Zwischenbericht Föderiertes Identity Management.nrw

Zwischenbericht des Umsetzungsprojekts

Aylin Gündogan,

Gabriel Guckenbiehl und Tobias Schöttler

für das Konsortium

IDM.nrw

Stand: September 2024

gefördert durch:
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Ein Kooperationsvorhaben empfohlen durch die DIGITALE HOCHSCHULE NRW
INNOVATION DURCH KOOPERATION

gefördert durch:
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

IDM.NRW

Inhalt

Einleitung

Der vorliegende Zwischenbericht liefert einen Überblick über den Stand des Vorhabens IDM.nrw bis einschließlich September 2024 und gibt einen Ausblick bis zum voraussichtlichen Projektende.[1] Die Projektförderung wurde im Juli 2024 seitens des Ministeriums für Kultur und Wissenschaft um ein Jahr verlängert, so dass es nach derzeitigem Stand mit dem Dezember 2025 endet. Im Kontext der Verlängerung kommen auch neue Arbeitspakete hinzu; siehe dazu besonders die Kapitel 2.5 und 2.6.

Mit dem vorliegenden Zwischenbericht kommt das Konsortium der Berichtspflicht nach, die es sich im Förderantrag zusätzlich zu den ‚gesetzlichen' Berichtspflichten selbst auferlegt hat. Die Entscheidung, die Hochschulöffentlichkeit regelmäßig über den Stand des Projekts zu informieren, ist dadurch motiviert, dass das Gelingen des Vorhabens wesentlich von der Partizipation der Hochschulen und der hochschulübergreifenden IT-Dienstleistungen abhängt, was wiederum voraussetzt, dass sie transparent über den Projektstand informiert sind.

Der Zwischenbericht gliedert sich in drei Teile: Der einführende *erste Teil* liefert den Hintergrund, vor dem die im Projekt durchgeführten Maßnahmen zu sehen sind. Es wird die übergreifende Zielsetzung sowie deren Motivation für ein föderiertes Identitätsmanagement erläutert. Ausgehend von den Gelingensbedingungen des Vorhabens werden Teilziele definiert, von denen sich wiederum konkrete Maßnahmen bzw. Arbeitspakete ableiten. Vor diesem Hintergrund werden im *zweiten Teil* die laufenden, aber auch die bereits abgeschlossenen Maßnahmen konkreter beschrieben. Der abschließende *dritte Teil* liefert einen Ausblick, indem jene Handlungsfelder skizziert werden, die bis zum Projektende im Fokus stehen werden.

Konzepte und Dokumentationen, die im Zuge des Projekts entwickelt werden, stehen den NRW-Hochschulen zur Verfügung. Im Bericht sind an entsprechender Stelle Links zu diesen Dokumenten angegeben. Am Ende des Berichts findet sich eine kurze Übersicht weiterführender Dokumente und Links.

1. Hintergrund: Zielsetzung(en) und Gelingensbedingungen

Die hochschulübergreifende Kooperation gewinnt immer mehr an Bedeutung. An verschiedenen Hochschulen werden zunehmend IT-Services (z. B. Hochleistungsrechner, Gitlab, Sciebo.nrw, Forschungsdatenmanagement.nrw) angeboten, die auch grundsätzlich von Mitgliedern anderer Hochschulen und Einrichtungen genutzt werden können. Insbesondere im Rahmen der Förderungen durch die Digitalisierungsoffensive NRW entstanden und entstehen in Nordrhein-Westfalen zunehmend mehr IT-Services, die hochschulübergreifend angeboten werden. Durch die Landesstrategien, die im Kontext der Digitalen Hochschule NRW entwickelt wurden und werden, werden jene IT-Services in Zukunft systematisch gebündelt und weiter ausgebaut.

Zur Stärkung der digitalen Infrastruktur in Nordrhein-Westfalen (NRW) ist es notwendig, dass sich die Nutzung für die Nutzenden selbst wie auch für die Hochschulen möglichst einfach und nutzendenfreundlich gestaltet. Angehörige der Hochschulen in NRW sollen zukünftig schnell und unkompliziert mit ihren Heimat-Accounts auf Services anderer Hochschulen zugreifen und auf diese Art mit Kolleg*innen in NRW einfach und effizient zusammenarbeiten können. Als Lösung bietet sich ein föderiertes Identitätsmanagement an: Viele IT-Services – eine gemeinsame Struktur: IDM.nrw!

[1] Die öffentlichen Zwischenberichte von IDM.nrw werden fortlaufend fortgeschrieben, so dass jeweils die Lektüre des aktuellen Zwischenberichts ausreicht.

1.1. Warum ein föderiertes Identitätsmanagement?

Das übergreifende Ziel von IDM.nrw besteht darin, den Hochschulmitgliedern einen möglichst einfachen Zugriff auf verteilte Dienste zu erlauben – d.h. auf die Dienste, die von einer Hochschule hochschulübergreifend angeboten werden. Ein föderiertes Identitätsmanagement ist nur eine Möglichkeit, einen solchen Zugriff zu realisieren. Die gängigen Optionen sollen zwecks Konturierung des föderierten IDM im Folgenden gegenübergestellt werden. Gemeinsam ist den verschiedenen Modellen, dass die Entscheidung, welche Berechtigungen die einzelnen Nutzenden erhalten sollen, durch die jeweilige Heimateinrichtung getroffen wird, während die Dienste den einzelnen Nutzenden die Berechtigungen zuweisen. Die Modelle unterscheiden sich im Wesentlichen darin, wie die Informationen zur Identifizierung und Authentifizierung übergeben werden. Technisch werden diese Informationen durch Attribute übergeben. Diese enthalten systematisch gespeicherte Informationen zu virtuellen Identitäten wie Namen, E-Mail-Adressen und/oder Rollen. Damit wird einerseits die Authentifizierung der Nutzenden ermöglicht, andererseits ermöglichen sie die Autorisierung, indem sich von den Rollen Berechtigungen ableiten lassen, welche die Nutzenden in den jeweiligen Services haben sollen.

Fragmentarisierung – bilateral abgestimmte Individuallösungen. Via Shibboleth (und ähnlicher Technologien) kann mit der lokalen ID (Heimat-ID) auf verteilte webbasierte Services zugegriffen werden. Allerdings setzt das eine Abstimmung zwischen dem Service-Provider und den Hochschulen voraus, weil der Service und die Hochschulen dieselben Attribute und Rollen im selben Format benutzen müssen, damit die Identifizierung und Autorisierung funktioniert. Ohne gemeinsame Standards an Attributen und Rollen muss jeder einzelne Dienst mit jeder Hochschule einzeln in Abstimmung gehen und jede Hochschule muss sich mit jedem neu entstehenden Service erneut abstimmen. Ohne gemeinsame Standards besteht daher die *Gefahr der Fragmentarisierung*, indem jedes Serviceangebot eigene Attribute und Rollen verwendet und sich die dienstnehmenden Hochschulen für jeden Dienst an anderen Strukturen orientieren müssen, was wiederum mit einem entsprechenden Aufwand einhergeht. Dieses Modell skaliert nicht, da aufgrund der potentiellen *Pluralität von Schemata* bei jedem Service und bei jeder Hochschule wieder neue Abstimmungen und Implementierungen erforderlich sind. Zudem ist dieses Modell nur für webbasierte Services anwendbar. Der Zugriff auf nicht-webbasierte Services (wie etwa HPC) ist damit nicht möglich.

Rechte- und Rollenmanagement im IDM des Service-Providers. Alternativ könnte das Rechte- und Rollenmanagement für die einzelnen Dienste im IDM des Service-Providers erfolgen. Auf diese Weise wird derzeit der Zugriff auf nicht-webbasierte Dienste wie HPC ermöglicht.[2] Die Service-Provider nehmen dazu Einträge in das eigene IDM vor.

Dieses Modell ist jedoch auf Seiten der Nutzenden wie auch des Serviceanbieters mit immensem administrativem und organisatorischem Aufwand sowohl bei der Einrichtung – teilweise mittels Papieranträgen – als auch in der Pflege aufgrund der doppelten Datenhaltung verbunden. Für die Nutzenden resultiert dieser Prozess in einem zusätzlichen Account mit eigenen Zugangsdaten. Gerade aufgrund des administrativen Aufwands ist dieses Vorgehen mit steigenden Nutzendenzahlen sowie einer steigenden Anzahl hochschulübergreifender Services nicht mehr skalierbar. Denn nur die Heimatinstitutionen verfügen über Informationen, welche Berechtigungen die Nutzenden jeweils erhalten sollen. In diesem Modell werden die Rollen und Berechtigungen nicht technisch übergeben, sondern müssen außerhalb des Systems zwischen der jeweiligen Hochschule und dem jeweiligen Dienstanbieter abgestimmt werden (und bei Bedarf aktualisiert werden). Aus der doppelten Datenhaltung ergibt sich auch ein Sicherheitsrisiko, da der zusätzliche Account nicht an den Account geknüpft ist, der an der Heimatinstitution gepflegt wird. Dadurch werden Statusänderungen der Nutzenden nicht automatisch erkannt, sondern müssen händisch weitergegeben werden. Sofern die Heimatinstitution oder

[2] IDM.nrw arbeitet an einem föderierten Lösungsansatz für den Zugriff auf Nicht-Webdienste; siehe dazu das Kapitel „Technologieevaluation“.

die Nutzenden dem Dienstanbieter Änderungen nicht oder verzögert mitteilen, ist eine Nutzung des IT-Services trotz fehlender Autorisierungsgrundlage weiterhin möglich.

Die ersten beiden Modelle beschreiben die IST-Situation für den Zugriff auf webbasierte und nicht-webbasierte Services. Mit zunehmender Anzahl hochschulübergreifender Services sind diese Modelle aufgrund des hohen administrativen Aufwandes nicht mehr skalierbar. Eine Alternative dazu stellen die folgenden beiden Modelle dar.

Zentrales Identitätsmanagement. Durch ein zentrales Identitätsmanagement würde der technische Teil der Rechte- und Rollenverwaltung ausgelagert, so dass dies nicht – wie bei dem oben beschriebenen Modell – im IDM des Service-Providers erfolgt. Gegenüber der Verwaltung der Rollen und Rechte im IDM des jeweiligen Service-Providers hat dieses Modell einen Vorteil für die Nutzenden, da diese nicht für jeden Dienst einen eigenen Account, sondern nur *einen* zusätzlichen Account für alle hochschulübergreifenden Dienste benötigen, die an das zentrale IDM angeschlossen sind.

Abgesehen davon halten sich die Vorteile dieses Modells in Grenzen. Zum einen entstünden Kosten für den Betrieb eines zentralen IDM. Sofern keine gemeinsamen Standards eingeführt werden, erhöht die Fragmentarisierung bzw. die Pluralität der Schemata die Betriebskosten, wenn jeder Dienst ein eigenes Schema verwendet. Zum anderen reduzieren sich trotz des Outsourcings die Aufwände für die Hochschulen nicht wesentlich. In dem Modell wird im Grunde nur ein weiterer Akteur eingeführt, so dass der Service-Provider weitgehend von den administrativen Aufwänden befreit ist, die Hochschulen haben diese Aufwände aber weiterhin und lediglich einen anderen Ansprechpartner. Damit ist das zentrale IDM mit denselben Problemen konfrontiert wie die Verwaltung der Rollen und Rechte im IDM des Service-Providers – insbesondere mit dem Problem der doppelten Datenhaltung mit dem entsprechenden Sicherheitsrisiko – und schon wegen des immensen administrativen Aufwandes (für die analoge Abstimmung für die Authentifizierung und Autorisierung) kaum skalierbar.

Föderiertes Identitätsmanagement. Alle drei oben skizzierten Optionen weisen Schwächen auf. Das erste Modell ist nicht für Nicht-Webdienste wie HPC geeignet. Zudem wäre das Modell nur skalierbar, sofern sich alle Dienste und Hochschulen auf gemeinsame Standards einigen. Die anderen beiden Modelle sind schon aufgrund der relativ hohen Betriebskosten und des hohen administrativen Aufwands nicht skalierbar. Außerdem resultiert aus der doppelten Datenhaltung ein nicht unerhebliches Sicherheitsrisiko.

Ein föderiertes Identitätsmanagement vermeidet oder reduziert diese Probleme – unter bestimmten Bedingungen. Indem die Rollen und Berechtigungen in dem IDM der Heimateinrichtung gepflegt und an den Service-Provider übergeben werden, werden die doppelte Datenhaltung und das damit verbundene Sicherheitsrisiko vermieden. Außerdem entfallen die zusätzlichen administrativen Aufwände bei Änderungen der Berechtigungen (durch Stellenwechsel usw.) einer Person, weil diese im lokalen IDM ohnehin gepflegt werden müssen und dann automatisch an die Service-Provider übergeben werden.

Der administrative Aufwand für die Abstimmung lässt sich durch die Einführung gemeinsamer Standards reduzieren. Freilich ist die Implementierung neuer Schemata (Attribute und Rollen) in den lokalen IDMs und bei bereits laufenden Diensten mit einem initialen Aufwand verbunden. Aber dadurch werden mittelfristig Aufwände reduziert, weil nicht zwischen jedem neuen Dienst und jeder Hochschule zusätzliche Abstimmungen erforderlich sind. Alles in allem ist ein föderiertes Identitätsmanagement anders als die anderen drei Modelle skalierbar.

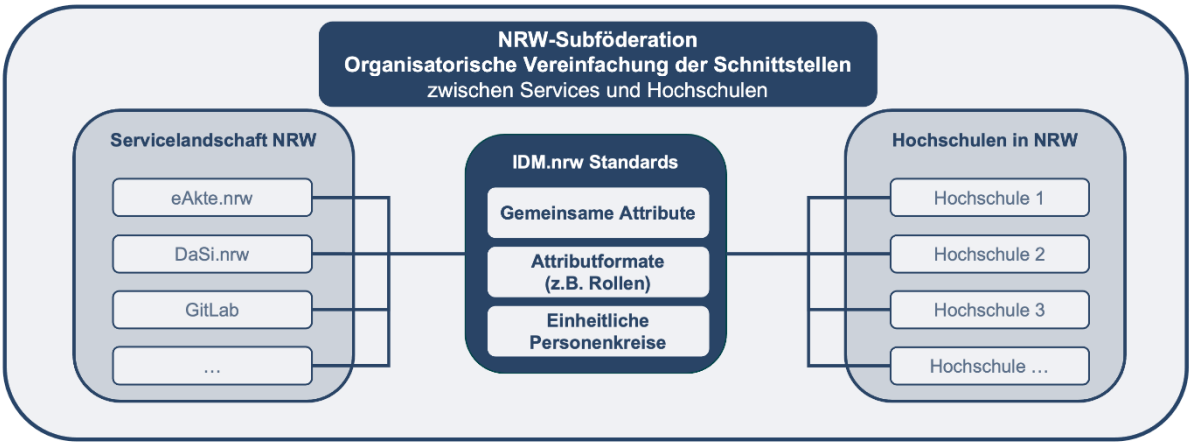

Abbildung 1: Workflow eines föderierten Identitätsmanagements

1.2. Gelingensbedingungen und Teilziele

Vor dem Hintergrund der bisherigen Ausführungen lässt sich das übergreifende Ziel von IDM.nrw folgendermaßen präzisieren: Ziel ist die Einführung eines föderierten Identity Managements für die Hochschulen, also eines Verbundes der lokalen Identitätsmanagement-Systeme (IDM-Systeme) in Nordrhein-Westfalen (NRW). So soll es den Angehörigen der Hochschulen in NRW ermöglicht werden, schnell und unkompliziert auf Services anderer Hochschulen in NRW mit ihren Heimat-Accounts zugreifen zu können. Dieses übergreifende Ziel setzt bestimmte Gelingensbedingungen voraus, wovon sich konkrete Teilziele ableiten lassen, welche wiederum die Maßnahmen definieren, welche im Projekt umgesetzt werden.

1.2.1. Konzeptionelle Gelingensbedingungen

Noch vor der Realisierung sind einige konzeptionelle Gelingensbedingungen anzusetzen.

Harmonisierung von Autorisierungsbereichen. Die Ergebnisse der Machbarkeitsstudie[3] zeigen, dass die Harmonisierung von Autorisierungsbereichen des Identitätsmanagements (gemeinsame Attribute, zentrale Personengruppen, einheitliches Rollen- und Rechtemanagement) an den einzelnen Hochschulen essenziell ist. Zurzeit verwenden die Hochschulen in NRW unterschiedliche Personenkreise (z. B. eingeschriebene Studierende, Professor*innen) als Basis für ihre Authentifizierungs- und Autorisierungsinfrastrukturen. Dabei werden teilweise gleiche Bezeichnungen für unterschiedlich definierte Kreise verwendet.

Die Skalierbarkeit eines föderierten Identitätsmanagements setzt voraus, dass man die Pluralität und Fragmentarisierung eindämmt und gemeinsame Standards einführt. Daher besteht ein wesentliches ***Teilziel*** darin, gemeinsame Standards zu entwickeln. In der ***Maßnahme*** werden gemeinsame Attribute, Rollen und zentrale Personengruppen definiert. Die Vorteile liegen auf der Hand. Sofern die IT-Dienste die entwickelten Standards verwenden, gestaltet sich die Serviceanbindung deutlich leichter. Damit ist auch der Pflegeaufwand für die Hochschulen deutlich geringer, weil sie einmal die gemeinsamen Standards implementieren müssen und diese dann einfach nutzen können, wenn sie einen neuen Dienst anschließen.[4] Die mittel- und

[3] Dem Projekt ging eine durch das MKW NRW geförderte Machbarkeitsstudie voraus. Details finden sich im Abschlussbericht: https://idm.dh.nrw/fileadmin/user_upload/idm/Abschlussbericht_Machbarkeitsstudie_IDM.pdf.

[4] Zumindest die hochschulübergreifenden IT-Services, die im Rahmen einer Förderung durch die DH.NRW entstehen, werden die gemeinsamen Standards verwenden, so dass deren Anschluss durch gemeinsame Standards erleichtert wird.

langfristigen Arbeitsersparnisse wiegen demnach den initialen Aufwand auf. Ohne gemeinsame Standards würde sich ein föderiertes IDM in der Pluralität divergierender Schemata verlieren. Ein weiterer Vorteil der Nutzung gemeinsamer Schemata besteht darin, dass dadurch eine länderübergreifende Vernetzung vereinfacht wird.

Akzeptanz der Lösungen von IDM.nrw. Ein föderiertes Identitätsmanagement lässt sich nur realisieren, wenn die Beteiligten sich auf gemeinsame Standards einigen und diese auch nutzen. Da IDM.nrw jene Standards entwickelt hat, ist die Akzeptanz dieser Standards Gelingensbedingung für ein föderiertes IDM in NRW. Ein ***Teilziel*** des Projekts ist daher darauf ausgerichtet, Akzeptanz für die vorgeschlagenen Lösungen von IDM.nrw zu schaffen. Auf dieses Ziel ist ein Teil der ***Kommunikationsmaßnahmen*** des Projekts ausgerichtet.

Bedarfsorientierung und Praxistauglichkeit. Die Konzepte werden nur angenommen, wenn sie sich an den konkreten Bedarfen orientieren und sich als praxistauglich erweisen. Um dies zu gewährleisten, ist ein ***Teilziel*** des Vorhabens darauf ausgerichtet, die dienstanbietenden Projekte einzubinden. Dazu dient die ***Maßnahme*** ‚Use Cases'. Die Zusammenarbeit mit dienstanbietenden Projekten dient mehreren Zwecken bzw. Teilzielen. Zum einen erlaubt es IDM.nrw die konkreten Bedarfe zu erfassen und die Praxistauglichkeit der Konzepte zu testen. Beispielsweise zeigte sich in der Zusammenarbeit mit Datensicherung.nrw, dass ein zusätzliches Attribut benötigt wird, was bis dahin nicht vorgesehen war. Zum anderen erfolgt im Zuge der Zusammenarbeit ein Onboarding, insofern die Projekte bei der Implementierung der gemeinsamen Standards unterstützt werden. Zum dritten können in der Zusammenarbeit mit laufenden Projekten zu hochschulübergreifenden IT-Diensten Best Practice-Lösungen entwickelt werden, die wiederum anderen Projekten zur Verfügung gestellt werden können bzw. die Grundlage für weitere Onboardings bilden.

Zukunftsfähigkeit bzw. Nachhaltigkeit. Nach und nach führen weitere Bundesländer ein föderiertes Identitätsmanagement ein. Im Zeichen der Nachhaltigkeit besteht ein ***Teilziel*** der NRW-Initiative darin, die länderübergreifende Anschlussfähigkeit der in NRW entwickelten Lösungen sicherzustellen. Als Teil seiner ***Kommunikationsmaßnahmen*** steht IDM.nrw daher mit vergleichbaren Initiativen außerhalb NRWs im Austausch.

1.2.2. Technische Gelingensbedingungen für eine dezentrale Infrastruktur

Auch wenn IDM.nrw kein zentrales Identitätsmanagement betreiben wird,[5] gibt es auch auf technischer Ebene Bedingungen, von deren Erfüllung das Gelingen des Vorhabens abhängt.

Technische Basis für die Implementierung. Als technische Grundlage für die Verwendung der gemeinsamen Standards soll eine Subföderation NRW der Authentifikation- und Autorisierungs-Infrastruktur des Deutschen Forschungsnetzes (DFN-AAI) dienen. Dadurch werden künftige Serviceanbindungen wesentlich erleichtert. Identitätsprovider werden nicht mehr mit jedem einzelnen Service individuelle Vereinbarungen treffen müssen. Vielmehr wird der Service an die NRW-Subföderation angebunden, wodurch die Nutzung der Services an den Hochschulen ermöglicht wird. Um dies zu ermöglichen, verfolgt IDM.nrw das ***Teilziel*** der Einrichtung einer Subföderation NRW. Dieses Teilziel wurde erreicht – siehe Kapitel 2.2.

Implementierungen auf Seiten der Dienste und der Hochschulen. Um den hochschulübergreifenden Zugriff auf Services zu ermöglichen, ist die technische Implementierung der NRW-Standards in bestimmten Autorisierungsbereichen des lokalen Identity Managements notwendig. Ein ***Teilziel*** von IDM.nrw ist darauf ausgerichtet, die Hochschulen darin zu unterstützen,

[5] Zu den Gründen, die gegen ein zentrales IDM sprechen, siehe Kapitel 1.1.

indem Entscheidungshilfen für die Auswahl technischer Lösungen bereitgestellt werden. Auf das Erreichen dieses Ziels ist die ***Maßnahme*** ‚Technologieevaluation' ausgerichtet.

Möglichkeit des föderierten Zugriffs auf Nicht-Webdienste. Es ist angestrebt, auch für Nicht-Webdienste (z. B. HPC) einen Zugriff mittels der Heimat-ID zu ermöglichen. Auch dies ist Gegenstand der Maßnahme ‚Technologieevaluation'.

Möglichkeit der Gruppenverwaltung. Die Berechtigung in einigen hochschulübergreifenden Services hängt auch von bestimmten (hochschulübergreifenden) Gruppenzugehörigkeiten (z. B. Mitglied in Verbänden oder bestimmten Projekten usw.) ab. Die Heimateinrichtung der einzelnen Person (als Identitätsprovider) ist aber in der Regel über derartige Gruppenzugehörigkeiten gar nicht informiert, geschweige denn, dass diese Informationen im Identitätsmanagement der Heimateinrichtung hinterlegt wären. Um also die gemeinsame Servicenutzung innerhalb von Gruppen zu ermöglichen, sind entsprechende Prozesse zur Gruppenverwaltung nötig. Dies zu ermöglichen ist ein neues ***Teilziel*** von IDM.nrw. Als ***Maßnahme*** hat das Projekt ein zusätzliches Arbeitspaket auf den Weg gebracht, das im ursprünglichen Antrag nicht vorgesehen war. Die konzeptionellen Arbeiten in dem Arbeitspaket empfehlen einen Identity Proxy zusammen mit einer Attribute Authority als Lösung. Die Empfehlung ist wesentlich dadurch motiviert, dass diese Lösung die Möglichkeit bietet, derartige Informationen zu Gruppenzugehörigkeiten einzuspeisen, während die eigentliche Nutzerverwaltung bei den Heimateinrichtungen der Personen verbleibt. (Die geplante Lösung wie auch die Gründe für diese werden etwas ausführlicher in Kapitel 2.5 behandelt.)

2. (Abgeschlossene und laufende) Maßnahmen

Zwecks Realisierung der oben ausgeführten Teilziele werden im Projekt verschiedene Maßnahmen durchgeführt. Selbstverständliche Rahmenbedingungen wie das Projektmanagement und die interne Koordination innerhalb des Konsortiums werden im Folgenden nicht eigens ausgeführt. Zur Einführung und Weiterentwicklung eines föderierten Identitätsmanagements ist eine kommunikative Schnittstelle notwendig. Daher spielt die Kommunikation im Projekt in verschiedenen Bereichen und auf verschiedenen Ebenen eine wesentliche Rolle. Die verschiedenen Kommunikationsmaßnahmen werden gebündelt dargestellt.

2.1. Entwicklung gemeinsamer Standards (abgeschlossen)

Das Gelingen eines föderierten Identitätsmanagements hängt wesentlich von der Etablierung gemeinsamer Standards ab. Viele IT-Services – eine gemeinsame Struktur: IDM.nrw! Bereits in der Machbarkeitsstudie wurden Grobkonzepte zur Harmonisierung von Autorisierungsbereichen des Identitätsmanagements (gemeinsame Attribute, zentrale Personengruppen, einheitliches Rollen- und Rechtemanagement) entwickelt. Diese wurden im Umsetzungsprojekt zu fertigen Fachkonzepten ausgearbeitet.[6] Die entsprechenden Arbeitspakete werden im Folgenden erläutert.

Zentrale Personenkreise. Ziel dieses Arbeitspakets ist die Entwicklung von einheitlichen zentralen Personenkreisen in NRW. Die Ergebnisse sollen eine Richtlinie darstellen, an der

[6] Diese konzeptionellen Grundlagen sind unabhängig von der technischen Umsetzung, legen also nicht die Wahl einer bestimmten Softwarelösung fest.

DIGITALE HOCHSCHULE NRW
INNOVATION DURCH KOOPERATION
gefördert durch:
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

sich die Hochschulen orientieren können. Bei der Erstellung wurden das Landeshochschulgesetz, das Kunsthochschulgesetz, Satzungen anderer Hochschulen und die Vorgaben bzw. Best Practices der DFN-AAI beachtet. Basierend auf den aufgeführten Gesetzen liefert IDM.nrw mit der Gruppensystematisierung die rechtlich festgelegte Definition der einzelnen Gruppen. Insgesamt wurden 66 Personenkreise herausgearbeitet. Die Gruppensystematisierung dient als Hilfestellung für Abstimmungen darüber, welche Personenkreise den eduPersonAffiliations zugeordnet werden. Es darf davon ausgegangen werden, dass verschiedene Personengruppen über ähnliche Berechtigungen verfügen, welche wiederum durch Rollen ausgedrückt werden. Dies vorausgesetzt, reduzieren sich die 66 Personengruppen auf eine überschaubare Anzahl von eduPersonAffiliations und Rollen.

Ein erster Vorschlag für einheitliche zentrale Personenkreise in NRW wurde erarbeitet und – nach Abstimmung mit der DFN-AAI in Person von Wolfgang Pempe – den Fachabteilungen der Hochschulen Anfang Juli 2022 über verschiedene Kanäle zwecks der Einholung von Feedback zugeleitet. Das eingegangene Feedback der Hochschulen wurde anschließend vom Konsortium in die Tabelle eingearbeitet und die konsolidierte Tabelle auf dem landesweiten Forum am 23. September 2022 vorgestellt.

Im Nachgang zum landesweiten Forum wurden letzte Anmerkungen eingearbeitet. Die finale Tabelle wurde in den IdM-Workshops (Technik-Treff) sowie über den ZKI-Verteiler kommuniziert und ist im Projekt-Wiki einsehbar.

***Gemeinsame Attribute*.** Die Informationen zu den virtuellen Identitäten der Nutzenden werden zwischen den Heimatorganisationen (der Identitätsprovider, in diesem Fall die Hochschulen) und den IT-Diensten durch Attribute übergeben. Die dadurch übergebenen Informationen sind die Basis für die Authentifizierung und Autorisierung der Nutzenden. Dieser Prozess setzt voraus, dass Identitätsprovider und Service-Provider gewissermaßen dieselbe Sprache sprechen; d.h. dass die von ihnen verwendeten Attribute dieselbe Struktur bzw. denselben Aufbau aufweisen. Dies betrifft insbesondere Attribute, die Berechtigungsvergaben (z. B. Rollen, Gruppen, etc.) nach sich ziehen. Bislang gibt es in NRW noch keine Einheitlichkeit in diesem Bereich. Daher ist das Ziel des Arbeitspakets, ein möglichst einheitliches Attribut-Format und ein gemeinsames Set an Basis-Attributen für NRW zu entwickeln.

Da die Empfehlungen der DFN-AAI für IDM.nrw-Zwecke nicht an allen Stellen ausreichen, hat IDM.nrw weitere Attribute entwickelt. Um die von IDM.nrw selbst entwickelten Attribute kenntlich zu machen, wurde der Vorsatz „idmNrw“ gewählt. Zu den Attributen gehört auch das eduPersonEntitlement, mit dem Rollen im IDM.nrw-Format übermittelt werden. Die zugehörigen ObjectIDs sind auf den Seiten der DFN-AAI aufgelistet.

Bislang wurden drei neue Attribute definiert, nämlich idmNrwDocumentGivenName, idmNrwDocumentSurname und idmNrwCriticalEntitlement. Die ersten beiden Attribute sollen abbilden, wie Personen auf offiziellen Dokumenten geführt werden müssen. Dies unterscheidet sich häufig in der Verwendung mehrerer Vornamen und von Namensbestandteilen, die auf ehemalige Adelsprädikate zurückführen.[7] Das dritte Attribut ist der Übergabe datenschutzrelevanter Informationen vorbehalten.

Ein erster Vorschlag eines gemeinsamen Sets an Attributen (einschließlich der neuen Attribute) wurde im Konsortium entwickelt. Auf dem ersten landesweiten Forum am 23. September 2022 wurden die Ergebnisse den Kolleg*innen der Hochschulen in NRW vorgestellt und ihr Feedback eingeholt. Im weiteren Verlauf wurden die Anmerkungen eingearbeitet. Die Attribute sind nach Abschluss des Arbeitspakets gesetzt und sollen zunächst nicht wieder verändert

[7] Das Konsortium rät von einer Nutzung des Attributs DisplayName aktiv ab, da dieser in unterschiedlichen Kontexten unterschiedlichen Bildungsregeln unterliegt. Jeder Service kann ihn sich aus den übrigen übermittelten Namensfeldern den eigenen Bedarfen entsprechend selbst konstruieren.

werden. Sie gelten als Empfehlung für die Hochschulen. Die Ergebnisse wurden in den IDM-NRW-Workshops (Technik-Treff) vorgestellt und über den ZKI-Verteiler verbreitet. Die Attributliste ist im Projektwiki hinterlegt. Dort finden sich auch weiterführende Informationen zu den gemeinsamen Attributen.

Rollen. Die Attribute stellen einen Transportweg bereit, also ein Mittel, um dem Service-Provider die erforderlichen Informationen zur Authentifizierung und Autorisierung der Nutzenden zukommen zu lassen. Die Rechte der einzelnen Nutzenden teilt der Service-Provider anhand der Rollen der jeweiligen Person zu. Die Rollen lassen sich in diesem Zusammenhang als Bündel von Funktionen betrachten, welche der jeweiligen Person in ihrer Heimateinrichtung zugewiesen werden, wovon sich wiederum Berechtigungen ableiten lassen.

Wenn jedoch ein Dienst die Berechtigungen anhand der übergebenen Rollen der Nutzenden vergeben soll, setzt dies voraus, dass sich der Service-Provider (SP) und die Identitätsprovider (IdP) auf einheitliche Rollen(-definitionen) geeinigt haben. Andernfalls setzt jeder Dienst eigene Rollendefinitionen voraus und es sind für jeden Dienst erneute Abstimmungen zwischen dem Dienst und den Hochschulen erforderlich. Ein solches Vorgehen ist offensichtlich nicht skalierbar. Gerade mit Blick auf die 66 zentralen Personengruppen (und deren uneinheitliche Verwendung an den verschiedenen Hochschulen) gilt es daher, die Vielfalt der Personenkreise einzuschränken und sich einheitlich auf Grundtermini zu einigen. Im Zuge der Harmonisierung von Autorisierungsbereichen des Identitätsmanagements hat sich IDM.nrw dieser Aufgabe angenommen.

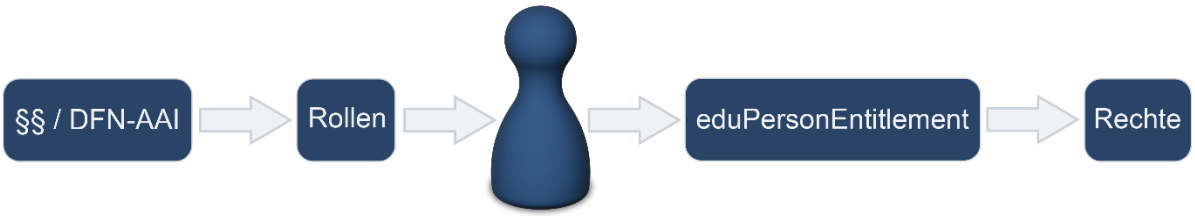

Abbildung 2: Prozess der Zuweisung von Rollen und Berechtigungen

Im Rahmen des Arbeitspakets Gemeinsame Attribute wurden daher einheitliche Rollen vom Typ eduPersonEntitlement für die Verwendung in NRW registriert. Durch den beim DFN registrierten urn-Namespace wird ein einheitliches Format für eduPersonEntitlements – also Attribute, die Berechtigungen veranlassen sollen – zur Verfügung gestellt. Die urn-Strings bilden die technische Form, mit der Rollen mit und ohne Kontext an die Dienstbetreibenden übermittelt werden können. Neben urn-strings für die Schreibrechte zum Wiki von IDM.nrw wurden bereits urn-strings für Rollen bei Datensicherung.nrw angelegt (vgl. dazu die Liste der registrierten Rollen im Wiki.) Die Nutzung von Partikularrollen wird nicht empfohlen.[8] (Eine Erläuterung der verschiedenen Strings und ihrer Einsatzmöglichkeiten findet sich im entsprechenden Wiki-Eintrag.)

Es wurde sich bewusst gegen ein Datenfeld entschieden, welches das Zielsystem enthält. So wird verhindert, dass bilaterale Absprachen zwischen IdP und SP notwendig sind. Für datenschutzrechtlich kritische Berechtigungen steht ein spezielles Attribut zur Verfügung, welches nur für bestimmte Services genutzt werden darf (idmNrwCriticalEntitlement).

[8] Eine Rolle gilt dann als Partikularrolle, wenn einer Nutzerin bzw. einem Nutzer ein einzelnes Recht in einem einzelnen Service eingeräumt wird.

DIGITALE HOCHSCHULE NRW
INNOVATION DURCH KOOPERATION
gefördert durch:
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Wir empfehlen entsprechende Rechte direkt im Dienst zu pflegen, weil der Gesamtaufwand dort geringer ist. Die Rollen müssten dagegen beim Identitätsprovider, also im IDM der Heimatorganisation der Nutzenden, gepflegt werden, da der Service-Provider nicht entscheiden kann, welche Rollen und Berechtigungen die Person nach Dafürhalten ihrer Heimatorganisation erhalten soll. Indem diese Informationen über das eduPersonEntitlement vom IdP an den SP übergeben werden, wird der administrative Aufwand reduziert, der sich bei einer Verortung des Rechte- und Rollenmanagements im IDM des Service-Providers oder in einem zentralen IDM einstellt. Zugleich wird das mit der doppelten Datenhaltung verbundene Sicherheitsrisiko vermieden. Wenn einer Person aufgrund eines Stellenwechsels o.Ä. in ihrem heimischen IDM Rollen entzogen werden, verliert sie automatisch auch die entsprechenden Rechte beim externen IT-Service.

2.2. Einrichten einer Subföderation NRW im DFN-AAI (abgeschlossen)

Die DFN-AAI bietet bereits die Möglichkeit, hochschulübergreifend auf webbasierte Services zuzugreifen. Darüber hinaus bietet sie eine Infrastruktur und schafft ein Vertrauensverhältnis zwischen den Organisationen. IDM.nrw möchte diese Infrastruktur *ergänzen* und hat sich in Form einer NRW-Subföderation in die DFN-AAI integriert. Technisch gesehen wird die NRW-Subföderation durch eine Entity Category realisiert. Identitätsprovider (IdPs), die an der Entity Category teilnehmen, geben damit ein definiertes Set von Attributen für alle teilnehmenden Service-Provider (SPs) frei. Indem die Vereinigung zu einer Entity Category gesammelte Attributfreigaben innerhalb der Föderation ermöglicht, vereinfacht sie die Attributfreigabe und die Identifizierung der zugriffsberechtigten IdPs. IDM.nrw hat eine entsprechende Entity Category in der DFN-AAI registriert, zzgl. der zugehörigen Object Identifier (das sind eindeutige Bezeichnungen der von IDM.nrw entwickelten Attribute). Zukünftige Serviceanbindungen lassen sich einfacher gestalten, da das Gewähren des Zugriffs auf eine Subföderation einfacher ist als den Zugriff für 42 Hochschulen individuell einzurichten. Dies gilt insbesondere mit Blick auf bundes-, europa-, oder weltweite Föderationen.

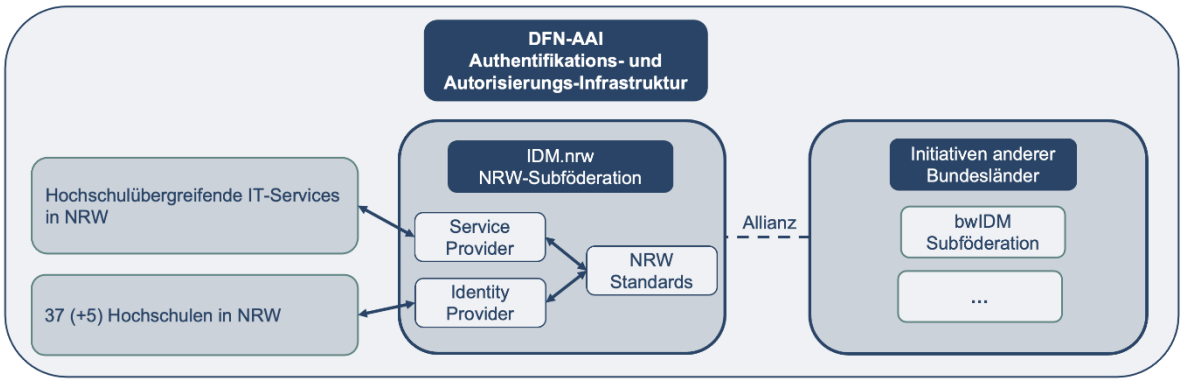

Abbildung 3: Einordnung in DFN-AAI

IDM.nrw ergänzt die Infrastruktur von DFN-AAI, indem sie gemeinsame Standards (Attribute und Rollen) für NRW einführt und bei Bedarf Attribute ergänzt. So reichten im Falle von Datensicherung.nrw die vorhandenen Attribute in der DFN-AAI nicht aus, weshalb zusätzliche Attribute notwendig waren, welche IDM.nrw in Abstimmung mit der DFN-AAI und Datensicherung.nrw eingeführt hat. Zudem arbeitet IDM.nrw derzeit an Lösungen für zwei Anforderungen, für die die DFN-AAI bisher keine oder nur rudimentäre Lösungen anbietet. Die DFN-AAI bietet keine Möglichkeit zur Verwaltung von (hochschulübergreifenden) Gruppen. Da aber gerade forschungsnahe IT-Services auch von Forschungsgruppen gemeinsam genutzt werden, muss

DIGITALE HOCHSCHULE NRW
INNOVATION DURCH KOOPERATION
gefördert durch:
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

ein föderiertes IDM auch die Möglichkeit zur Integration und Verwaltung entsprechender Gruppen bieten. IDM.nrw adressiert diesen Bedarf in dem Arbeitspaket Identity Proxy. Für den föderierten Zugriff auf nicht-webbasierte Dienste stellt die DFN-AAI aktuell nur eine rudimentäre Lösung bereit. IDM.nrw arbeitet im Kontext der Technologieevaluation an einer Lösung für einen föderierten Zugriff auf Nicht-Webdienste wie HPC.

Aktuell nehmen folgende Hochschulen und Service-Provider an der NRW-Subföderation teil: Fachhochschule Aachen, Hochschule Düsseldorf, Hochschule Rhein-Waal, Ruhr-Universität Bochum, RWTH Aachen, Universität Duisburg-Essen, Datensicherung.nrw und Coscine.nrw. Mit dem Beitritt zur NRW-Subföderation stimmen die Einrichtungen dem Code of Conduct zu. Weitere Informationen zum Beitritts-Prozedere sind dem Wiki zu entnehmen.

2.3. Technologieevaluation (Daueraufgabe)

In der Machbarkeitsstudie wurden bereits einige Technologien im Bereich Autorisierung und Authentifizierung recherchiert und evaluiert. Im Umsetzungsprojekt wird diese Aufgabe intensiviert. In diesem Arbeitspaket wird eng mit dem baden-württembergischen FIDM-Projekt bwIDM2, geleitet durch das Karlsruher Institut für Technologie (KIT), zusammengearbeitet.

IDM.nrw hat in einem eigenen Arbeitspaket bereits *Bewertungskriterien* für Technologien erarbeitet, welche größtenteils auch in der Allianz verwendet werden. Ursprünglich war die Erfüllung von BSI-Kriterien Teil der Bewertungskriterien von IDM.nrw. Die Erfüllung der BSI-Kriterien ist allerdings abhängig von der Umgebung, in der die Software eingesetzt wird. Daher konzentrieren sich die Technologieevaluationen bezüglich des Themas Sicherheit auf den Aspekt Security-by-Design (z. B. Vermeiden von Standardpasswörtern etc.). Entsprechend wurde dieses Kriterium umbenannt in Datenschutz und Informationssicherheit. Eine kommentierte Darstellung der Bewertungskriterien findet sich im Projekt-Wiki.

Aus der Bedarfsanalyse aus dem Vorprojekt sowie den föderierten Diensten in NRW im Rahmen der Digitalen Hochschule.NRW wurden die für die Hochschulen relevanten Anwendungsfälle herausgearbeitet – im Einzelnen: Multifaktor-Authentifizierung (MFA), Single Sign-On (SSO) und Autorisierungsverwaltung. Die Auswahl der zu evaluierenden Technologien orientiert sich an diesen Anwendungsfällen bzw. an den Bedarfen, die sich aus der Nutzung verteilter Services ergeben. Es wurden und werden vor allem Technologien in den Bereichen Access Management, Rechteverwaltung und Multifaktor-Authentifizierung evaluiert. Eine Übersicht mit Links zu den einzelnen Evaluierungsberichten findet sich im Projekt-Wiki.

Im Falle der Multifaktor-Authentifizierung (MFA) hat das Konsortium über die Evaluation einzelner Technologien das Thema allgemein aufbereitet und eine Empfehlung für die Ansiedelung des zweiten Faktors erarbeitet, welche auf einer vergleichenden Analyse der verschiedenen Möglichkeiten basiert.

Aktuell stehen zwei Themen im Fokus der Technologieevaluation, nämlich zum einen die Möglichkeiten zur *Communityverwaltung* (vgl. dazu Kap. 2.5) und zum anderen technische Lösungen für einen *föderierten Zugriff auf Nicht-Webdienste*. Für einen föderierten Zugriff auf Nicht-Webdienste werden aktuell zwei Arten von Lösungen ausgelotet, nämlich RegApp-as-a-Service und FedSSH.

RegApp-as-a-Service ist ein föderiertes Open-Source-Identity-Management-System, das am Scientific Computing Center (SCC) am KIT entwickelt wird.[9] Das System ermöglicht einen Zugriff mittels des von ihrer Heimatorganisation bereitgestellten Kontos und verspricht einen fö-

[9] Vgl. hierzu und zum Folgenden https://www.scc.kit.edu/dienste/regapp.php, 15.04.2024.

derierten Zugriff auf nicht-webbasierte Dienste wie HPC. Im Kontext Nationales Hochleistungsrechnen (NHR) nimmt das IT Center der RWTH Aachen daher am Vernetzungsprojekt RegApp-as-a-Service teil. Der hochschulübergreifende Zugriff auf verteilte HPC Cluster soll so über die RegApp ermöglicht werden. Die RegApp-Komponente wird installiert und in die bestehende LDAP-Infrastruktur der RWTH integriert. Darüber hinaus wird evaluiert, wie die RegApp als Authentifizierungsprovider für JARDS (einer Software zur Vergabe von HPC-Ressourcen) dienen kann. Die aktuellen, gemeinsamen Aktivitäten mit IDM.nrw und HPC.nrw stehen in engem Zusammenhang mit diesem Vorhaben.

Parallel evaluiert IDM.nrw derzeit verschiedene Lösungsmöglichkeiten für ein ***föderiertes SSH***. Es wurden verschiedene Lösungsansätze evaluiert. In der Verlängerungsphase, also dem Haushaltsjahr 2025, werden bis zu zwei Lösungen in einem Testbetrieb mit Blick auf die Anforderungen von IDM.nrw weiterentwickelt.

Bei Bedarf nimmt das Konsortium weitere Technologien zur Evaluierung auf. Der jeweils aktuelle Stand der evaluierten und der in der Evaluierung befindlichen Technologien ist im Wiki dokumentiert.

2.4. Use Cases (einzelne Use Cases abgeschlossen)

IDM.nrw arbeitet mit DH.NRW-Projekten zusammen, die hochschulübergreifende Services anbieten – die also Anwendungsfälle für ein föderiertes IDM darstellen. Sowohl die Ergebnisse aus Gemeinsame Attribute und Rollen als auch aus der Evaluierung von Technologien kommen in der Zusammenarbeit mit den Anwendungsfällen zum Einsatz.

Die Zusammenarbeit mit den Anwendungsfällen erfüllt aus der Sicht von IDM.nrw mehrere Funktionen. Zum einen wird damit sichergestellt, dass sich die im Rahmen von IDM.nrw entwickelten Konzepte an konkreten Bedarfen orientieren. Zum anderen werden die bereits erarbeiteten Konzepte in der Praxis erprobt. Zum dritten werden durch das Onboarding des jeweiligen Dienstes erste Schritte zur Etablierung eines gemeinsamen Standards der hochschulübergreifenden Dienste unternommen, so dass die Hochschulen als Identitätsprovider nicht für jeden Dienst neue, eigene Standards nutzen müssen. Zum vierten liefern die Use Cases auch Best-Practice-Beispiele, die anderen hochschulübergreifenden Diensten zur Verfügung gestellt werden.

Aktuell sind die folgenden Use Cases geplant oder in Bearbeitung bzw. bereits abgeschlossen:

- Datensicherung.nrw (abgeschlossen)
- Coscine.nrw (in Bearbeitung)
- E-Akte.nrw (in Bearbeitung)
- HPC.nrw (geplant)
- CRIS.nrw (geplant)
- Sciebo.nrw (geplant)

Aktuell zeichnet sich eine Zusammenarbeit mit weiteren Diensten ab.

gefördert durch:
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

2.5. Community-Verwaltung: Identity Proxy und Attribute Authority (laufende Maßnahme)

Im laufenden Projekt hat sich der Bedarf für ein weiteres Arbeitspaket herausgestellt, das im ursprünglichen Antrag nicht vorgesehen war. Dieser Bedarf betrifft die Verwaltung von Gruppenzugehörigkeiten. Darunter ist beispielsweise die Zugehörigkeit von Mitgliedern verschiedener Hochschulen zu einem gemeinsamen Forschungsprojekt zu verstehen. Damit diese Mitglieder einen gemeinsamen Bereich in einem hochschulübergreifenden Dienst nutzen können, muss der Service-Provider zuallererst über ihre Gruppenzugehörigkeit informiert sein, um die entsprechenden Berechtigungen zu vergeben. Die Heimateinrichtung (als Identitätsprovider) ist aber in der Regel nicht darüber informiert, welchen Forschungsgruppen, -verbänden u. Ä. ihre Mitglieder angehören – geschweige denn, dass derartige Informationen im Identitätsmanagement der Heimateinrichtung hinterlegt wären.

Als Lösung bietet sich ein Identity Proxy – orientiert am Blueprint des AARC Projects GÉANT – an. Das Konsortium hat sich aus mehreren Gründen für diesen Lösungsansatz entschieden. Zum einen arbeitet IAM4NFDI mit einer Proxy-Infrastruktur, vernetzt also vorhandene Proxys miteinander. Die Nutzung eines Identity Proxys gewährleistet die Anschlussfähigkeit an diese Infrastruktur. Zum anderen – und vor allem – bietet der angedachte Identity Proxy die Möglichkeit, Informationen zur Gruppenzugehörigkeit einzuspeisen, während die eigentliche Nutzerverwaltung bei den Heimateinrichtungen der Personen verbleibt. Die zusätzlichen Nutzendendaten (wie die Gruppenzugehörigkeiten) können über einen Identity Proxy gekoppelt an einen Attribute Service eingespeist werden. Vereinfacht gesagt, wird der Identity Proxy zwischen die IdPs der Heimateinrichtungen und die Services geschaltet, um die Informationen seitens der IdPs mit den Gruppen- oder Projekteinrichtungen ‚anzureichern'. (Das Schaubild stellt die Konstruktion schematisch dar.)

Die Pflege der Informationen zur Gruppenzugehörigkeit sollte von den jeweiligen Gruppen übernommen werden, um die administrativen Aufwände möglichst gering zu halten. Da Identity Proxys miteinander verschachtelt werden können, könnte eine Community auch einen eigenen Identity Proxy betreiben, um Community-spezifische Nutzendendaten einzuspeisen. Da aber jede noch so kleine Forschungsgemeinschaft dann einen eigenen Proxy bräuchte, würde sich die Komplexität der Verschachtelung immens erhöhen und damit der Support deutlich erschwert. Zudem ist es fraglich, ob sehr kleine und ggf. zeitlich begrenzte Projektgruppen den Aufbau und Betrieb eines Identity Proxys finanziell und personell bewältigen könnten. Vor diesem Hintergrund erscheint es deutlich kosteneffizienter, wenn das Konsortium eine zentrale Proxy-Infrastruktur betreibt.

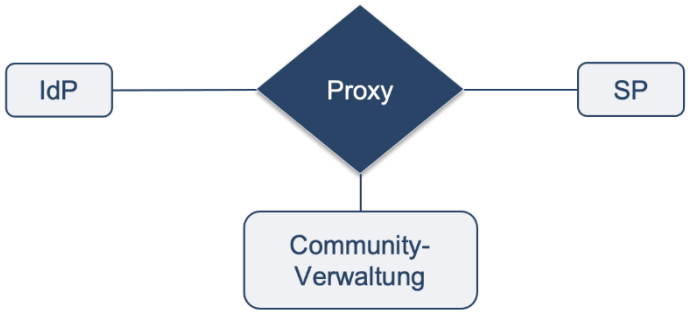

Abbildung 4: Proxy zur Gruppenverwaltung

Im Kontext der Projektverlängerung von IDM.nrw wurden durch das MKW auf Empfehlung der DH.NRW auch finanzielle Mittel für den Aufbau und die Implementierung des Identity Proxys und die Attribute Authority bewilligt. Aktuell wird in Zusammenarbeit mit einem externen Dienstleister ein Feinkonzept entwickelt. In der Verlängerungsphase (2025) erfolgt die technische Realisierung. Zudem werden eine Supportstruktur aufgesetzt und Datenschutzrichtlinien

DIGITALE HOCHSCHULE NRW
INNOVATION DURCH KOOPERATION
gefördert durch:
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

erarbeitet. Noch in der Verlängerungsphase soll das Onboarding von Piloten durchgeführt werden.

2.6. Pilot zum länderübergreifenden Zugriff mit Baden-Württemberg (geplante Maßnahme)

Aktuell gibt es in vielen Bundesländern Initiativen zur Einführung eines hochschulübergreifenden Identitätsmanagementsystems. Perspektivisch sollen die IDMs der Bundesländer miteinander vernetzt werden. Mitarbeitende von IDM.nrw stehen diesbezüglich im regelmäßigen Austausch mit den anderen Bundesländern, der nun auch institutionell verankert ist. Derzeit sind die Anstrengungen im Bereich eines föderierten IDMs in Baden-Württemberg und in Nordrhein-Westfalen am weitesten gediehen. Daher soll in der Verlängerungsphase gemeinsam mit Baden-Württemberg ein Pilotprojekt durchgeführt werden, im Zuge dessen die Attribute und Rollen ihrer föderierten IDMs angeglichen werden, um den länderübergreifenden Zugriff auf IT-Services in den jeweils anderen Bundesländern zu ermöglichen. Dieses Vorhaben erfordert selbstverständlich eine Übersetzung der Attribute und Rollen sowie deren technische Implementierung. Darin erschöpfen sich die Aufgaben jedoch nicht; denn schließlich sollen Hochschulangehörige Dienste nutzen dürfen, die von einem anderen Bundesland betrieben und finanziert werden.

2.7. Kommunikation (Daueraufgabe)

Die Kommunikation ist auf verschiedenen Ebenen und unterschiedlichen Kontexten eine Daueraufgabe im Projekt.[10] Dies ergibt sich einerseits daraus, dass IDM.nrw mit Blick auf das föderierte Identitätsmanagement als kommunikative Schnittstelle zwischen den NRW-Hochschulen, den Dienstanbietern sowie den Initiativen in anderen Bundesländern fungiert. Andererseits ergibt sich die enge Kommunikation mit den Hochschulen vor allem aus dem Selbstverständnis des Projekts, die Grundlagen eines föderierten Identitätsmanagements *für* die Hochschulen und *mit* den Hochschulen zu entwickeln. Es hat sich jedoch gezeigt, dass die Erkenntnisinteressen der Hochschulangehörigen bezogen auf die Idee eines föderierten Identitätsmanagements wie auch die entsprechenden Kenntnisse sehr heterogen sind. Da der Erfolg des Vorhabens wesentlich von der Akzeptanz seitens der Hochschulangehörigen abhängt, werden die Kommunikationsmaßnahmen im Projekt zukünftig intensiviert und ausdifferenziert. Durch die abgeschlossenen Arbeitspakete ist zugleich die Grundlage gegeben, um den länderübergreifenden Austausch zu intensivieren. Dies erhöht nicht nur die bundesweite Sichtbarkeit von IDM.nrw, sondern schafft auch die Grundlagen für einen potentiellen bundesweiten Zugriff auf hochschulübergreifende Dienste.

Die obigen Ausführungen machen deutlich, dass die Außenkommunikation von IDM.nrw verschiedene Ziele verfolgt. So sind mehrere Maßnahmen darauf ausgerichtet, die Bekanntheit des Vorhabens zu steigern. Die betroffenen Gruppen innerhalb NRWs sollen zudem transparent über den Projektstand und die weitere

[10] Im Folgenden wird lediglich die Außenkommunikation von IDM.nrw betrachtet. Die Kommunikation innerhalb des Konsortiums in Form regelmäßiger Projekttreffen usw. wird nicht eigens dargestellt.

Planung informiert werden. Zugleich soll auch sichergestellt werden, dass die konkreten Bedarfe der hochschulübergreifenden Dienste wie auch der Hochschulen Berücksichtigung finden. Im Zuge dessen soll insbesondere die Akzeptanz für ein föderiertes Identitätsmanagement geschaffen werden. Mit Blick auf länderübergreifende Entwicklungen sind überdies Abstimmungen mit verwandten Initiativen in anderen Bundesländern und nicht zuletzt mit der DFN-AAI wichtig, um die Zukunftsfähigkeit eines föderierten IDM in NRW zu gewährleisten.

Dementsprechend adressieren die Kommunikationsmaßnahmen von IDM.nrw sehr unterschiedliche Zielgruppen. Je nach Zielgruppe werden unterschiedliche Themen in unterschiedlichen Detailgraden kommuniziert. Die Wahl der Formate erfolgt ebenso mit Blick auf die jeweilige Zielgruppe und Zielsetzung. Die Kommunikationsstrategie von IDM.nrw stellt sich folglich als mehrdimensionales Gefüge dar. Die folgende Klassifikation der Zielgruppen und Formate soll einen ersten Überblick ermöglichen.

Zielgruppen und Themen. IDM.nrw adressiert Zielgruppen innerhalb und außerhalb NRWs. Je nach Zielgruppe stehen dabei andere Themen(aspekte) und Zielsetzungen im Mittelpunkt.

Innerhalb NRWs richten sich verschiedene Kommunikationsmaßnahmen an Angehörige der Hochschulen. Ganz allgemein zielen die Kommunikationsmaßnahmen darauf ab, die Hochschulen über die Projektfortschritte zu informieren und ihnen die Möglichkeit zur Partizipation zu geben. Bislang wurde hauptsächlich die Zielgruppe der IDM-Fachexpert*innen betrachtet. Für diese stellt IDM.nrw vor allem technische Informationen und Empfehlungen sowie perspektivisch Best-Practice-Beispiele (anhand der Use Cases) im Projekt-Wiki zur Verfügung.

Auch die mittlerweile etablierten Veranstaltungsformate weisen einen stark technisch orientierten Schwerpunkt auf. Zusätzlich sollen in Zukunft die Lehrenden, Forschenden sowie die Leitungen von Rechenzentren und DH-Projekten stärker adressiert werden. Diesen Zielgruppen soll das Projekt erklärt werden, zudem sollen die aus dem Projekt resultierenden Vorteile vermittelt werden. Damit reagiert IDM.nrw auf eine Herausforderung, die sich aus einem Zirkel ergibt. Es bedarf der Akzeptanz seitens der Hochschulen, damit die digitale Servicelandschaft weiter ausgebaut werden kann; zugleich erreicht man die Akzeptanz am ehesten durch positive Erfahrungen mit der Servicelandschaft. Vor dem Ausbau der Servicelandschaft kann die erforderliche Akzeptanz also nur dadurch erreicht werden, indem die zukünftigen Vorteile eines föderierten IDMs erklärt werden.

Außerhalb NRWs steht der Austausch mit verwandten Initiativen im Mittelpunkt. Etablierte Kooperationen gibt es bislang mit dem DFN-AAI und mit dem Projekt bwIDM2 (Baden-Württemberg); vgl. dazu auch Kapitel 2.6.

Während der gesamten Projektlaufzeit wird das Konsortium eng mit der ***Authentifikations- und Autorisierungs-Infrastruktur des Deutschen Forschungsnetzes*** (DFN-AAI) kooperieren. Insbesondere werden große Entscheidungen vor der Veröffentlichung abgestimmt (siehe dazu oben die Ausführungen zur Einrichtung einer Subföderation NRW).

Das Projekt ***bwIDM2*** verfolgt als Zielsetzung die Etablierung eines föderierten Identity Managements in Baden-Württemberg und die Weiterentwicklung der im Vorprojekt bwIDM entwickelten RegApp. Da IDM.nrw und bwIDM2 das gleiche Ziel verfolgen und um von gegenseitigen Erfahrungen profitieren zu können, wurde eine Allianz aus beiden Projekten gegründet. Insbesondere im Arbeitspaket Evaluierung von Technologien arbeiten die Projekte eng zusammen. Ziel der Kooperation ist es, von gegenseitigen Synergieeffekten zu profitieren und übertragbare Blaupausen zu entwickeln.

Neben diesen beiden etablierten Kooperationen gewinnt der Austausch mit verwandten Initiativen aus anderen Bundesländern zunehmend an Bedeutung, also mit Initiativen, die für die Hochschulen in ihrem jeweiligen Bundesland ein föderiertes Identitätsmanagement einführen.

Dadurch wird nicht nur eine länderübergreifende Wissensteilung ermöglicht, sondern es werden auch die Grundlagen für einen potenziellen bundesweiten Zugriff auf IT-Services geschaffen. (Die Anbindung an andere Bundesländer wird sich deutlich einfacher gestalten, wenn in NRW bereits gemeinsame Standards genutzt werden.) Der bundesweite Austausch erfolgt im Rahmen sogenannter ‚Ländertreffen'. Auf dem zweiten Ländertreffen zum Föderierten IDM (13 & 14. März 2024) wurde beschlossen die Ländertreffen regelmäßig, in einem halbjährlichen Rhythmus, fortzuführen.

Formate. Je nach Thema und Zielsetzung bedient sich IDM.nrw verschiedener Formate in der Außenkommunikation, insbesondere die Projektwebseite, das Wiki von IDM.nrw, Mailings und Veranstaltungen. Nähere Informationen und weiterführende Links zu diesen Formaten finden Sie im Anhang dieses Berichts im Abschnitt „Quellen und Formate".

Während im Wiki von IDM.nrw hauptsächlich technische Dokumentationen, Evaluationen und Empfehlungen (zu den gemeinsamen Attributen, den Rollen und den zentralen Personengruppen) zur Verfügung gestellt werden, ermöglichen die Veranstaltungen als dialogisches Format den direkten Austausch. Dadurch können Missverständnisse ausgeräumt werden, offene Fragen geklärt werden und nicht zuletzt die Wünsche und Bedarfe der Akteure erfasst werden. Daher nehmen Veranstaltungen in verschiedenen Varianten einen sehr großen Raum im Kontext der Kommunikationsmaßnahmen des Projekts ein.

Etablierte Formate sind das etwa halbjährlich stattfindende *IDM.nrw Forum* und die zu geeigneten Zeitpunkten stattfindenden *Technologieworkshops für IDM-Fachexpert*innen*. Im Anhang finden Sie weiterführende Informationen und Links zu diesen beiden und weiteren Formaten. Neben den von IDM.nrw organisierten Veranstaltungen hat das Konsortium das Vorhaben im Rahmen verschiedener Veranstaltungen vorgestellt. Eine Übersicht findet sich im Anhang im Anschnitt „Projektvorstellungen". Die Projektvorstellungen steigern auch die Bekanntheit des Vorhabens. Ähnliches gilt auch für die Beratungsleistungen von IDM.nrw außerhalb des Hochschulwesens in NRW. So hat IDM.nrw Tischler.NRW und VIDIS zum Thema föderiertes IDM beraten. (Nähere Informationen dazu finden sich im Anhang des Berichts.)

Im Zuge der Weiterentwicklung des Projekts zeigte sich jedoch, dass die verschiedenen Teile des Projekts für unterschiedliche Gruppen und in je eigener Detailtiefe relevant sind. Dem trägt das Konsortium Rechnung, indem die Informationsangebote in Zukunft stärker differenziert werden, was sich vor allem in der Konzeption der Veranstaltungen niederschlägt. Die Veranstaltungen werden jedoch in Zukunft weniger darauf ausgerichtet sein, einen Gesamtüberblick über den Projektstand zu liefern, sondern themenspezifische Schwerpunkte setzen und damit speziellere Zielgruppen ansprechen. Dies wird dadurch erreicht, dass neben den etablierten Veranstaltungsformaten weitere Formate angeboten werden. So wendete sich der am 20.02.2024 in Bochum durchgeführte IDM-Workshop nicht ausschließlich an diejenigen, die an ihrer Hochschule operativ für den Betrieb des hochschuleigenen IDMs verantwortlich sind, sondern auch an interessierte Rechenzentrumsleitungen.

3. Schluss: Ausblick

In der aktuellen Phase des Projekts sind die Arbeitspakete zur Schaffung der konzeptionellen Grundlagen abgeschlossen. Die gemeinsamen Attribute wie auch die zentralen Personengruppen und die Rollen wurden definiert, abgestimmt und in der NRW-Subföderation implementiert. Damit sind die Voraussetzungen für eine gemeinsame Struktur geschaffen. *Viele IT-Services – eine gemeinsame Struktur: IDM.nrw!* Damit wurde erfolgreich der Grundstein für die Anwendung der Ergebnisse in der folgenden Phase gelegt.

Im Juli 2024 wurde das Projekt IDM.nrw seitens des MKW NRW auf Empfehlung der DH.NRW um ein weiteres Jahr verlängert, also bis 31.12.2025. In diesem Zeitraum stehen vor allem die folgenden Maßnahmen im Mittelpunkt.

Kommunikation. Das Gelingen des föderierten Identitätsmanagements hängt wesentlich davon ab, dass die hochschulübergreifenden Dienste überhaupt genutzt werden und die gemeinsamen Standards auf Seiten der Hochschulen wie auch der Dienste implementiert werden. Dementsprechend zielen die Kommunikationsmaßnahmen von IDM.nrw verstärkt darauf ab, die Bekanntheit des Vorhabens und vor allem die Akzeptanz der gemeinsamen Standards zu steigern. Dafür wird zum einen die Zielgruppe der Kommunikationsmaßnahmen ausgeweitet und zum anderen werden eben jene Maßnahmen stärker hinsichtlich der Themen und Detailgrade ausdifferenziert – wie oben unter „Kommunikation“ ausgeführt.

Communityverwaltung. Die Integration einer Möglichkeit zur Communityverwaltung bzw. zur Einspeisung von Informationen zur Gruppenzugehörigkeit bilden einen weiteren Arbeitsschwerpunkt in der verbleibenden Projektlaufzeit. Als technische Lösung kristallisierte sich ein Identity Proxy heraus. Aktuell wird ein Konzept für einen solchen Proxy abgestimmt und ausgearbeitet. In der Verlängerungsphase erfolgt die technische Realisierung, also der Aufbau und Implementierung des Identity Proxys und der Attribute Authority.

Länderübergreifende Vernetzung. Der länderübergreifende Austausch spielt eine wesentliche Rolle, um die Weichen für einen bundesweiten Zugriff auf IT-Services zu stellen. Als erster Schritt in Richtung einer Interoperabilität zwischen den föderierten Identitätsmanagement-Systemen der Bundesländer wird in der Verlängerungsphase gemeinsam mit Baden-Württemberg ein Pilotprojekt durchgeführt. Im Zuge dessen werden die Attribute und Rollen ihrer föderierten IDMs angeglichen, um den länderübergreifenden Zugriff auf IT-Services in dem jeweils anderen Bundesland zu ermöglichen. Gemeinsame Standards in NRW erleichtern eine solche länderübergreifende Vernetzung und entsprechend die Interoperabilität. Angesichts des Entwicklungsstands in einigen Bundesländern wird die bundesweite Vernetzung jedoch nicht mehr innerhalb der derzeit geplanten Projektlaufzeit von IDM.nrw abgeschlossen sein.

Pilot zu einer FedSSH-Lösung in der Technologieevaluation. Im Bereich der Technologieevaluation wurden in den letzten Monaten mehrere FedSSH-Lösungen für den föderierten Zugriff auf Nicht-Webdienste gesichtet und evaluiert. Vor dem Hintergrund dieser Evaluationen werden in der Verlängerungsphase ein bis zwei Lösungen implementiert und weiterentwickelt bzw. auf die Bedarfe von IDM.nrw und die Strukturen in der NRW-Hochschullandschaft angepasst.

Use Cases und Onboarding. Das Gelingen des föderierten IDMs hängt wesentlich von der Partizipation der Hochschulen und der IT-Services ab. Dementsprechend spielt das Onboarding beider Gruppen auch in der Verlängerungsphase eine wesentliche Rolle.

Das Onboarding der Dienste erfolgt im Rahmen der Use Cases. Dieses Arbeitspaket wird in der Verlängerungsphase fortgeführt und um weitere Anwendungsfälle erweitert. Damit wird dafür Sorge getragen, dass einerseits die IT-Services die gemeinsamen Standards adaptieren und dass andererseits ggf. erforderliche Erweiterungen vorgenommen werden. Angesichts dessen, dass weitere Services in NRW im Aufbau befindlich sind oder zumindest geplant sind, wird dieser Prozess zum Projektende nicht endgültig abgeschlossen sein.

Um den Beitritt der Hochschulen zur NRW-Subföderation und die Adaption der gemeinsamen Standards zu unterstützen, entwickelt das Konsortium von IDM.nrw in Zusammenarbeit mit dem Programmausschuss der DH.NRW geeignete Unterstützungsmaßnahmen.

Die Ergebnisse aus dem bisherigen Verlauf des Projekts wie auch der Abgleich mit Projekten aus anderen Bundesländern bestätigen die Einschätzung, dass für die Zielsetzungen eines föderierten Identitätsmanagements in NRW eine kontinuierliche Weiterentwicklung und Erneuerung der geschaffenen Strukturen und Prozesse unabdingbar sind. Nur dadurch kann ein langfristiger Erfolg des Projekts gewährleistet werden. Dementsprechend kann im Rahmen der geplanten Projektlaufzeit auch nur der initiale Aufbau eines IDMs erfolgen. Es werden Grundlagen geschaffen. Mittel- und langfristig ergeben sich jedoch Bedarfe für die Weiterentwicklung und den Ausbau des FIDM NRW.

gefördert durch:
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

4. Weiterführende Dokumente, Informationen und Links

4.1. Quellen und Formate (allgemein)

- ***Webseite.*** Die Projektwebseite kann als erste Anlaufstelle dienen, um sich über das Projekt zu informieren. Sie liefert einen Überblick über das Projekt (unterteilt nach den beiden Phasen: Machbarkeitsstudie und das aktuell laufende Umsetzungsprojekt) und verlinkt auf weiterführende Informationen:

  https://idm.dh.nrw/

- ***Wiki.*** Das Wiki von IDM.nrw stellt technische Dokumentationen und Empfehlungen (wie die zu den gemeinsamen Attributen, den Rollen und den zentralen Personengruppen) sowie weiterführende Informationen zur Technologieevaluation und den Use Cases zu Verfügung. Zudem sind dort Informationen zu durchgeführten Veranstaltungen (Folien und Protokolle) abgelegt:

  https://doku.idm.nrw/mediawiki/index.php/Hauptseite

- ***Mailings.*** Aktuellere Informationen, wie z. B. Einladungen zu Veranstaltungen, werden per Newsletter versendet. Eine Anmeldung ist über diesen Link möglich:

  https://lists.rwth-aachen.de/postorius/lists/newsletteridmnrw.lists.rwth-aachen.de/

- ***Veranstaltungen:***
  - Ankündigungen auf Webseite: https://idm.dh.nrw/news-und-termine/news/termine
  - ***IDM.nrw Foren.*** Um die Hochschulen in NRW stets auf dem aktuellen Stand zu halten und ihr Feedback zu den Arbeitsergebnissen zu erhalten, werden nach jedem abgeschlossenen Meilenstein und mindestens zwei Mal pro Jahr landesweite Workshops durchgeführt. Um den Teilnehmerkreis an den regelmäßigen Terminen zur Ergebnisvorstellung bzw. Austausch über aktuelle Themen zu vergrößern, wurde bereits die Bezeichnung „Workshop“ in „IDM.nrw Forum“ umbenannt. So soll deutlich werden, dass es sich nicht um eine Arbeitsaufforderung, sondern um eine Ergebnispräsentation handelt. Eine Übersicht über die bisher durchgeführten Foren findet sich im Projekt-Wiki. Dort sind auch die Folien und die Protokolle zu den Veranstaltungen abgelegt:

    https://doku.idm.nrw/mediawiki/index.php/IDM.nrw_Forum

  - Technologieworkshops:

    https://doku.idm.nrw/mediawiki/index.php/Technologieworkshops

  - (weitere) Veranstaltungen:

    https://doku.idm.nrw/mediawiki/index.php/(Weitere)_Veranstaltungen

4.2. Themenspezifische Dokumente und Erläuterungen

- Gemeinsame Attribute:
  https://doku.idm.nrw/mediawiki/index.php/Gemeinsame_Attribute
- Zentrale Personengruppen:
  https://doku.idm.nrw/mediawiki/index.php/Zentrale_Personengruppen

- Rollen:
  https://doku.idm.nrw/mediawiki/index.php/Rollen
- NRW-Subföderation:
  https://doku.idm.nrw/mediawiki/index.php/NRW-Subf%C3%B6deration
- Multifaktor-Authentifizierung:
  https://doku.idm.nrw/mediawiki/index.php/MFA
- Evaluierung von Technologien:
  - Bewertungskriterien:
    https://doku.idm.nrw/mediawiki/index.php/Bewertungskriterien
  - Evaluierte Technologien:
    https://doku.idm.nrw/mediawiki/index.php/Technologien
  - Erfahrungsberichte:
    https://doku.idm.nrw/mediawiki/index.php/Erfahrungsberichte

4.3. Projektvorstellungen

Das Konsortium hat das Projekt IDM.nrw im Rahmen verschiedener Veranstaltungen innerhalb und außerhalb NRWs vorgestellt:

- DV Pro Sitzung | 01.06.2021
- Programmausschuss DH.NRW | 26.07.2021
- IDM Techniktreff | 31.08.2021
- Vorstandssitzung der DH.NRW | 10.09.2021
- DH.NRW Tagung inkl. virtuellem Stand | 14./15.09.2021
- AG Informationsinfrastruktur | 21.09.2021
- ZKI AK IAM | 02.12.2021
- DFN Betriebstagung | 29.03.2022
- bwIDM2 Betriebstagung | 27.04.2022
- DV-Pro III | 08.11.2022
- ARNW |11.07.2023

4.4. Beratungsleistungen für Akteure außerhalb des Hochschulwesens in NRW

Bislang hat IDM.nrw zwei Einrichtungen außerhalb des Hochschulwesens zum Thema föderiertes IDM beraten, nämlich Tischler.NRW und VIDIS.

Tischler.NRW ist der Fachverband des Tischlerhandwerks Nordrhein-Westfalen. Sie ist die gesetzliche Interessenvertretung der in 49 Tischlerinnungen organisierten klein- und mittelständischen Handwerksbetriebe. In diesem Zusammenhang möchte Tischler.NRW Lehrlingen im Tischler-Handwerk die Möglichkeit bieten, unkompliziert Zugang zu Services anderer Berufsschulen, Betrieben und überbetrieblichen Lehrwerkstätten zu erlangen. Bislang fehlt hier allerdings die nötige Single-Sign-On-(SSO)-Infrastruktur. Dabei steht IDM.nrw beratend zur Seite.

VIDIS. Das Projekt VIDIS wird federführend durchgeführt vom Institut für Film und Bild in Mecklenburg-Vorpommern, finanziert wird es im Rahmen des DigitalPakts Schule 2019–2024. Ziel des Projekts ist die Entwicklung eines SSO, mit Hilfe dessen Schüler*innen und Lehrkräfte einfach und unkompliziert mit bestehenden Nutzerkonten auf digitale Bildungsangebote (z. B.

Lernplattformen oder digitale Lerninhalte) zugreifen können. Die Anmeldung erfolgt beim jeweiligen Landesportal und der Zugriff auf Dienste anschließend über VIDIS.

5. Verzeichnis der Schaubilder