf dem für den Betrieb der Föderation relevanten aktuellsten Stand zu halten.

Die verwendeten föderativen Metadaten sind aktuell zu halten. Änderungen an den eigenen Metadaten sind dem operationalen Gremium schnellstmöglich mitzuteilen.

Die einzelnen Mitglieder sind dazu verpflichtet Maßnahmen zu ergreifen, damit bwIDM-bezogene Supportanfragen bearbeitet werden.

9 Verpflichtungen eines Identity Providers

Die Identity Provider erkennen an, dass ihre Endbenutzer durch die reine Mitgliedschaft in der Föderation noch keinerlei Anrecht dazu haben, die in der Föderation angebotenen Dienste zu verwenden. Die Verwendung der einzelnen Dienste kann bilaterale Verträge zwischen den Organisationen der Identity Provider und denjenigen der Service Provider voraussetzen.

Der Identity Provider stellt sicher, dass er die in der Attributspezifikation definierten Daten liefern kann. Der Identity Provider erkennt an, dass die in der Attributspezifikation definierten Daten nur den Kernsatz darstellen. Die Verwendung der einzelnen Dienste kann die Lieferung weiterer Attribute voraussetzen. Diese Attribute können der Service Access Policy des Dienstes entnommen werden.

Der Identity Provider verpflichtet sich, korrekte Informationen über seine Endbenutzer zu liefern. Die Korrektheit wird über die Attributspezifikation und die Richtlinien des DFN definiert. Für Attribute die nicht im Kernsatz definiert sind, gelten die Anforderungen des jeweiligen Service Providers (siehe Service Access Policy).

Der Identity Provider muss ausreichende Protokoll-Informationen vorhalten, um einen eventuellen Missbrauch seiner Endbenutzer aufklären zu können. Die Datenschutzbestimmungen sind einzuhalten.

Der Identity Provider muss seine Endbenutzer auf die in der Föderation geltenden Acceptable Use Policies hinweisen und sie zur Einhaltung verpflichten.

Der Identity Provider verpflichtet sich, den Benutzer über die von ihm an den Service Provider zu übermittelnden Daten in Kenntnis zu setzen.

10 Verpflichtungen eines Service Providers

Der Service Provider ist dazu verpflichtet, die von ihm zur Diensterbringung benötigten Attribute an das operative Gremium der Föderation zu melden. Änderungen an dem benötigten Attributsatz sind ebenfalls dem operativen Gremium mitzuteilen.

Der Serviceprovider versichert, dass er die personenbezogenen Daten der Endbenutzer nur zu dem in der SPP aufgeführten Zweckverwendet.

11 Haftung und Datenschutz

Die bwIDM-Mitglieder, ihre Mitarbeiter oder Beauftragten haften untereinander nur für vorsätzlich oder grob fahrlässig herbeigeführte Schäden. Eine Haftung für Folgeschäden ist ausgeschlossen.

Gegenüber dem Endbenutzer haben die teilnehmenden Einrichtungen sicherzustellen, dass eine Haftung des Service Providers und des Identity Providers im gesetzlich zulässigem Rahmen auf ein Mindestmaß beschränkt wird.

Jede teilnehmende Einrichtung ist für die Einhaltung der datenschutzrechtlichen Bestimmungen in seinem Bereich (als Service- oder Identity Provider) selbst verantwortlich.

Jede teilnehmende Einrichtung ist für die Bereitstellung der benötigten Lizenzen und Einhaltung der Lizenzbedingungen selber verantwortlich.

12 Änderungen

Änderungen an dieser Policy können durch das strategische Gremium vorgenommen werden. Die Änderungen werden den Mitgliedern in Textform zugestellt.

13 Sonstiges

Sollte eine Bestimmung dieser FAP unwirksam sein oder werden, so berührt dies weder die Wirksamkeit der übrigen Bestimmungen noch die Vereinbarung in ihrer Gesamtheit. Die Bestimmung soll rückwirkend durch eine Regelung ersetzt werden, die rechtlich zulässig ist und in ihrem Gehalt der ursprünglichen Bestimmung am nächsten kommt. Entsprechendes gilt für bestehende Regelungslücken.

Die FAP unterliegt deutschem Recht und deutscher Gerichtsbarkeit.