Abschlussbericht des Vorprojekts „Machbarkeitsstudie föderiertes Identity Management.nrw“

Projektgruppe “Machbarkeitsstudie föderiertes Identity Management.nrw“ | Konsortium: Rheinisch-Westfälische Technische Hochschule Aachen (Aylin Gündogan, Ann-Kathrin Wluka, Thomas Eifert, Thorsten Kurth, Michael Gerhards) mit Universität Bielefeld (Norbert Sand, Nico Urbanczyk), Ruhr-Universität Bochum (Haiko te Neues, Alexander Schluck), Universität Duisburg-Essen (Andreas Bischoff, Burkhard Wald, Gabriel Guckenbiehl) und Universität zu Köln (Beate Schlesiona)

Laufzeit: 01.04.2019 - 30.09.2020

Ein Kooperationsvorhaben empfohlen durch die:
DIGITALE HOCHSCHULE NRW
INNOVATION DURCH KOOPERATION

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

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AaaS ..... *Authentification as a Service*
AD ..... *Active Directory*
AP ..... *Arbeitspaket*
CIO ..... Chief Information Officer
CSV ..... *Comma-separated values*
DFN-AAI ..... Deutsches Forschungsnetz- Authentifikations- und Autorisierungs-Infrastruktur
DV Pro ..... *Datenverarbeitungsprojektgruppe*
DVZ-Leiter *Arbeitskreis der Leiter der Datenverarbeitungszentralen an den Fachhochschulen in NRW*
FIDM ..... *föderiertes Identity Management*
HPC ..... *High Performance Computing*
IdP ..... *Identity Provider*
KISS ..... *Keep It Short and Simple*
KUMUs ..... *Kunst- und Musikhochschulen*
LDAP ..... *Lightweight Directory Access Protocol*
SAML ..... *Security Assertion Markup Language*
SP ..... *Service Provider*
VRZ ..... *Verbundrechenzentrum*
ZKI ..... *Zentren für Kommunikationsverarbeitung in Forschung und Lehre*

1. Abstract

Der vorliegende Abschlussbericht der Projektgruppe “Machbarkeitsstudie föderiertes Identity Management.nrw“ beschreibt zentrale Ergebnisse zur Konzeption eines föderierten Identity Managements für Hochschulen des Landes Nordrhein-Westfalen (NRW) unter besonderer Berücksichtigung von kleinen Einrichtungen bzw. Fachhochschulen und Kunst- und Musikhochschulen. Mit einem föderierten Identity Management (FIDM) soll es zukünftig möglich sein, hochschulübergreifende Services zu nutzen bzw. anzubieten. Die Authentifizierung selbst soll an der jeweiligen Heimateinrichtung erfolgen, sodass zur Anmeldung am jeweiligen Service die lokalen Anmeldedaten genügen. Aufgrund des Themenkomplexes und um eine entsprechende bedarfsgerechte Lösung zu konzipieren, ist zunächst die Erfassung von Anforderungen notwendig. Nachdem in Kapitel 2 die Rahmenbedingungen des Projektvorhabend erläutert werden, werden in Kapitel 3 die zentralen Erkenntnisse aus den durchgeführten Befragungen vorgestellt. Des Weiteren werden deutschland- und europaweite Verbünde recherchiert und nach ihrer Technik und Struktur untersucht. Die Erkenntnisse aus der Anforderungsanalyse in Kapitel 4 zeigen, dass sich drei große IDM-Themen (sowohl organisatorisch als auch technisch) als zentrale Anforderungen festhalten lassen. Neben der Ermittlung eines Attribut-Sets, das gemeinsame Attribute in NRW beinhaltet, sollen zentrale Personengruppen-Definitionen in NRW möglichst homogenisiert werden. Beide Themenbereiche erfordern einen engen Austausch mit den Hochschulen und Servicebetreibern in NRW. Die erarbeiteten Grobkonzepte werden in Kapitel 5 näher beschrieben. Das dritte und sehr wichtige Thema ist die Evaluierung von Technologien. Hier sollen Technologien evaluiert werden, um u.a. Lösungen für einen föderativen Zugriff auf Nicht-Webanwendungen zu erarbeiten. Denn laut der Anforderungsanalyse gibt es derzeit an keiner Hochschule in NRW ein Konzept, welches die oben beschriebene Technologielücke löst. Die konkrete Ausarbeitung der Fachkonzepte ist ein Teil des Umsetzungsplan, welches in Kapitel 6 näher beschrieben wird.

2. Rahmenbedingungen

2.1. Hintergrund und Vision

Die Hochschulen in Nordrhein-Westfalen (NRW) bieten ihren Nutzenden eine Vielzahl von IT-Services und Ressourcen an, die auch von Angehörigen und Mitgliedern anderer Hochschulen genutzt werden könnten. Beispiele dafür sind die Bereitstellung von verteilten (Rechen- oder Speicher-) Ressourcen, oder die Teilnahme an Kursen an anderen Hochschulen (E-Learning) durch Studierende. Da oftmals die einfache Verwendung dieser Dienste auf die Angehörigen und Mitglieder der eigenen Einrichtung zugeschnitten sind, ist derzeit für eine hochschulübergreifende Nutzung noch die Verwendung dieser Services mit hohem Aufwand verknüpft. Demnach müssen z.B. hochschulexterne Nutzende bei der Hochschule, die den Dienst anbietet, einen eigenen Zugang beantragen, was zu einem erhöhten Aufwand bei der Datenverwaltung von Identitäten für beide Seiten (Hochschulen sowie Anbieter und Nutzende) führt. Diese Situation stellt keine effiziente und effektive Grundlage für intensive, hochschulübergreifende Kooperationen in NRW dar, da ein gesichertes Identity Management die Voraussetzung für moderne und integrierte Servicenutzung ist. Das Ziel von IDM.NRW ist der hochschulübergreifende Austausch lokal verwalteter Identitätsdaten. Dadurch wird zum einen die übergreifende Servicenutzung ohne Accounts an fremden Einrichtungen erreicht und ermöglicht und zum anderen die Datenqualität und Sicherheit erhöht, da Personeninformationen ausschließlich von vertrauenswürdigen Datenquellen akzeptiert werden.

Unter der Leitung der Rheinisch-Westfälische Technischen Hochschule (RWTH), federführend durch das IT Center, wurde deswegen im Rahmen der Digitalen Hochschulen NRW (DH.NRW) ein Vorprojekt zur Erstellung eines Landeskonzepts für ein gemeinsames föderiertes Identity Management „Machbarkeitsstudie föderiertes Identity Management.nrw“ gestartet. Konsortialpartner sind die Universität Bielefeld, die Ruhr-Universität Bochum, die Universität Duisburg-Essen und die Universität zu Köln. Das Ziel ist es, ortsunabhängig und über Hochschulgrenzen hinweg den Zugang zu Services in NRW sicherzustellen und die Kooperationen zwischen den Hochschulen so einfach wie möglich zu gestalten. Hierbei sollen nicht nur Studierende der NRW Hochschulen unterstützt werden, sondern auch Organisationsverantwortliche, Forschende und Lehrende. Die Stärkung der Infrastruktur steht im Fokus des Projektvorhabens. Die Datenerhebung sowie Aufbereitung erfolgt unter Beteiligung aller genannten Universitäten, sowie unter besonderer Berücksichtigung bereits bestehender Kooperationsprojekte (z.B. hpc.nrw, AcademicGroupware.nrw). Hier geht es u.a. um die Aufbereitung eines aktuellen Forschungsstandes zum Thema, sowie die Sammlung bereits bestehender Aktivitäten (z.B. in der DFN-AAI Föderation (Deutsches Forschungsnetz-Authentifikations- und Autorisierungs-Infrastruktur), im ZKI-Arbeitskreis Identity und Access

Management und Projekte in Sachsen und Baden-Württemberg sowie die Sammlung der gewonnenen Erkenntnisse auf Landesebene. Darüber hinaus wird der Status Quo der IT-Infrastrukturen bzw. der Prozesse aller Hochschulen in NRW, die Grundfunktionalitäten eines föderierten Identity Management (FIDM) und die Anforderungen, die sich daraus ergeben, erfragt. Nach der Datenerhebung werden mithilfe von Use Cases (auch nicht webbasierte Dienste), z.B. Sciebo oder GigaMove, berücksichtigt, um ein möglichst effektives Grundkonzept für IDM.NRW zu erarbeiten. Die Machbarkeitsstudie soll durch die Bereitstellung einheitlicher Identity Management (IDM) -Prozesse die Grundlage zur einfachen und einheitlichen Nutzung von Services diverser Hochschulen sein. Das gemeinsame Verständnis erhöht die Durchlässigkeit bei der Prozessorganisation. Für die gegenseitige Serviceerbringung ist dies eine Voraussetzung.

Als Inputgruppen haben die Arbeitsgemeinschaft der Leiter wissenschaftlicher Rechenzentren in NRW (ARNW), der Arbeitskreis der Leiter der Datenverarbeitungszentralen an den Fachhochschulen in NRW (DVZ-Leiter), die Datenverarbeitungsprojektgruppe (DV Pro), der Chief Information Officer (CIO) der Kunst- und Musikhochschulen und das Verbundrechenzentrum der Kunst- und Musikhochschulen (VRZ) ihre Unterstützung zur Förderung des Antrags ausgesprochen. Das Projektvorhaben wurde vom Ministerium für Kunst und Wissenschaft bewilligt und die Mittel zur Durchführung zugewiesen. Das Projektvorhaben startete zum 01.04.2019, um ein Konzept für ein föderiertes Identity Management (FIDM) in NRW zu erarbeiten.

2.2. Arbeitspakete und Vorgehen

Innerhalb der Machbarkeitsstudie werden die beschriebenen Aufgaben vornehmlich durch das IT Center der RWTH Aachen University koordiniert und in Zusammenarbeit mit allen Konsortialpartnern durchgeführt. Wichtigstes Element ist die enge Zusammenarbeit aller Mitarbeitenden mit entsprechender Expertise im Bereich IDM aller beteiligter Hochschulen. Die Erarbeitung der Machbarkeitsstudie erfolgte entlang von vier Arbeitspaketen (AP), die im Folgenden näher erläutert werden.

Das erste Arbeitspaket (AP 1) wurde in der Kick-Off-Veranstaltung am 03.10.2019 in Aachen bearbeitet. Es wurden Erwartungen an das Projekt und das konkrete Ziel besprochen und gemeinsam festgelegt. Dies war von besonderer Bedeutung, um ein gemeinsames Voranschreiten und Vorantreiben des Projekts zu gewährleisten. Des Weiteren wurden Rahmenbedingungen zur gemeinsamen Arbeit sowie Kommunikation festgelegt. Um einen regen Austausch und Abstimmungen in der Projektgruppe aufrechtzuerhalten, wurden regelmäßige Videokonferenztermine (14-tägig) durchgeführt. Zudem wurden Termine festgelegt, in denen die erarbeiteten Ergebnisse der jeweiligen Meilensteine vorgestellt und

diskutiert wurden. Dies erfolgte in Form von interaktiven Workshops mit einem großen Diskussionsanteil. Um die Projektergebnisse nachhaltig zu sichern, wurde als gemeinsame Dokumentations- und Austauschplattform Sciebo gewählt. Grundregeln für das Team wurden definiert, um auch hier die bereits erwähnte erfolgreiche und zielführende Zusammenarbeit zu fördern.

Im Nachgang wurde das zweite Arbeitspaket (AP 2) analysiert und Aufgaben wurden definiert. In diesem Zusammenhang wurde eine Status-Quo Erfassung im Land NRW durchgeführt. Zum einen wurde die IDM-Systemlandschaft in NRW analysiert und zum anderen wurde die Servicelandschaft in NRW betrachtet. Dazu wurden nicht nur bereits vollumfänglich betriebene Services betrachtet, sondern auch Projektinitiativen der DH.NRW. Zur Erfassung der IDM-Systemlandschaft wurde eine Onlineumfrage mit dem Online Umfragetool EvaSys mit IDM-spezifischen Fragen erstellt und an die Einrichtungen (42 DH.NRW Mitglieder) in NRW verteilt. Nach einer ersten Auswertung der Ergebnisse wurde eine Nacherfassung mithilfe von Experteninterviews durchgeführt. Ziel der Nacherfassung war es, vage Antworten aus der Umfrage zu konkretisieren, um fundierte Rückschlüsse über die IDM-Systemlandschaft in NRW zu erzielen. Parallel wurde die bundesweite IDM-Systemlandschaft betrachtet, um Gemeinsamkeiten und Unterschiede zu ermitteln. Dazu wurde ein Wiki herangezogen, dass vor Jahren von dem ZKI-Arbeitskreis IAM aufgesetzt wurde.[1] Zur Erfassung der Servicelandschaft wurden ebenfalls Experteninterviews mit Servicebetreibern und Projektverantwortlichen geführt. Insbesondere wurden gewünschte Funktionalitätsanforderungen an das IDM abgefragt. Aus den Resultaten beider Erfassungen (IDM-Systemlandschaft und Servicelandschaft NRW) wurden entsprechende Anforderungen ermittelt und formuliert, um bedarfsgerechte Lösungen zu skizzieren. Unter anderem wurden spezifische Anforderungen und Grundfunktionalitäten eines FIDM sowie der anzuschließenden Dienste und Services ermittelt.

Daneben wurden bereits etablierte landesweite sowie bundesweite Projekte und Initiativen untersucht, um einen Gesamteindruck über das Angebot und aktuelle Projekte zu erhalten, welche Schnittstellen zu dem IDM.NRW Projekt aufweisen. Dies war besonders wichtig, um ggf. existierende Resultate von bestehenden Ansätzen in die Konzepterstellung IDM.NRW zu integrieren. Die Ergebnisse aus AP 2 wurden in einem Workshop, der am Standort Essen stattfand, vorgestellt und diskutiert. Weiterführende Diskussionen und Teilaufgaben konnten, aufgrund der „Corona-Situation“, nicht wie geplant in Bochum und Bielefeld durchgeführt werden, sondern sind in Form von Onlineworkshops erfolgt. Die Ergebnisse aus den

[1] S. 71-83

Befragungen sowie die resultierenden Anforderungen für ein FIDM sind in den nächsten Kapiteln 3 und 4 im Detail beschrieben.

Die Aufgaben und die weitere Vorgehensweise wurden im dritten Arbeitspaket (AP 3) festgehalten. Das AP 3 beinhaltete die Erarbeitung der Konzepte, die sich aus den Anforderungen der jeweiligen Einrichtungen und Services ergeben. Es wurden, in Anlehnung an bereits etablierte IDM-Prozesse und Funktionalitäten, Grobkonzepte erstellt und einem weiteren Onlineworkshop vorgestellt. Das sind *zentrale Personengruppen an Hochschulen*, *Evaluierung von Technologien*, die im Rahmen IDM genutzt werden, *Konsensschaffung in NRW* und *Gemeinsame NRW-Attribute*. Die Ergebnisse werden im Kapitel 5 näher vorgestellt.

Im vierten Arbeitspaket (AP 4) wurden weitere Schritte für jedes einzelne Grobkonzept definiert, welche im Folgeprojekt detailliert bearbeitet werden sollen. Diese Schritte beinhalten sowohl die Umsetzungsplanung der Konzepte hinsichtlich der direkten Nutzungsmöglichkeit für ausgewählte Services und Dienste als auch die grundsätzliche Einführung des FIDM in NRW und die zugehörigen Konzepte. Die Umsetzungsplanung beinhaltet neben der Einführung ebenfalls die Partizipationsplanung von Einrichtungen in NRW sowie die Verstetigung der Erkenntnisse und Inhalte des Projekts IDM.NRW. Wie die Umsetzung im Detail geplant wird, ist in Kapitel 6 hinterlegt.

Grundsätzlich ergeben sich aus der Machbarkeitsstudie FIDM neue Erkenntnisse zu relevanten Anforderungen an ein FIDM. Mittels der durchgeführten Arbeitspakete wurden eine gemeinsame Vorgehensweise und ein Voranschreiten in NRW entwickelt. Der Wissensgewinn sowie die Ergebnisse wurden Mitgliedern der DH.NRW im Rahmen von Workshops vorgestellt. Damit konnte ein regelmäßiger Austausch sichergestellt werden. Die Resultate tragen wesentlich zur Weiterentwicklung und Vereinheitlichung von Prozessen rund um das IDM bei. Prozesse werden ggfs. einmal entwickelt und können an diversen partizipierenden Einrichtungen der DH.NRW genutzt werden. Das gemeinsame Verständnis erhöht dabei die Durchlässigkeit bei der Prozessorganisation. Für die gegenseitige Serviceerbringung ist dies eine Voraussetzung. Neben den ermittelten Ergebnissen wurden auch weitere Bedarfe ermittelt, die im Folgeprojekt angegangen und umgesetzt werden sollen.

2.3. Rahmenwerk und Grundprinzipien des Projekts

In diesem Abschnitt werden zum einen das Rahmenwerk und zum anderen die Grundprinzipien des Projekts definiert. Diese sind wesentlich für die zielführende Durchführung der Machbarkeitsstudie und die erfolgreiche Zusammenarbeit. Die hier festgelegten Bestimmungen werden während der gesamten Projektlaufzeit eingehalten.

Bereits zu Beginn ist es sehr wichtig zentrale Eckpunkte festzuhalten und eine homogene Sichtweise auf das Projekt zu entwickeln. Beispielsweise hat sich die Projektgruppe bereits am ersten Tag darauf geeinigt, dass es in dem Projekt nicht um die Einführung eines zentralen IDM-Systems in NRW handelt. Demnach sind Eingriffe in die lokalen IDM-Systeme der einzelnen Einrichtungen in NRW keineswegs vorgesehen. Es geht vielmehr um die Prozessebene und die Kooperationen zwischen Einrichtungen. Demnach wird der Fokus aus Bereiche zwischen den Hochschulen gelegt, um ein föderiertes Identity Management in NRW zu ermöglichen. Um geeignete Prozesse auszugestalten und diese technisch zu realisieren, ist die Berücksichtigung und Wahrnehmung der IDM-Systemlandschaft eine Grundvoraussetzung. In Anbetracht der heterogenen IDM-Landschaft in NRW sind ohne eine ausführliche Bedarfs- und Anforderungsanalyse keine fundierten Rückschlüsse abzuleiten.

Aufgrund der Komplexität und der Vielfalt des Bereiches IDM, ist als erstes die Schaffung eines kleinsten gemeinsamen Nenners in NRW notwendig. Diesbezüglich ist eine Priorisierung der Anforderungen, sowie Einhaltung von festgelegten Arbeitsabläufen erforderlich. In Anbetracht dessen ist dringend zwischen Machbarem und Nicht-Machbarem zu unterscheiden, um nicht vom Projektziel abzuweichen. Hierfür ist eine Identifikation der technischen Umgebung in NRW dringend zu empfehlen. Insbesondere um keine Parallelstrukturen zu entwickeln und vor allem die Passfähigkeit der entwickelten Konzepte zu bestehenden Strukturen zu gewährleisten. Des Weiteren ist es von großem Vorteil bestehende Standards zu berücksichtigen und Konzepte zu erstellen. Zuzüglich wurde sich innerhalb des Projekts mit bestehenden Services (Sciebo, HPC, etc.) auseinandergesetzt, um vorhandene Techniken und Konzepte mit zu berücksichtigen. Nicht zuletzt hat sich die Projektgruppe dazu entschieden entsprechende Arbeitskreise, Veranstaltungen und Initiativen (edu-ID, MyAcademicID, SaxID, etc.) wahrzunehmen bzw. zu verfolgen. Auch hier ist das Ziel kompatible Lösungsansätze zu entwickeln und klare Anforderungen an teilnehmende Einrichtungen zu stellen.

Eine weitere sehr wichtige Festlegung, die in jedem Fall Berücksichtigung finden muss, ist das „Keep It Short and Simple-Prinzip“ (KISS). Dies ein Grundprinzip, welches in jeder Projektphase daran erinnern soll, dass wir uns bei der Erstellung der Lösungsansätze nicht in komplexen Strukturen verirren möchten. Das Projektziel und Aufgabenpakete müssen klar umrissen sein, um ausufernde Erfassungen sowie Bewertungen zu vermeiden. Demnach sollen die entwickelten Lösungskonzepte so „short and simple“ wie möglich sein, um eine schnelle und einfache Umsetzung zu gewährleisten, sodass auch kleine Einrichtungen mit wenig Aufwand einen großen Nutzen generieren. In Anbetracht der bisherigen Festlegungen hat die Projektgruppe gemeinsam das Projektziel „Identifikation gemeinsamer technischer und

organisatorischer Maßnahmen zur Nutzung entfernter Services in NRW basierend auf lokalen Identitäten“ definiert.

Die Kommunikation nach außen in Form einer transparenten Darstellung des Vorgehens und der Lösungen bei den Inputgruppen ARNW, DVZ, sowie den Kunst- und Musikhochschulen (KUMUs) ist unerlässlich. Aufgrund dessen wurde bereits zu Beginn des Projektes aus den festgelegten Grundprinzipien Mission-Statements entwickelt und an die Inputgruppen in NRW weitergeleitet.

Nicht zuletzt hat sich die Projektgruppe darauf geeignet, durch die Erarbeitung der Lösungskonzepte einen Beitrag zu kooperativer Erbringung von Services zu leisten und die Forschung und Lehre zu unterstützen. Die genaue Formulierung eines Angebots zur Unterstützung, insbesondere für kleine Einrichtungen, wird im Hauptantrag erfolgen. Dass aus den Grundprinzipien entstandene Rahmenwerk lenkt das Projektvorhaben in die festgelegte Richtung und verhilft zur zielführenden und erfolgreichen Durchführung des Projekts.

3. Status Quo Erfassung

In dem ersten Abschnitt dieses Kapitels (3.1) werden zunächst die Ergebnisse aus der Onlineumfrage zur Status Quo Erfassung der IDM-Systemlandschaft in NRW vorgestellt. Der nächste Abschnitt (3.2) beschreibt die Status Quo Erfassung der bundesweiten IDM-Systemlandschaft. Diese Betrachtung ist wichtig, um Gemeinsamkeiten sowie Unterschiede festzustellen und dadurch Profite für das Projekt IDM.NRW zu erzielen. Aufgrund der hohen Komplexität des IDM Themenfelds ist es relevant die bundesweite IDM-Entwicklung im Blick zu behalten, aber auch um die bundesweite Nutzung von Services zu ermöglichen. Neben der IDM-Systemlandschaft ist die Betrachtung der Servicelandschaft in NRW relevant. Der Abschnitt 3.3 stellt zum einen das Serviceportfolio und zum anderen die Ergebnisse aus der Expertenbefragung mit den Servicebetreibern vor. Damit einhergehend ist, die in Abschnitt 3.4 beschriebene, Untersuchung bereits etablierter Projekte bzw. Initiativen auf Bundesebene unerlässlich. Die Erfassung und Beobachtung etablierter bzw. geplanter Projekte oder Initiativen ist für das Projekt IDM.NRW wichtig, um eine hohe Kompatibilität der Konzepte zu gewährleisten.

3.1. IDM-Systemlandschaft NRW

In diesem Abschnitt werden die Ergebnisse aus der Onlinebefragung und der IDM-Nacherfassung dargestellt. Wie im Abschnitt 2.2 bereits erläutert wurde mithilfe dieser Methoden die IDM-Systemlandschaft in NRW erfasst und gleichzeitig Bedarfe und

Anforderungen an ein FIDM abgefragt. Der Aufbau der Onlineumfrage sowie der Experteninterviews zur Nacherfassung, die wichtigsten Ergebnisse und die zentralen Erkenntnisse aus den beiden Befragungen werden im Folgenden näher beschrieben. Die Gesamtauswertung der Onlineumfrage sowie die Expertenbefragungen sind im Anhang nachzulesen. Die Zielgruppe der Onlineumfrage waren Einrichtungen, die ein lokales IDM-System betreiben und sich mit den gängigen Fragestellungen rund um das Themengebiet IDM beschäftigen. In NRW gibt es 35 Einrichtungen, die ein lokales IDM-System betreiben. An der Onlineumfrage nahmen 25 Einrichtungen teil, sodass eine recht hohe Rücklaufquote von 71% erreicht wurde.

Die Onlineumfrage[2] umfasst insgesamt 46 Fragen, die sich in die folgenden sieben Kategorien einteilen lassen: IST-Analyse, IDM-System, IDM-Schnittstellen, IDM-Daten, IDM-Authentifizierung, IDM-Autorisierung und Hochschulübergreifende Kooperationen. Bei der IST-Analyse geht es um Fragen wie das Vorhandensein eines IDM-Konzepts an der Einrichtung, Ressourcenbereitstellung für IDM-Themen und den Rückhalt bzgl. IDM Themen durch die Hochschulleitung. In der zweiten Kategorie werden das Vorhandensein eines IDM-Systems und der Produktname erfragt. Die Kategorie IDM-Schnittstellen beschäftigt sich mit der Frage, welche Quell- und Zielsysteme es in den Einrichtungen gibt und welche an das IDM-System angeschlossen sind. Des Weiteren können die Befragenden die Quell- und Zielsysteme nach ihrer Qualität bewerten und Auskunft über die Regulierung des Datenaustausches geben. Außerdem haben die Teilnehmenden die Möglichkeit ihre Sicherheitsbedenken, Schnittstellen nach außen anzubieten, zu äußern. In der Kategorie IDM-Daten finden Fragen zur Eindeutigkeit der Identitäten, sowie der Identitätsprüfung in den Einrichtungen Platz. Des Weiteren werden Fragen zu Funktionsidentitäten, zum Identitäts-Lifecycle und die Weitergabe von Uni-Kennungen an Drittsysteme gestellt. Die nächste Kategorie befasst sich mit Fragen zu Authentifizierungssystemen und solcher die als *Authentification as a Service* (AaaS) angeboten werden. Die Kategorie IDM-Autorisierung beinhaltet Fragen zu zentralen Personengruppen und Konzepten für Rollen-, Rechte- und Gruppenverwaltung. Die siebte Kategorie erfragt hochschulübergreifende Kooperationen als Anbieter/ Nutzender. Zudem wird erfragt, ob es an den Einrichtungen bereits Konzepte gibt, den Zugriff auf Nicht-Webdienste föderativ zu ermöglichen. Des Weiteren beschäftigt sich die Kategorie mit der Frage welche Anforderungen an Services gestellt werden, damit diese gut über das eigene IDM-System genutzt werden können. Zum Abschluss werden die Teilnehmenden gefragt, ob der Bedarf eines föderativen Identity Managements gesehen wird.

Nach der Auswertung und Analyse der Onlineumfrage wurden die Erkenntnisse über die IDM-Systemlandschaft in NRW festgehalten. Um erweiterte Rückschlüsse zu ziehen und

[2] S.61-67

bestehende Erkenntnisse zu unterstreichen, wurden im Rahmen von Experteninterviews Telefon- und Videokonferenzen mit den teilnehmenden Hochschulen durchgeführt. Dazu wurde ein Fragebogen, bestehend aus neun offenen und geschlossenen Fragen, erstellt.

Als erstes wurden die teilnehmenden Hochschulen gefragt, ob derzeit die Einführung eines neuen IDM-Systems geplant ist. Falls dem so ist, konnten die Befragenden Auskunft über das Produkt geben. Bei der zweiten Frage hatten die Befragenden die Möglichkeit anzugeben, ob in der jeweiligen Hochschule der Single-Sign-On-Dienst Shibboleth betrieben wird oder nicht. Als nächstes wurde gefragt, ob die Hochschulen über ein Trouble-Ticket-System verfügen und ob dieses an das IDM-System der Hochschule angeschlossen ist. Die IDM-Prozesse laufen in jeder Hochschule unterschiedlich ab. Um herauszufinden in welchem Maße noch händisches Eingreifen in IDM-Prozesse erfolgt und vor allem durch welche Fachabteilungen, wurde auch diese Fragen im Rahmen der Experteninterviews gestellt. Zuzüglich wurde als nächstes gefragt, welche Prozesse explizit nicht durchautomatisiert laufen. Bei der sechsten Frage, konnten die Befragenden Angaben über ihr Know-How bezüglich Webschnittstellen, wie SOAP, REST, etc. machen. In der Onlineumfrage wurde erfragt, ob die Teilnehmenden Sicherheitsbedenken haben Schnittstellen nach außen anzubieten. Im Rahmen der Experteninterviews wurde nach konkreten Sicherheitsbedenken gefragt, um dementsprechende Lösungen im Hauptprojekt zu konzipieren. Die achte Frage bezog sich auf Funktionsidentitäten und ob diese von normalen Identitäten unterscheidbar sind. In der Onlineumfrage wurde ermittelt, ob es bereits an den Hochschulen Versuche gab, Services föderativ anzubieten bzw. zu nutzen. Die Teilnehmenden konnten während der Experteninterviews Angaben machen, ob und warum diese Versuche bislang gescheitert sind. Nachdem der Aufbau beider Befragungsmethoden vorgestellt wurde, sollen im Weiteren die Kernaussagen dargestellt werden. Da die Befragungen aufeinander aufbauen und sich unterstützen, werden die Ergebnisse als Gesamtauswertung beschrieben.

Ein Ergebnis aus den Befragungen zeigt, dass IDM als Konzept in den Einrichtungen zentral verankert ist. Hier haben alle teilnehmenden Hochschulen angegeben, dass IDM als Konzept bereits vorhanden ist. Ein weiteres sehr wichtiges Ergebnis zeigt die untenstehende Abbildung 1. Während fast 61 % der Teilnehmenden angaben, dass im Bereich IDM der Rückhalt durch die Hochschulleitung „sehr stark bis stark“ einzustufen ist, gaben ca. 39 % der teilnehmenden Einrichtungen an, dass Rückhalt eher „wenig stark“ ist. Damit verbunden machen die Teilnehmenden Angaben zu fehlenden Ressourcen im Bereich IDM, wie z.B. Personalmangel.

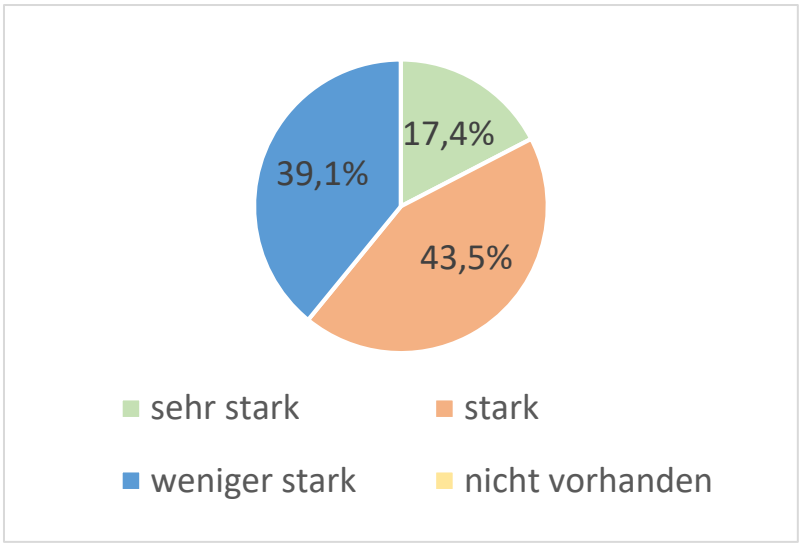

Abbildung 1: Wie stark ist der Rückhalt von IDM durch die Hochschulleitung?

Ein weiteres sehr interessantes Ergebnis ist, dass alle teilnehmenden Hochschulen ein IDM-System haben. Welches Produkt am häufigsten genannt wurde, zeigt die untenstehende Abbildung 2. Demnach sticht als führendes IDM-System in NRW das Produkt MicroFocus hervor. In der Onlinebefragung hatten sechs Hochschulen angegeben, dass sie eine Eigenentwicklung betreiben. Von diesen sechs Hochschulen haben drei während der Experteninterviews gesagt, dass ein Wechsel zu MidPoint (OpenSource Produkt) geplant ist.

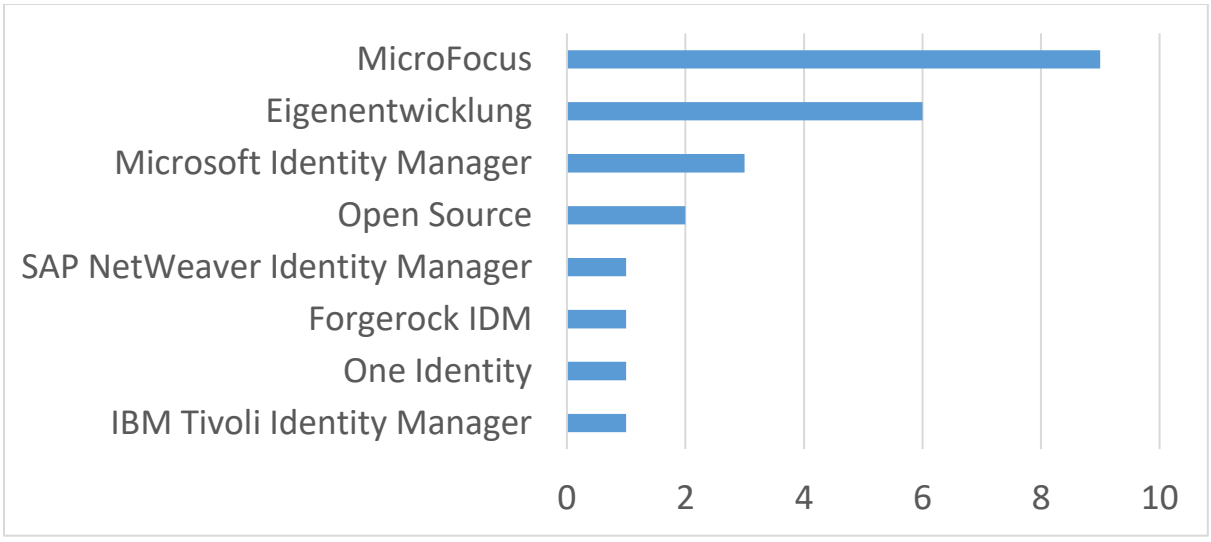

Abbildung 2: Welches IDM-System ist im Einsatz?

Eine relevante Kernaussage aus den Befragungen zeigt, dass überwiegend eine hohe Datenqualität in den Einrichtungen existiert. Dies wird u.a. durch den mindestens einmal täglichen Datenaustausch verstärkt (siehe Abbildung 3).

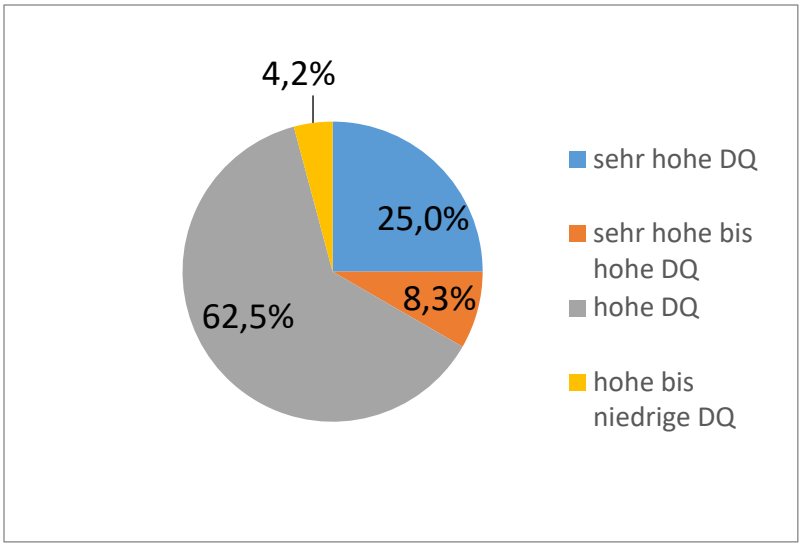

Abbildung 3: Wie ist die Datenqualität (DQ) der Systeme in NRW?

Ein weiteres Ergebnis zeigt, dass ca. 71 % der Einrichtungen regelmäßiges händisches Eingreifen in IDM-Prozesse durch den Support oder das IDM-Team vornehmen müssen. An dieser Stelle lässt sich schlussfolgern, dass der Grad der Automatisierung gesteigert werden kann (siehe Abbildung 4).

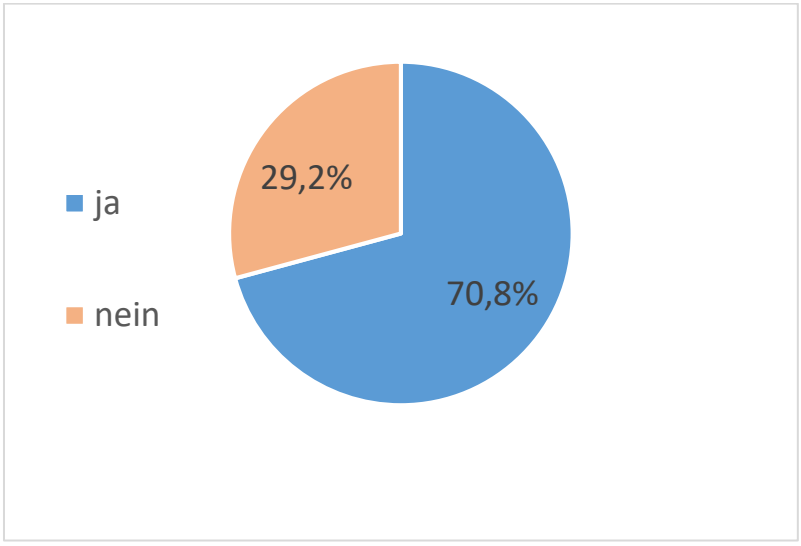

Abbildung 4: Gibt es Prozesse im IDM, die regelmäßiges händisches Eingreifen durch den Support oder das IDM-Team erfordern?

Im Rahmen der Experteninterviews gaben die Teilnehmenden zusätzlich an, dass händisches Eingreifen vermehrt durch die IDM-Fachabteilung und den IT ServiceDesk erfolgt (siehe Abbildung 5).

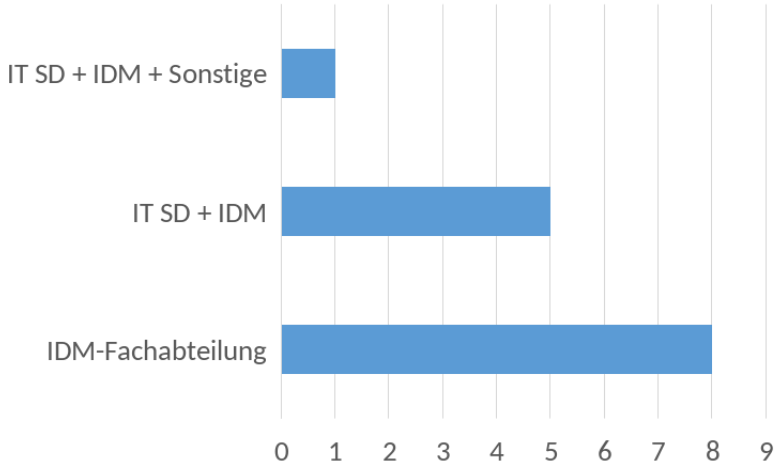

Abbildung 5: Von wem wird händisch in IDM Prozesse eingegriffen?

Zudem wurde gefragt, welche Prozesse noch nicht zu vollautomatisiert sind. Die Abbildung 6 zeigt die Übersicht aller Prozesse, die händisches Eingreifen erfordern. Demnach sind die meist genannten Prozesse die Vergabe/ Löschung von Kennungen und Mailadressen/-accounts, Berechtigungsvergabe und Entzug, u.a. bei Gruppenmitgliedschaften und Matching/ Zusammenlegung von Identitäten. Hier können Prozessen entwickeln werden, um das händische Eingreifen zu minimieren.

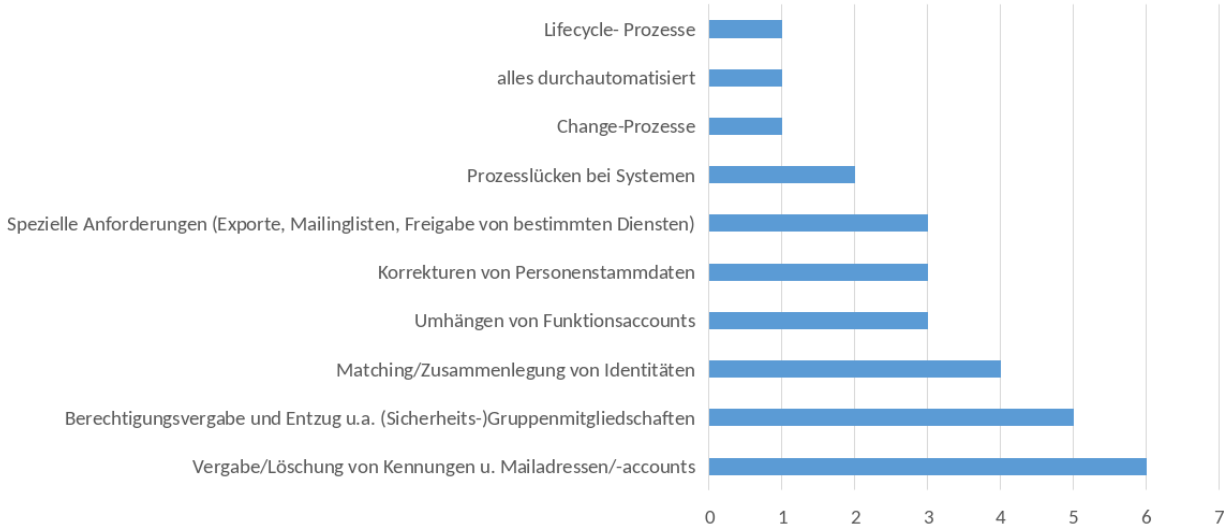

Abbildung 6: Welche Prozesse sind nicht zu 100% durchautomatisiert?

Des Weiteren vertreten knapp 96 % der Teilnehmenden die Meinung, dass ein föderatives Identity Management in NRW sinnvoll ist. Gleichzeitig äußern 96 % der Teilnehmenden ihre Sicherheitsbedenken Schnittstellen nach außen anzubieten (siehe Abbildung 7). An dieser Stelle wird deutlich, dass IDM ein sicherheitskritisches System ist und dass Einrichtungen deshalb vermehrt auf Datensparsamkeit achten.

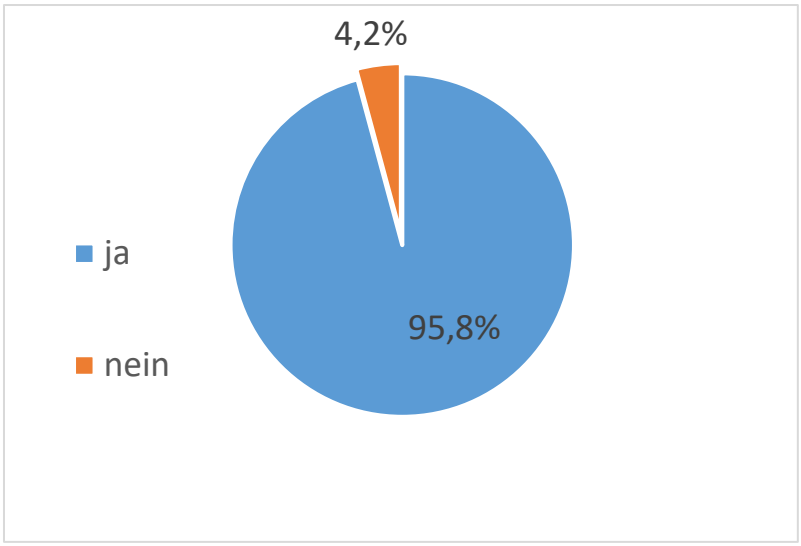

Abbildung 7: Gibt es an Ihrer Hochschule Sicherheitsbedenken Schnittstellen nach außen anzubieten?

In den Experteninterviews gaben die Teilnehmenden zusätzlich Auskunft über ihre konkreten Sicherheitsbedenken (siehe Abbildung 8). Demnach sind Datenschutz, Missbrauch, IT-Sicherheit, Denial-of-Service Attacke und unsichere Schnittstellen die meist genannten Bedenken. Des Weiteren wurden Bedenken zu Datenqualität, Datenverlust und unautorisierter Zugriff auf Services geäußert.

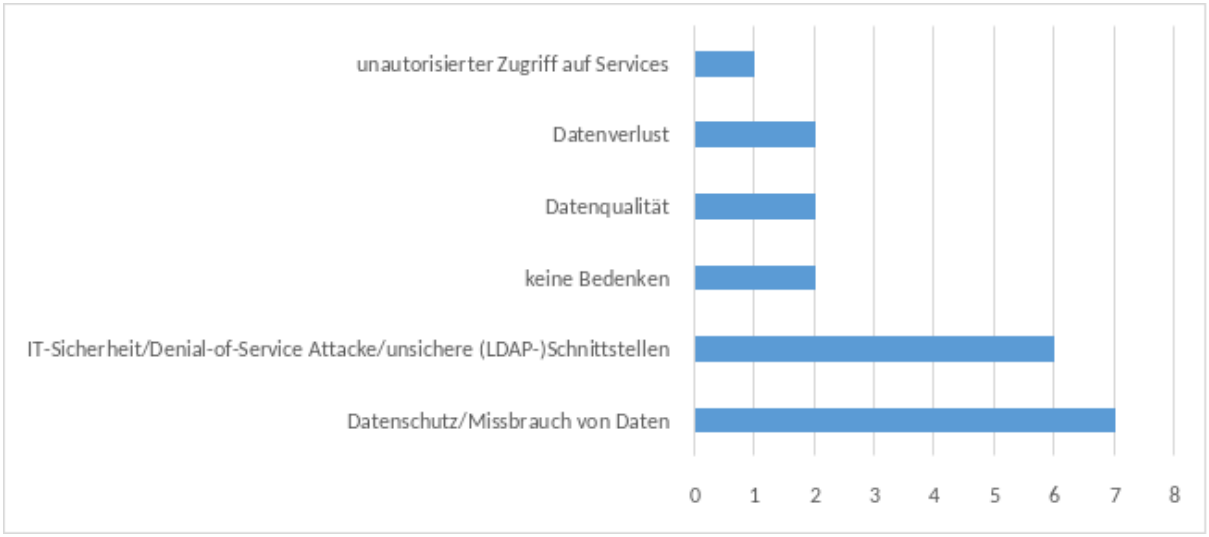

Abbildung 8: Sicherheitsbedenken Schnittstellen nach außen anzubieten

Im weiteren Verlauf werden die Auswertungen zu den Fragen bzgl. Eindeutigkeit von Identitäten und Lifecycle-Prozessen betrachtet. Wie in Abbildung 9 zu erkennen ist, werden Identitätsüberprüfungen in den Einrichtungen verstärkt über die Personalausweiskontrolle durchgeführt. Dadurch wird eine hohe Eindeutigkeit von Identitäten und Stammdaten gewährleistet.

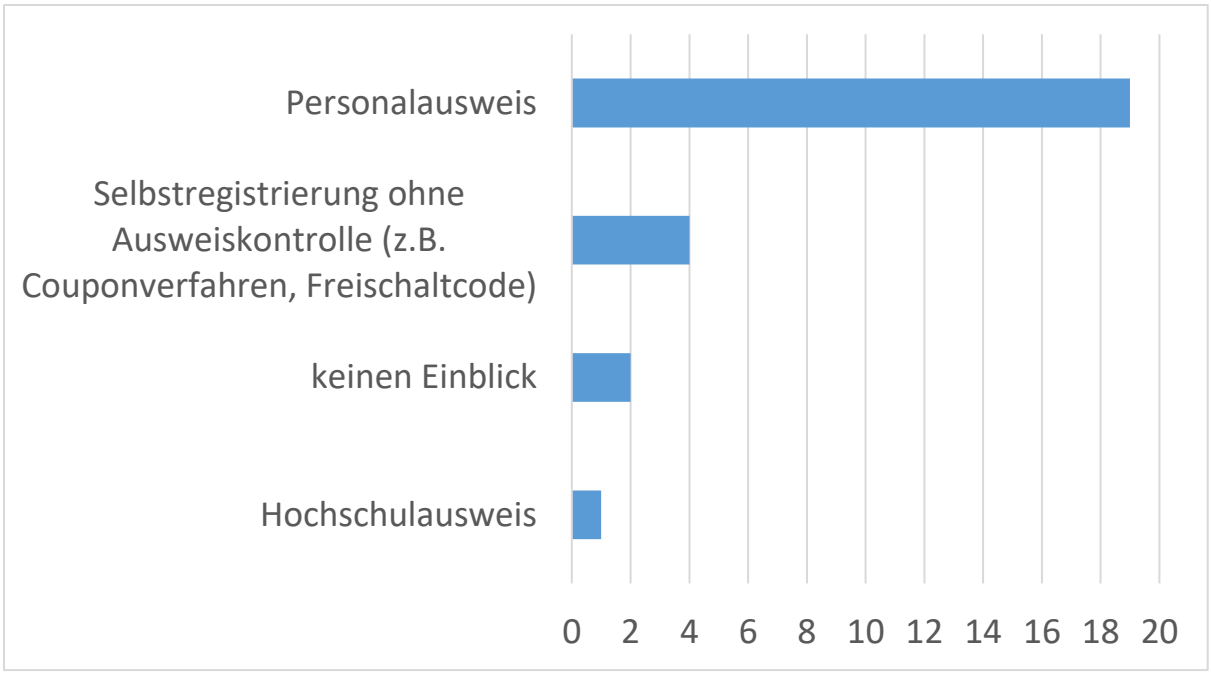

Abbildung 9: Wie findet die Registrierung bzw. die Identitätsüberprüfung statt?

Die Analysen zu den Lifecycle-Prozessen ergeben, dass der Identitäts-Lifecycle in den Einrichtungen zu 78 % automatisiert, zu 22 % manuell und zu 7 % gar nicht erfolgen (siehe Abbildung 10).

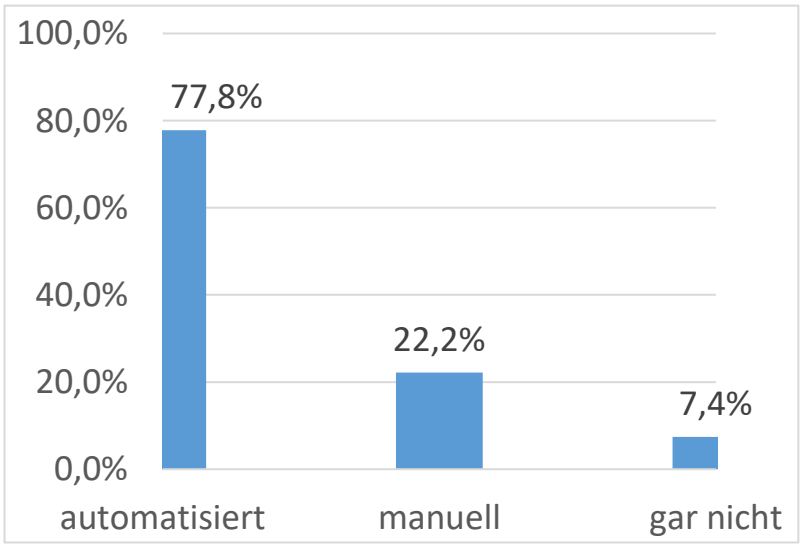

Abbildung 10: Wie ist der Identitäts-Lifecyle an Ihrer Hochschule geregelt?

Für die Teilnehmenden, die einen automatisierten und/ oder manuellen Identitäts-Lifecycle angegeben haben, wurde eine erweitere Frage zur Geschwindigkeit des Prozesses gestellt. Die Abbildung 11 zeigt, dass ca. 71 % der Befragenden angaben, dass der Identitäts-Lifecycle zeitnah erfolgt. Ca. 33 % der Einrichtungen geben an einen verzögerten Lifecycle-Prozess zu haben.

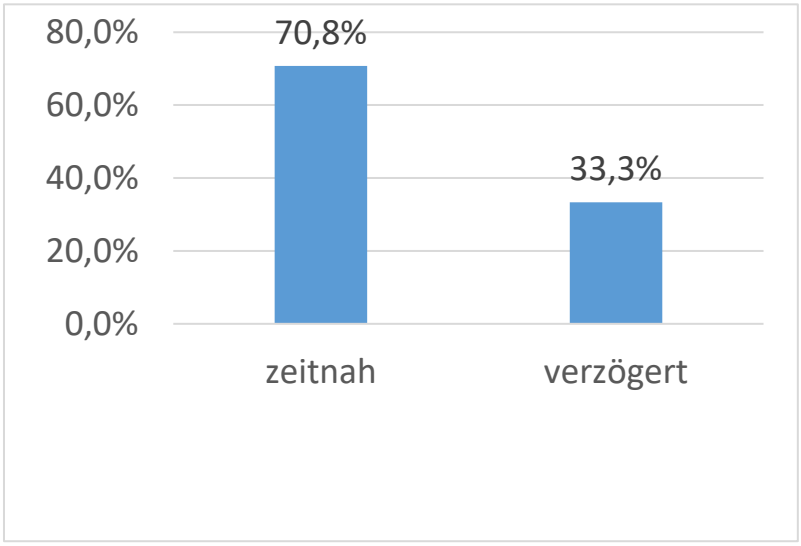

Abbildung 11: Falls der Identitäts-Lifecycle automatisiert oder manuell geregelt ist, wie schnell ist dieser?

Ein weiteres Ergebnis ist, dass es an einzelnen Einrichtungen Funktionsidentitäten gibt, die von einer oder mehreren Personen genutzt werden (siehe Abbildung 12). Bei der Frage, ob diese von anderen Identitäten unterscheidbar sind oder nicht, gaben 50 % ja und 50 % nein an.

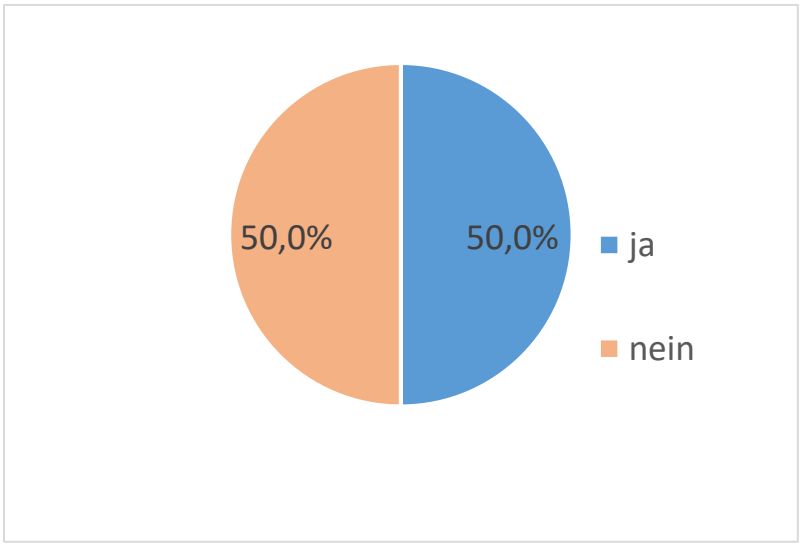

Abbildung 12: Werden Funktionsidentitäten von einer oder mehreren Personen genutzt?

Eine weitere Kernaussage zeigt, dass sich als Basistechnologien in NRW deutlich der Active Directory (AD), das Lightweight Directory Access Protocol (LDAP) und Shibboleth herausgestellt haben (siehe Abb.13). Fast jede Hochschule betreibt einen Identity Provider (IdP) und ist auch Mitglied in der DFN-AAI. Security Assertion Markup Language (SAML) ist hier die dominierende Basistechnologie und reicht aktuell als Struktur aus. Erkenntnisse aus den Experteninterviews unterstützen diese Ergebnisse. Denn alle Befragenden gaben an, dass sie Shibboleth kennen und die jeweilige Hochschule über eine DFN-AAI Anbindung verfügt.

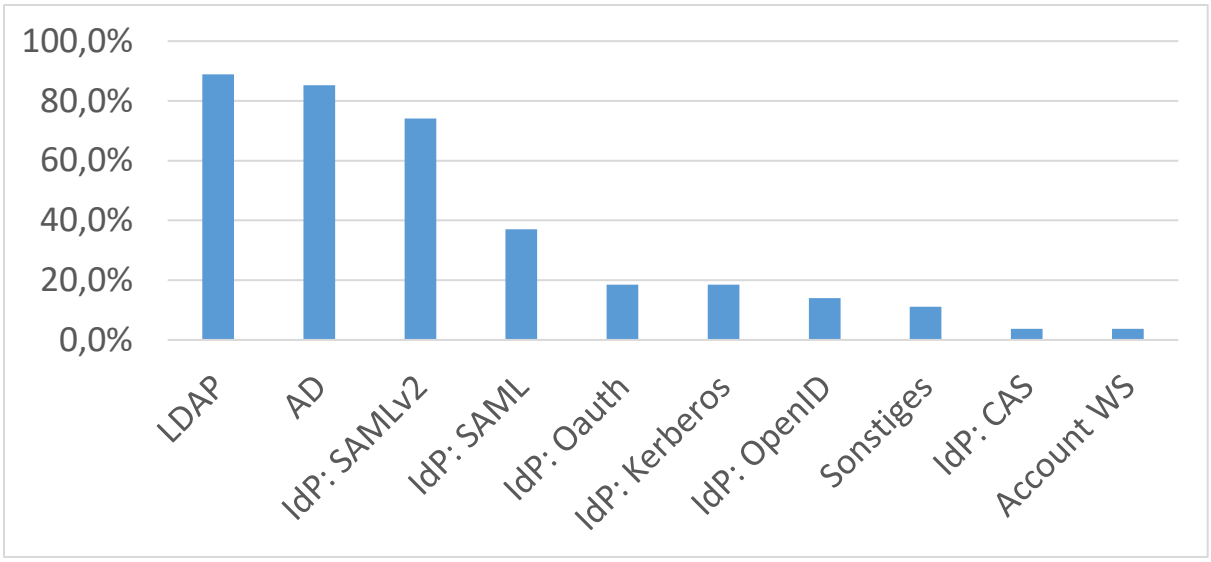

Abbildung 13: Welche Authentifizierungssysteme gibt es an Ihrer Hochschule?

Des Weiteren wurden in den Experteninterviews Kompetenzen zu Webservices erfragt. Die untenstehende Abbildung zeigt, dass die teilnehmenden Hochschulen über Kompetenzen sowohl in SOAP als auch in REST Schnittstellen verfügen (siehe Abbildung 14).

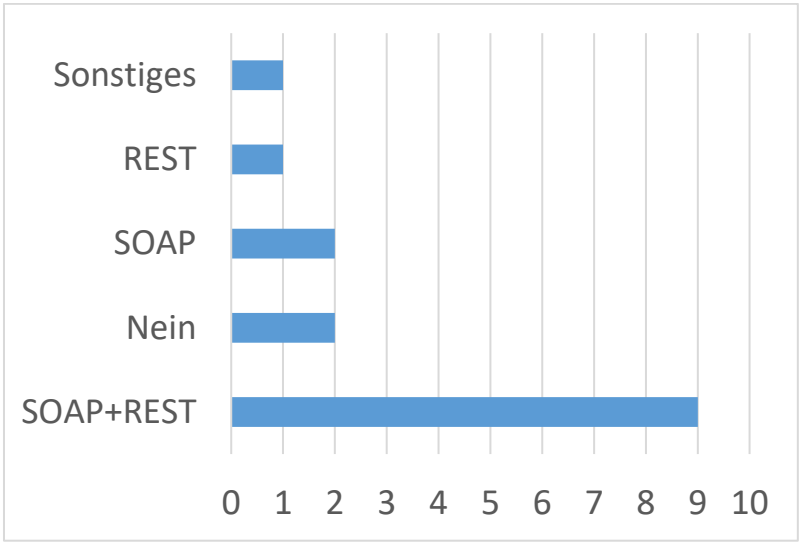

Abbildung 14: Liegen Kompetenzen/ Know How zu Webservices vor?

Weitere Auswertungen machen deutlich, dass es in den Einrichtungen diverse zentrale Personengruppen gibt. Nicht nur die Anzahl und die Benennung sind verschieden, sondern auch die Definition dieser Personengruppen unterscheidet sich. Laut den Auswertungen sind die am häufigsten verwendeten Personengruppen in NRW: Studierende, Mitarbeitende, Gäste/ Externe, Lehrbeauftragte/ Lehrende/ Lehrpersonal, Ehemalige Mitarbeitende/ Person Altbestand, Ehemalige Studierende.[3] Des Weiteren wurde in der Onlineumfrage ermittelt, ob

[3] Siehe im Anhang unter Auswertung der Onlineumfrage.

die teilnehmenden Hochschulen Konzepte für eine Rollen-/ Rechte-/ Gruppenverwaltung haben (Abbildung 15). Ca. 25 % der Einrichtungen gaben an, dass ein Konzept für eine Rollen-/ Rechte-/ Gruppenverwaltung in der jeweiligen Hochschule fehlt. Dahingegen gaben 75 % an, ein solches Konzept etabliert zu haben. An dieser Stelle ist jedoch anzumerken, dass die Konzepte unterschiedlich konzipiert und umgesetzt werden. Hieraus lässt sich schlussfolgern, dass es in NRW keine einheitlichen zentralen Personengruppen und Konzepte für Rollen-/ Rechte-/ Gruppenverwaltung gibt. Insbesondere bei diesem Thema ist eine Homogenisierung in NRW wünschenswert und für die Einführung eines föderierten IDMs von Vorteil.

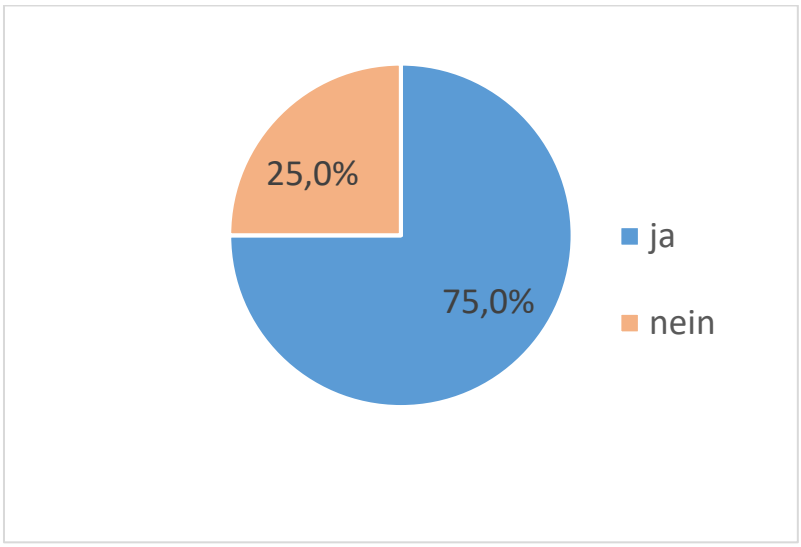

Abbildung 15: Gibt es eine Rollen-/Rechte-/ Gruppenverwaltung?

Eine weitere sehr wichtige Erkenntnis ist, dass es bislang in NRW keinen einheitlichen Vorgang darüber gibt, wie Identitäten bei einer hochschulübergreifenden Kooperation übermittelt werden. Ein Großteil der Antworten wurde gemäß einem Clustering-Verfahren ausgewertet. Demnach erfolgt die Übermittlung gemäß verschlüsseltem Austausch via CSV (Comma-separated values) und SAML oder es erfolgt eine manuelle Übermittlung.

Des Weiteren kann festgehalten werden, dass es bisher keine Lösung für einen föderativen Zugriff von Nicht-Webdiensten gibt. Jede Hochschule hat eine DFN-AAI Anbindung und ist mit dem Authentifizierungs- und Autorisierungsverfahren Shibboleth vertraut. Jedoch hat keine der teilnehmenden Hochschulen ein Konzept für einen Authentifizierungsmechanismus, der den föderativen Zugriff auf Nicht-Webdienste, wie beispielsweise den HPC Cluster an der RWTH Aachen, möglich macht (siehe Abbildung 16).

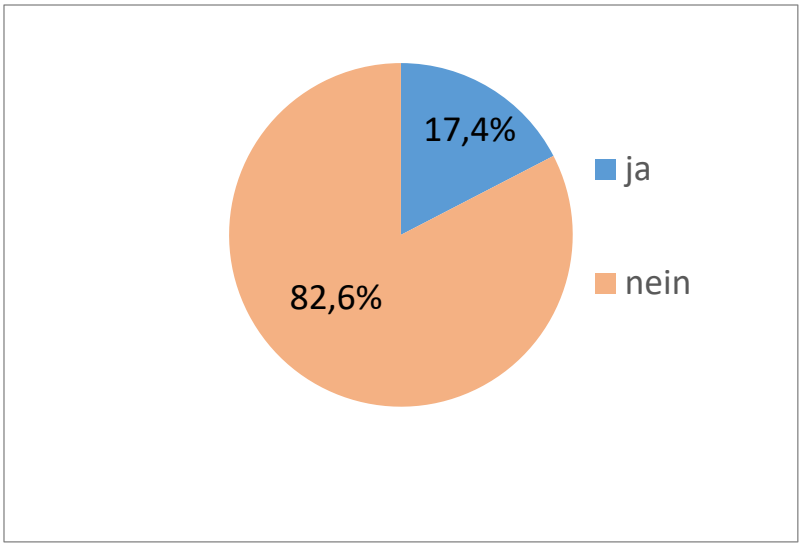

Abbildung 16: Gibt es an Ihrer Hochschule ein Konzept "Nicht Web-Dienste" föderativ zugreifbar zu machen?

Es wurden zwar Versuche gestartet, um hochschulübergreifend Dienste an das IDM anzubinden, jedoch sind diese allen Angaben der Teilnehmenden nach gescheitert (siehe Abbildung 17). Hierzu gibt es verschiedene Gründe, wie Ressourcenkapazitäten, Performance, Koordinationsschwierigkeiten bzw. organisatorische Hürden oder unterschiedliche technische Anforderungen/ strategische Vorgaben. Nichtsdestotrotz zeigen die Versuche, dass ein Interesse für diese Thematik besteht und dadurch ergibt sich für das Projekt IDM.NRW ein gewisses Potenzial.

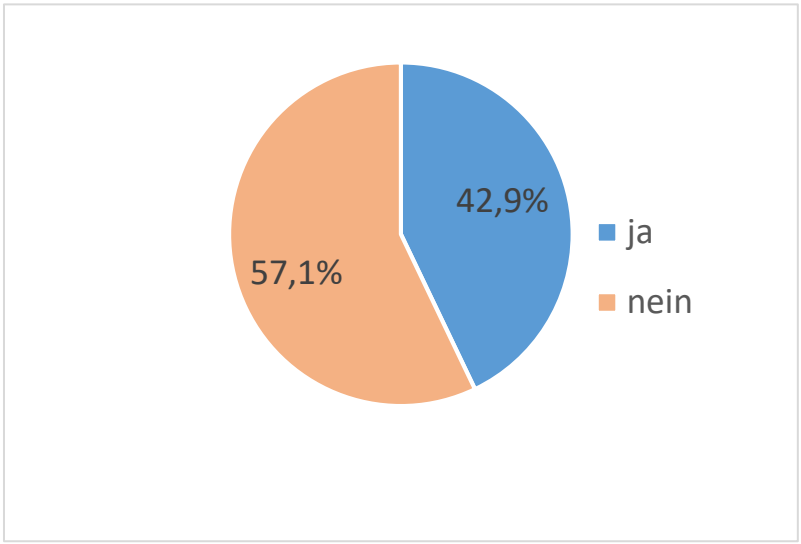

Abbildung 17: Gibt es Dienste, bei denen die Anbindung an das IDM bisher gescheitert ist?

Eine wichtige Frage, die in der Onlineumfrage gestellt wurde, ist die Frage nach den Anforderungen für ein föderiertes IDM. Hierzu wurden sehr unterschiedliche Antworten eingereicht. Diese wurden anhand eines Clustering-Verfahrens in Kategorien unterteilt. Die in NRW als relevanten Anforderung für die Realisierung eines föderativen Identity Management genannten Themen sind: Sicherheitsstandards, eindeutige Zielgruppen-Definition, Standard

Schnittstellen, Gemeinsame Attribute in NRW, Technisches Know-How und eine Gruppen-/ Rollen-/ Rechteverwaltung. Der Hintergrund der Themenbereiche und Lösungsansätze im Rahmen des Projekts IDM.NRW werden in Kapitel 4 näher erläutert.

Ein weiteres aussagekräftiges Resultat wird in der untenstehenden Abbildung 18 deutlich. Demnach sehen ca. 96 % der teilnehmenden Hochschulen den Bedarf hochschulübergreifende Services anzubieten bzw. zu nutzen. Daraus lässt sich schlussfolgern, dass die Hochschulen in NRW die Relevanz für hochschulübergreifende Services erkannt haben und ein föderiertes IDM wünschen.

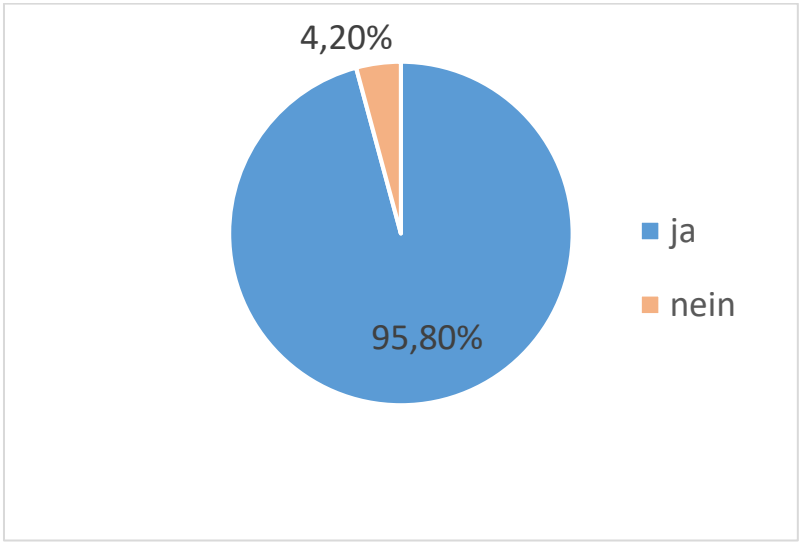

Abbildung 18: Sehen Sie den Bedarf hochschulübergreifend Services zu nutzen bzw. anzubieten?

Final kann festgehalten werden, dass hochschulübergreifende Services in NRW aktuell im Trend sind bzw. zukunftsträchtig sein werden. Nicht nur seitens der DH.NRW sondern auch durch die Unterstützung des MKW werden zahlreiche Serviceprojekte initiiert und teilweise in NRW angeboten. Durch die steigende Anzahl der Services in NRW steigen die Anforderungen an lokale IDM-Systeme. Wie diese Anforderungen im Detail aussehen, ist in Kapitel 4 dargestellt. Es gibt derzeit nicht viele Services die hochschulübergreifend genutzt werden (können), das Interesse seitens der Einrichtungen ist aber durchaus vorhanden. Genau hier greift das Projekt IDM.NRW ein, um eine möglichst schnelle und einfache Umsetzung zu konzipieren, sodass auch kleine Einrichtungen mit geringem Aufwand einen größtmöglichen Nutzen ziehen können. Anhand der Ergebnisse wird erneut deutlich, dass IDM kein einmaliges Projekt ist, sondern eine Daueraufgabe, die stetig Prozessaktualisierungen mit sich zieht.

3.2. IDM-Systemlandschaft bundesweit

In diesem Abschnitt wird die bundesweite IDM-Systemlandschaft näher beschrieben. Es lässt sich festhalten, dass alle Rechenzentren von Hochschulen in der Bundesrepublik ein

Identitätsmanagement betreiben. Ein fachlicher Austausch für das Thema erfolgt über den ZKI-Arbeitskreis "Identity und Access Management" der früher "Arbeitskreis Verzeichnisdienste" hieß. Die Treffen waren bislang halbjährig und beinhaltet Best-Practice-Vorträge aus den eigenen Reihen sowie Vorträge von eingeladenen Fachleuten (z.B. zu Rechtsfragen) und Firmenvorträgen.

Immer wiederkehrende Themen der Treffen sind:

- Onboardingprozesse (Ausrollen von Zugangsdaten)
- Offboarding (Entzug von Berechtigungen)
- Student-Life-Cycle
- Rollen und Rechte
- Genehmigungsworkflows
- Selfcare
- Umgang mit Personen, die nicht Studierende oder Mitarbeitende sind. (Graubereich)
- Authentification as a Service (AAAS)
- Passwortregeln und Zweifaktorauthentifizierung
- Kontaktmanagement (Telefonbuch)
- Datenschutz
- Bedeutung der Organisationstruktur für das Identitätsmanagement
- Protokolle, Techniken und Software

Die Realisierung des Identitätsmanagements an den einzelnen Hochschulen ist höchst unterschiedlich. Das betrifft sowohl die eingesetzte Software als auch die Art und Intensität, wie das Identity Management in die Prozesse der Hochschule eingebunden ist. Eine systematische Übersicht gibt es nicht. Im ZKI-Arbeitskreis wurde vor Jahren der Versuch gemacht, eine solche Übersicht zu erstellen. Die Angaben der jeweiligen Hochschulen wurden in einem Wiki von einem Arbeitskreismitglied der Hochschule gemacht. Wir haben den für uns relevanten Inhalt herausgezogen.[4] Es muss beachtet werden, dass die Angaben unterschiedlich aktuell sind. Dennoch ergibt sich ein ungefähres Bild darüber, welche Systeme im Einsatz sind:

[4] Siehe Anhang unter IDM-ZKI, S.69-81.

- MicroFocus/NetIQ/Novell (verbreitet, wegen einzelner Landeslizenzen)
- Microsoft Forefront Identity Manager
- OpenIDM (vielfach als Nachfolger von SUN-Identity Manager)
- Midpoint (aktuell beliebt bei Hochschulen, die sich neu orientieren)
- SAP-IDM
- weitere kommerzielle Systeme, die (an den Hochschulen) nur einmal eingesetzt werden
- Eigenentwicklungen der Hochschulen
- Eigenentwicklungen externer Dienstleister

Grundsätzlich muss noch folgendes angemerkt werden:

- Meist werden auch die final nutzbaren (extern und intern) IDM-Systeme durch eigenentwickelte Komponenten ergänzt.
- Vielfach sind Altsysteme noch zusätzlich im Betrieb.

Eine direkte Zusammenarbeit von Hochschulen beim Thema IDM gibt es nur vereinzelt; z.B. in Thüringen oder in Städten mit mehreren Hochschulen. Ein gemeinsamer Nenner zu dem sich ein Großteil aller Hochschulen kommittet haben, ist die Teilnahme an der Föderation DFN-AAI.

3.3. Servicelandschaft NRW

In Abschnitt 3.1 und 3.2 wurden aus den Status Quo Erfassungen der bundesweiten und landesweiten IDM-Systemlandschaft Anforderungen an ein FIDM definiert. Auf der anderen Seite müssen Anforderungen auf Serviceseite abgefragt werden. Denn diese können je Service unterschiedlich komplex sein. Um die Anforderungen zu identifizieren, wurde im ersten Schritt ein Serviceportfolio mit Diensten (DH.NRW Dienste bzw. Projekte und hochschulinterne Dienste) aufgestellt, die im Rahmen eines FIDM hochschulübergreifend genutzt bzw. angeboten werden können. Nach Identifizierung der möglichen Services, wurden Experteninterviews mit Servicebetreibern durchgeführt. Hierzu wurde im Vorfeld ein Fragebogen erstellt.

Das Serviceportfolio beinhaltet folgende Dienste:

- Campus-OWL-IT-Services.nrw
- Sciebo
- Datensicherung.nrw
- AcademicGroupware.nrw

- eAkte.nrw
- FD-Storage.nrw
- E-Learning Dienste
- PVP.nrw
- HM4MINT.nrw
- Backup/Restore RWTH Aachen
- RWTH Compute Cluster
- LVN.nrw

Die Analyse der Interviews mit den verantwortlichen der DH.NRW Services lassen sich in 6 zentrale Aspekte zusammenfassen. Diese sind erwartungsgemäß weniger von technischer, sondern eher von inhaltlicher oder prozessualer Natur. Diese sechs Kernelemente sind genauestens beim Aufbau eines DH.NRW föderiertem Identity Managements (IDM) zu betrachten, da jede gefundene technische Lösung unter den folgenden Rahmenbedingungen gestaltet werden muss:

1. **Reichweite**

Es wurde zum Zeitpunkt der Befragung kein Service ermittelt, der eine Reichweite außerhalb NRWs hat und nicht bereits am föderierten DFN-AAI teilnimmt (und damit bereits eine Authentifizierung- und Autorisierungslösung hat) (siehe Abbildung 19).

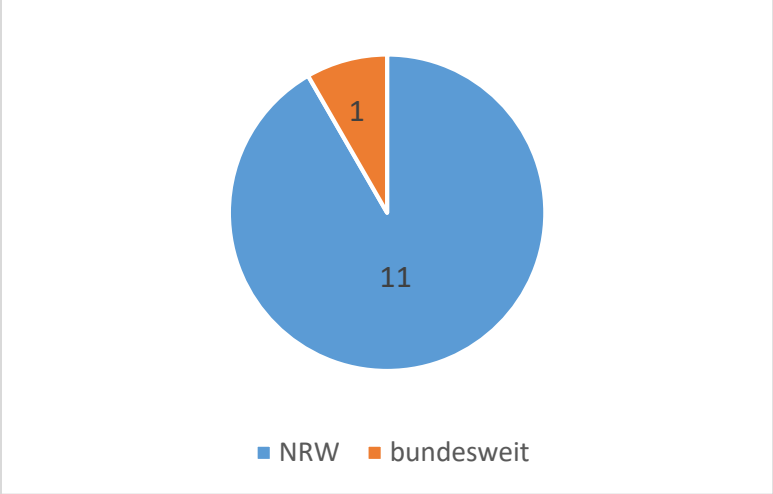

Abbildung 19: Geplante Reichweite der Services

Jedoch war die Aussage, wie viele Nutzer ein konkreter Service hat sehr heterogen, die Zahlen schwankten zwischen 100 und 150.000 Kunden pro Service. Auch bei den Kundengruppen zeichnet sich ein sehr breites Bild ab (siehe Abbildung 20).

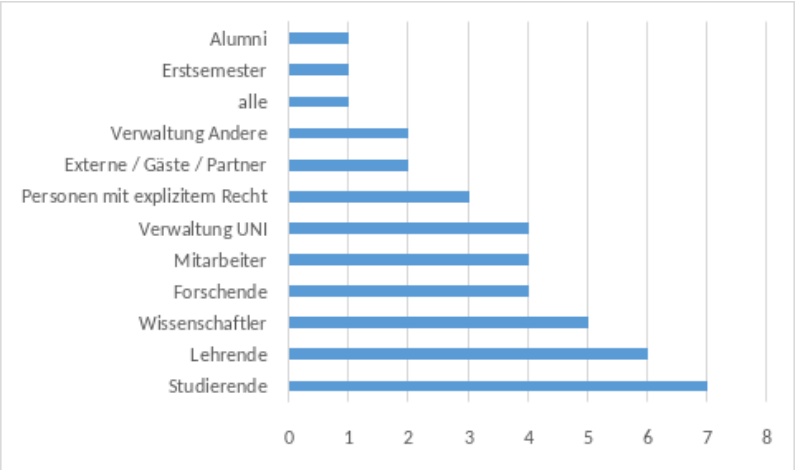

Abbildung 20: Nennungen der Gruppen nach Häufigkeit

Für IDM.NRW lässt sich daraus ableiten, dass es erforderlich ist, ein landesweites Verständnis über die jeweilige Statusgruppe zu bekommen. Hierbei stimmt die IDM.NRW Projektgruppe überein, dabei keine juristischen Fragen klären oder gar Verantwortung für die Validität übernehmen zu können. IDM.NRW wird technische Lösungen bieten, wie Informationen zwischen einem Service und einem IDM.NRW ausgetauscht werden können, nicht aber deren inhaltliche Prüfung vornehmen; dies muss in der Hoheit der jeweiligen Universität oder Fachhochschule bleiben. Das ist auch beim DFN-AAI der Fall: innerhalb der Föderation werden sowohl einer teilnehmenden Lehranstalt als auch einem teilnehmenden Service vertraut, eine Aktualität der Daten wird vertraglich zugesichert [1]. Eine ähnliche vertragliche Verpflichtung sollte auch für IDM.NRW zwischen den Bildungseinrichtungen gefunden werden. IDM.NRW wird auch dafür juristische Unterstützung brauchen.

Unklar in der Machbarkeitsstudie IDM.NRW bleibt, ob es sinnvoll ist, eine NRW-weite Speicherung von Gruppeninformationen zu etablieren oder diese eher dezentral zu speichern und in Echtzeit von den beteiligten Hochschulen liefern zu lassen. Beim DFN-AAI ist letzteres der Fall und funktioniert in der Praxis auch zuverlässig, allerdings kennt das vereinbarte Gruppenschema weniger Statusgruppen (lediglich: faculty, student, staff, alumni, member, affiliate, employee, library-walk-in) [2], als von den Services als Anforderung formuliert wurden.

Aktuell existiert außerhalb der DFN-AAI noch keine technische Lösung weder für eine zentrale noch eine dezentrale Speicherung von solchen übergreifenden Gruppeninformationen.

Weiterhin kann ein IDM.NRW auch kein zielsystemspezifisches Wissen über Gruppenvererbung, Gruppenhierarchien oder Compliancefragen aufbauen. Es ist daher sinnvoll und auch an den meistens Hochschulen und Fachhochschulen gelebte Praxis, im IDM nur Wissen über die Geschäftsrolle einer Person zu hinterlegen, nicht aber die vollständigen konkreten Anwendungsrollen aller Zielsysteme abzubilden.

2. Fehlender Identity Lifecycle

Identity Lifecycle ist ein Begriff für den vollständigen Lebenszyklus einer elektronischen Identität und damit oft der Zugang für einen Benutzer auf einem bestimmten System. In den Interviews wurde deutlich, dass kaum ein DH.NRW Service zum Erstellen, Aktualisieren, Entziehen oder Löschen von Identitätsdaten, Authentifizierungsdaten oder Autorisierungsdaten ein Konzept hat. 8 von 12 Services haben abgeben, aber genau das zu brauchen (siehe Abbildung 21).

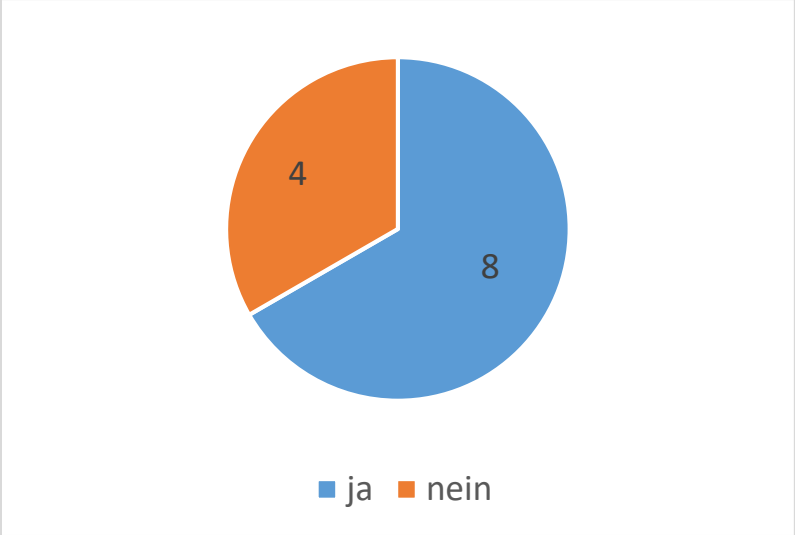

Abbildung 21: Anzahl Antworten, ob Identity Lifecycle benötigt wird

Dies ist besonders hervorzuheben, da nahezu alle Services eine Laufzeit von über 5 Jahren angeben, in denen vermutlich viele Daten erzeugt, gespeichert und gelöscht werden (siehe Abbildung 22).

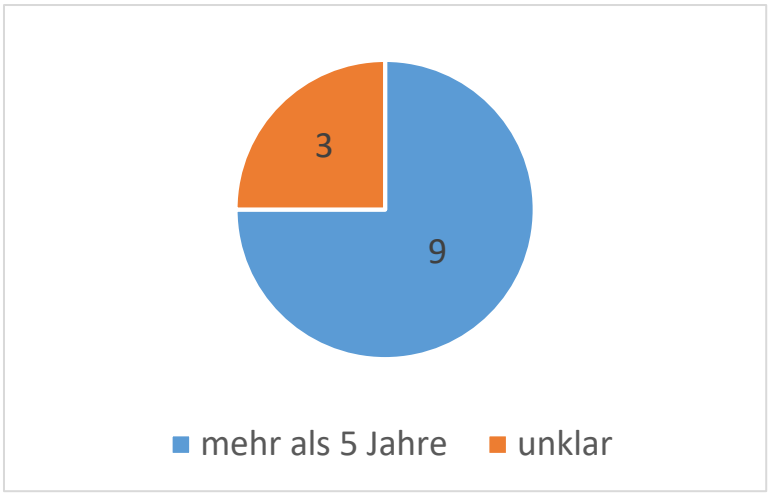

Abbildung 22: Erwartete Laufzeit nach Anzahl Angaben

Es ist für die Projektgruppe IDM.NRW klar, dass eine dauerhafte Beratung für DH.NRW Services erforderlich sein wird, damit alle Vorteile eines IDMs auch langfristig Wirkung zeigen. Dies gilt zum Beispiel speziell, aus Datenschutz- und Informationssicherheitsaspekten, für den zeitnahen Entzug von Statusgruppen und das Löschen von Benutzerkonten. Viele Services rechnen zudem mit einer wachsenden Anzahl an Nutzerdaten (siehe Abbildung 23).

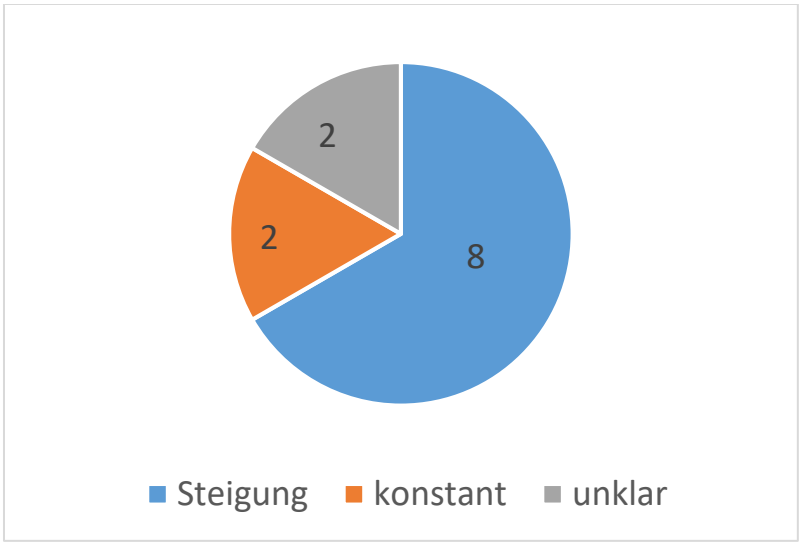

Abbildung 23: Erwartete Nutzerzahlen

3. Human Interface Devices (HID)

Die meisten DH.NRW Services haben angegeben, dass sie eine Weboberfläche als Schnittstelle zum Benutzer anbieten werden (siehe Abbildung 24).

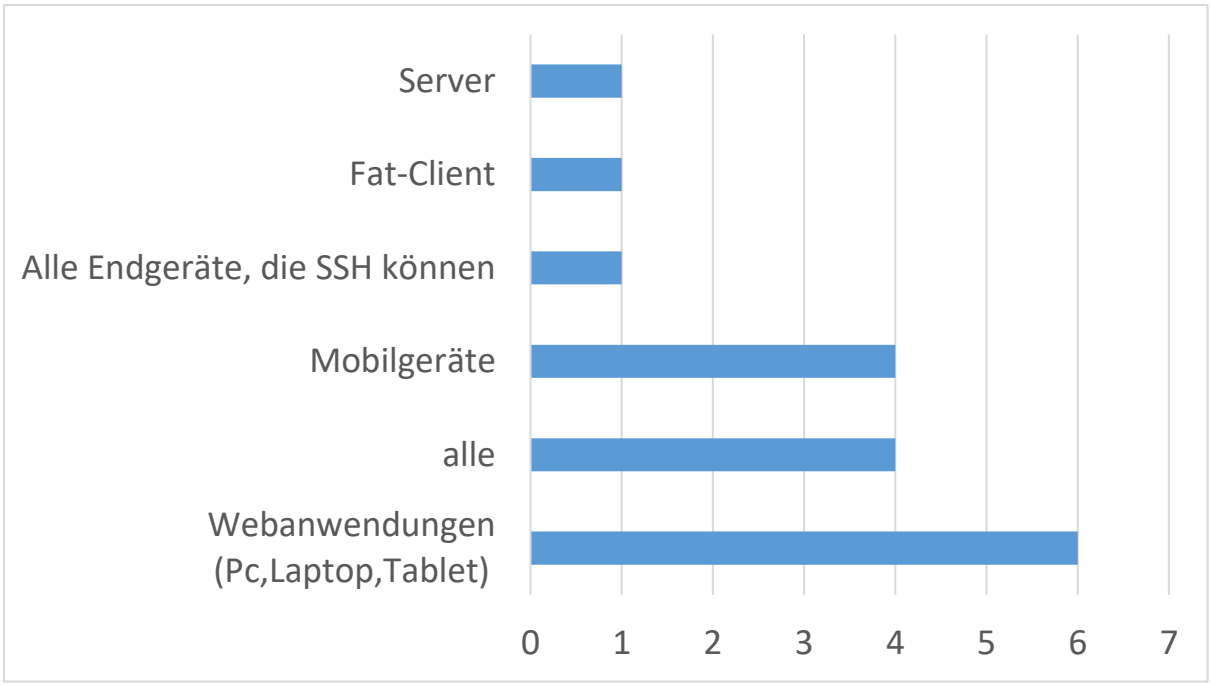

Abbildung 24: Genannte HIDs nach Häufigkeit

Dies ist für IDM.NRW von Vorteil, da die berechtigte Hoffnung besteht, die DFN-AAI mit NRW-spezifischen Erweiterungen (Modell wie beim „bwIDM“ in Baden-Württemberg) hauptsächlich für diese Services nutzen zu können.

Am zweithäufigsten wurden Mobilgeräte als Schnittstelle zum Benutzer genannt. Hier konnten die DH.NRW-Serviceinterviewpartner nicht genau spezifizieren, ob es sich dabei wirklich um explizite Apps für Mobilgeräte handelt oder die Webseiten eines Services derart responsiv sind, dass sie über einen mobilen Browser genutzt werden können.

Am dritthäufigsten wurden, neben SSH und Server, Fat-Clients genannt, also in der Regel Programme, die explizit als Software auf einem Linux- oder Windows-OS laufen. Gerade diese könnten für IDM.NRW aus zweierlei Gründen eine besondere Herausforderung darstellen, denn häufig sind diese Programme nicht in der Lage, nichtlokale Authentifizierungsmechanismen zu unterstützen, sondern sie verlassen sich oft darauf, dass zum Beispiel ein lokales Active Directory oder lokaler LDAP-Service bereitsteht. Bei DH.NRW-Diensten, die über viele Standorte hinweg mit Fat-Clients arbeiten müssen, ist es leicht vorstellbar, dass dezentrale technische Lösungen zur Zugriffsteuerung schwierig sein könnten. Dies wird auch am zweiten Grund deutlich: gibt es zum Beispiel einen Service der mehrere GUI-Varianten anbietet, so muss der Benutzer, egal über welchen Weg er kommt, mit den gleichen Berechtigungen ausgestattet sein. Wenn nun aber die Weboberfläche und Fat-Client oder Weboberfläche und Mobilgerät unterschiedliche Authentifizierungs- und Autorisierungstechnologien verwenden, zum Beispiel LDAP und SAMLv2, kann es

möglicherweise zu Diskrepanzen in den Berechtigungen kommen – ein Risiko aller Services, die verschiedene HIDs parallel anbieten.

4. Kommunikationsstrukturen

Die Interviews haben gezeigt, dass zum Zeitpunkt der Durchführung bei vielen DH.NRW Services keine einheitliche Rollenbesetzung im Projektsinne vorliegt. Zudem sind an einigen mehrere Hochschulen und Fachhochschulen beteiligt (siehe Abbildung 25) und auf der DH.NRW Projektinternetseite wird nur die projektleitende Person genannt.

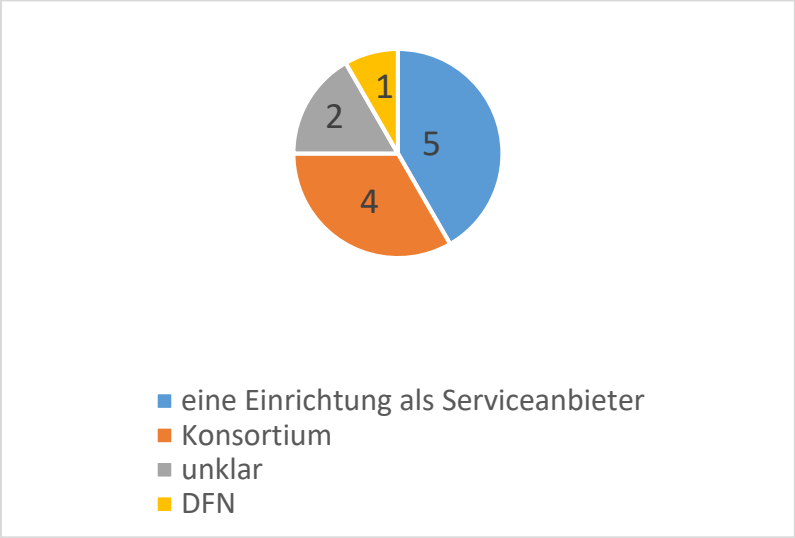

Abbildung 25: Beteiligte Einrichtungen pro Service

Da IDM Fragen intrinsisch nicht nur einen technischen, sondern prozessualen Charakter haben, sind erwartungsgemäß mehrere Ansprechpartner/innen bei einem Service für die erfolgreiche Anbindung an IDM.NRW erforderlich. Die IDM.NRW Projektgruppe schlägt daher vor, neben der Nennung der Gesamtprojektleitung, auch die fachverantwortliche Person und die technische Projektleitung eines DH.NRW Services zu benennen.

5. Ressourcen

Alle DH.NRW Services haben auf Nachfrage keine speziellen IDM-Ressourcen vorgesehen. Dies kann, je nach IDM Problemkomplexität, ein großes Projektrisiko bedeuten. Generell ist nicht geklärt, ob das Land NRW, die Services selber oder die jeweilige Hochschule oder Fachhochschule dieses Risiko tragen. Dies gilt nicht nur für neue DH.NRW Services, sondern insbesondere auch dann, wenn bereits an den Hochschulen und Fachhochschulen existierende Services in der DH.NRW zentralisiert werden. Genau hier spielen Benutzererfahrungen und Datensicherheit eine große Rolle für die Akzeptanz einer Zentralisierungsstrategie.

6. Sicherheits- und Betriebskonzept

Sicherheits- und Betriebskonzepte liegen auf Nachfrage nur bei einem Teil der Services vor (siehe Abbildung 26). Das kann unter Umständen kritisch für Systeme sein, die im hohen Maße personenspezifische Daten verarbeiten.

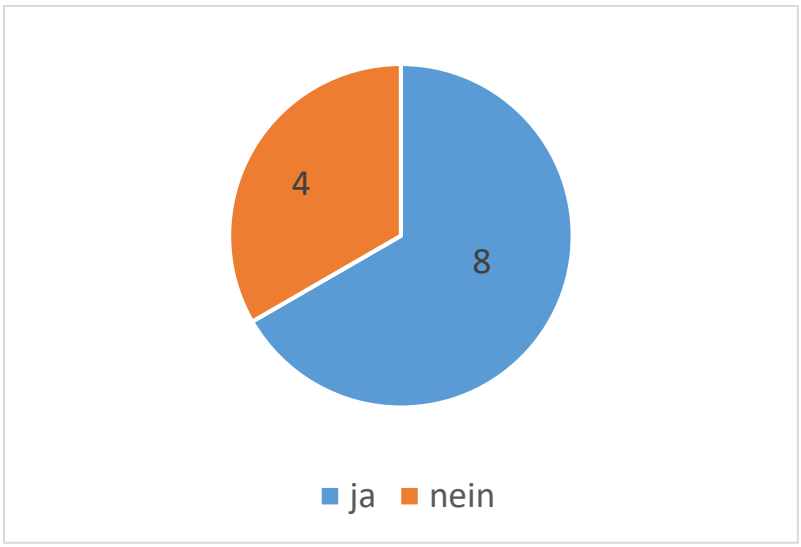

Abbildung 26: Angaben nach Anzahl, ob ein Sicherheits- und Betriebskonzept vorliegt

IDM.NRW schlägt vor, ein Mindestmaß an Dokumentation einzufordern, sowie Mindeststandards zu setzen, die die ausschließliche Verwendung von verschlüsselten Protokollen wie HTTPS oder LDAPS fordern.

Die technischen Anforderungen der meisten DH.NRW Services, speziell derer, die stark auf Webtechnologien setzen, erscheinen umsetzbar. Schwierigkeiten drohen bei Services, die keine Möglichkeit bieten, an ein föderiertes IDM gekoppelt zu werden oder Fat-Clients dezentral benötigen.
Die größere Herausforderung wird darin bestehen, in NRW Gruppen zu vereinheitlichen und eine für alle IDMs und Services abgestimmte Syntax zu definieren, sowie über deren zeitliche Validität vertragliche Verpflichtung einzufordern.
Ein weiteres Risiko besteht darin, wenn die Projektleitungen der DH.NRW-Services den IDM-Fragen nicht genug Projektzeit innerhalb ihres Projektes lassen.
IDM-Lösungen helfen in der Regel sehr, können aber eine, je nach Anforderung, hohe technische und prozessuale Komplexität aufweisen.

3.4. Untersuchung bereits etablierter Projekte bzw. Initiativen

Um von den Erkenntnissen eventuelle bereits vorhandener Lösungen zu profitieren, wurde ein Überblick über existierende Verbünde erstellt. Diese Verbünde wurden daraufhin untersucht, welche Technik eingesetzt wird, wie der jeweilige Verband strukturiert ist und welcher Erkenntnisgewinn daraus gezogen werden kann. Dazu wurden öffentlich verfügbare Dokumentationen ausgewertet. Aufgrund der Vielzahl bereits existierender Verbünde musste eine stark eingeschränkte Vorauswahl getroffen werden. So wurde die Suche eingeschränkt auf in Deutschland verfügbare Verbünde, zu deren Struktur öffentlich verfügbare Dokumentation existiert. Andere europäische oder internationale Verbünde oder Projekte wurden betrachtet, wenn ein neuartiger oder vielversprechender Ansatz verfolgt wurde.

Zur Bewertung der Relevanz für das Projekt wurde die Tauglichkeit für die zwei Nutzungsarten von organisationsübergreifend genutzten Rechnersystemen überprüft, die im IDM-Alltag erfahrungsgemäß am Häufigsten vorkommen. Das sind einerseits Webanwendungen, die mittels eines Browsers genutzt werden, und andererseits Serversysteme, auf die der Zugriff mittels SSH erfolgt. Eine hohe Relevanz haben hier Ansätze, die komfortablen und sicheren Zugriff auf die Anwendungen bzw. Systeme anderer Universitäten ermöglichen mit einem möglichst hohen Grad an Automatisierung und einer geringen Notwendigkeit für manuelle Intervention. Es zeigt sich hier, dass sich für Webanwendungen SAML als Quasi-Standard etabliert hat.

SAML-Architekturen

SAML als Protokoll gibt keine Topologie vor, wie Identity Provider (IdP) und Service Provider (SP) verbunden sein müssen. Daraus ergeben sich mehrere mögliche Varianten. Das eduGAIN-Projekt hat die Topologien der teilnehmenden Verbünde untersucht und die Ergebnisse auf ihrer Homepage veröffentlicht. Die vorkommenden Topologien werden im Folgenden kurz vorgestellt (Bilder von eduGAIN).

Mesh Federation

In der Mesh (Netz)-Föderation sind sämtliche Elemente dezentral ausgelegt. Jede Teilnehmer-Organisation betreibt eigene IdP und Discovery Services (DS). Identitäten und deren Life Cycles werden durch die Teilnehmer-Organisationen verwaltet. Benutzer authentifizieren sich grundsätzlich gegen die IdP ihrer Heimat-Organisationen. Optional kann es einen zentralen DS geben. Diese Variante ist die am häufigste vorkommende Topologie. Sie erlaubt den Teilnehmer-Organisationen maximale Souveränität und erfordert minimale Anpassungen an den Identitäten und Life Cycles.

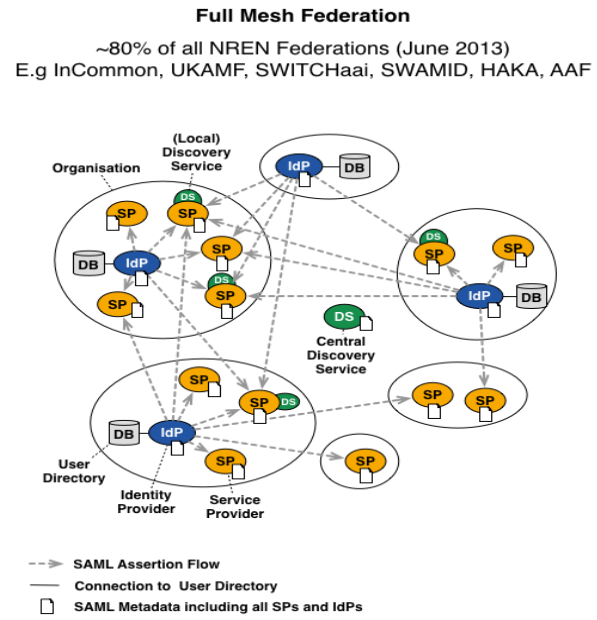

Abbildung 27: Full Mesh Federation (Quelle: eduGAIN)

Hub and Spoke Federation mit dezentraler Autorisierung

In der Hub and Spoke (Stern)-Föderation werden Identitäten dezentral vorgehalten, allerdings gibt es einen zentralen IdP-Proxy, der zwischen den SP und den IdP zwischengeschaltet ist und mit einem zentralen DS zusammenarbeitet. Die Benutzer authentifizieren sich auch hier gegen die IdP ihrer jeweiligen Heimat-Organisationen, allerdings kontrolliert der Proxy, welche Attribute der Benutzer weitergegeben werden. Die Übertragung der Authentisierungsdaten erfolgt mittels SAML. Diese Topologie kommt noch relativ häufig vor. Die Zentralisierung erfordert ein größeres Maß an Abstimmung als in der Mesh Federation.

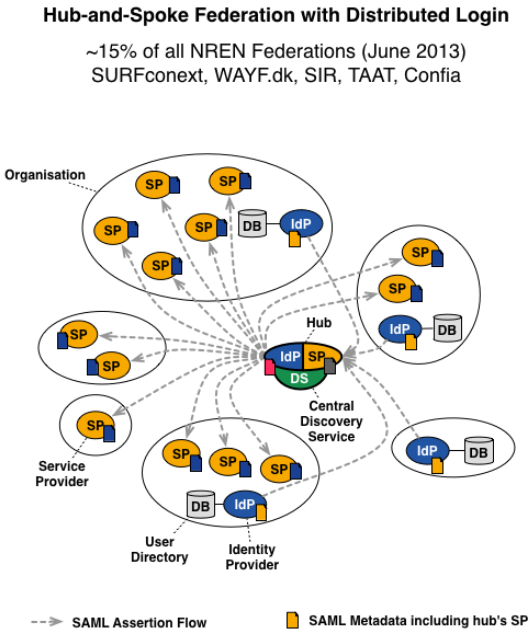

Abbildung 28: Hub-and-Spoke Federation with Distrubuted Login (Quelle: eduGAIN)

Hub and Spoke Federation *mit zentraler Autorisierung*

In dieser Föderationsform gibt es nur einen (zentralen) IdP. Alle Benutzer authentifizieren sich gegen diesen zentralen IdP. Die Benutzerpflege kann dezentral erfolgen, allerdings werden die Benutzerdaten über ein Drittprotokoll (z.B. per Datenbankverbindung) übertragen. Diese Topologie kommt am seltensten vor. Der hohe Grad an Zentralisierung bietet Vorteile durch Nutzung von Synergien, erfordert aber ein hohes Maß an Koordination und Vertrauen.

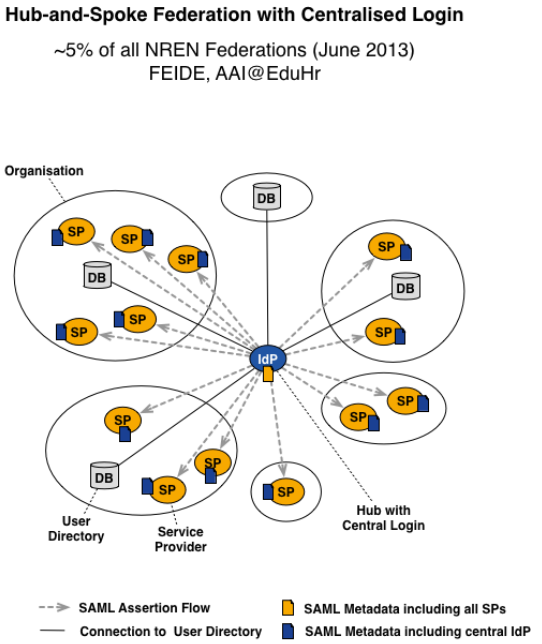

Abbildung 29: Hub-and-Spoke Federation with Centralised Login (Quelle: eduGAIN)

Betrachtete Verbünde

DFN-AAI

Die DFN-AAI ist ein Dienst des DFN-Vereins. Ein Großteil der Hochschulen in Deutschland ist Mitglied in der DFN-AAI Föderation. Diese Föderation basiert auf dem SAML2-Protokoll auf Basis von Shibboleth. Die Föderation ermöglicht es Nutzern, sich mit den Authentifizierungsmerkmalen der Heimatorganisation bei Webdiensten von teilnehmenden Organisationen anzumelden. Dazu betreibt DFN-AAI einen zentralen Discovery / Where are you from (WAYF)-Service, der den Nutzer an die dezentralen Authentisierungsserver weiterleitet. IDM findet vollständig dezentral in den teilnehmenden Hochschulen statt. Zur Teilnahme müssen allerdings Vorgaben an Datenqualität und -umfang erfüllt werden, die durch die DFN-AAI vorgegeben sind. Damit ist die DFN-AAI eine Mesh-Federation. Es sind bereits eine Vielzahl an browserbasierten Diensten auf Basis von SAML in DFN-AAI eingebunden. Weitere Protokolle werden nicht angeboten.

bwIDM

Der technische Verbund bwIDM wurde als Subföderation innerhalb der DFN-AAI realisiert mit dem Ziel des Aufbaus und der gegenseitigen Nutzung von Services in Baden-Württemberg. Beim Entwurf wurde besonderes Augenmerk auf die Nutzung von Services per SSH gelegt. Zu diesem Zweck wurde eine LDAP-Fassade für SAML implementiert, welche per LDAP in die Services eingebunden wird und die Authentifizierung nachgelagert über Shibboleth durchführt. Diese Lösung hat den besonderen Vorteil, dass sie weder im Verbund noch in den Zielsystemen spezielle Anpassungen der verwendeten Software erfordert. bwIDM ist grundsätzlich eine Mesh Federation, mit der Ergänzung um die zentrale LDAP-Bridge. Während der Machbarkeitsstudie IDM.NRW hat sich die Projektgruppe des Öfteren mit den Projektverantwortlichen von bwIDM ausgetauscht. Dieser Austausch ist ebenfalls im Folgeprojekt weiterzuführen, um ggf. Lösungen kompatibel zu gestalten.

Saxid

Die SAXid ist ebenfalls eine Unterföderation des DFN-AAI im Bereich des Landes Sachsen. Hier kommt ebenfalls SAML zum Einsatz. Darüber werden einige browserbasierte Services angeboten. SAXid ist als Mesh Federation organisiert. Die Technische Universität Dresden bietet im Rahmen des Verbundes einen Zugang zu Ihrem HPC-Cluster. Dafür ist ein Zugang im IDM der TU Dresden erforderlich, allerdings ist die Antragstellung digital per Shibboleth möglich.

MPG-AAI

Die Max-Planck-Gesellschaft besteht aus über 50 Untergesellschaften, die heterogene IDM-Konzepte betreiben. Diese sind zusammengeschlossen in der MPG-AAI, die wiederum eine Unterföderation der DFN-AAI ist. Um zu vermeiden, dass die 50 Gesellschaften die Auswahlliste des WAYF-Service in der DFN-AAI unnötig aufbläht, und weil nicht jede Untergesellschaft einen IdP oder gar ein IDM betreibt, ist die MPG-AAI über einen IdP-Proxy an die DFN-AAI angeschlossen. Dieser aggregiert die Identitäten der einzelnen Gesellschaften, so dass nach außen nur der Proxy sichtbar ist. Den einzelnen Gesellschaften steht es dabei frei, ob sie selbst einen IdP betreiben, ein eigenes IDM über andere Schnittstellen an den Proxy anschließen, oder das IDM komplett zentral auslagern. Die Topologie der MPG-AAI entspricht am ehesten der Hub and Spoke Topologie mit einem zentralen IdP.

eduGAIN

eduGAIN ist ein internationaler Meta-Verbund, der durch das europäische GEANT-Projekt entwickelt wurde. eduGAIN baut auf das SAML-Protokoll auf und verbindet die nationalen

Verbünde mit Hilfe eines sog. Metadata Distribution Service (MDS) miteinander. Dieser MDS nimmt Daten über IdP und SP der einzelnen Verbünde entgegen, aggregiert sie und verteilt sie an die Verbünde zurück. Zur Teilnahme muss die Verteilung der Metadaten der eigenen IdP gezielt freigeschaltet werden (Opt-In). Von dem MDS abgesehen ist eduGAIN als Mesh Federation organisiert.

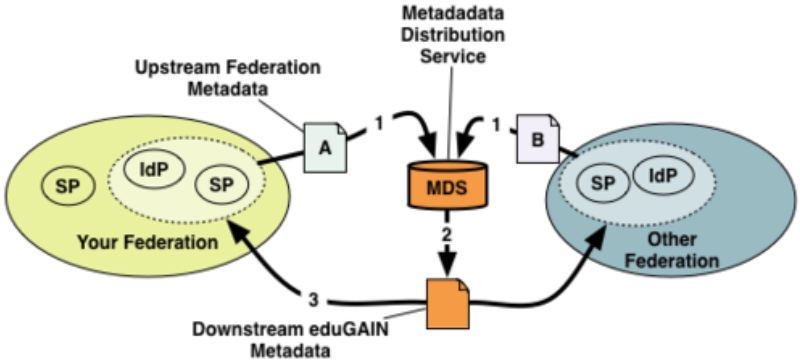

Abbildung 30: Funktionsweise des Metadata Distribution Service (Quelle: eduGAIN)

SWITCH edu-ID

Die edu-ID der schweizerischen Gesellschaft SWITCH ist der Nachfolger der aktuellen SWITCH-AAI auf Basis von SAML. Jeder Nutzer an einer der teilnehmenden Hochschulen erhält eine landesweit eindeutige lebenslange ID, deren Stammdaten zentral gepflegt werden. Diese können die Hochschulen mit ihren eigenen Informationen anreichern. Der Vorteil dieses Konzeptes ist, dass die ID auch bei einem Wechsel der Hochschule ihre Gültigkeit behält. Die Topologie der SWITCH edu-ID entspricht am ehesten der Hub and Spoke Topologie mit einem zentralen IdP.

MyAcademic-ID

MyAcademic-ID soll eine Brücke zwischen eduGAIN und digitalen Signaturverfahren herstellen, um es Studierenden einfacher zu ermöglichen, im Rahmen des ERASMUS-Programms Lehrangebote von Universitäten in Europa wahrzunehmen. Ziel ist es, den Verwaltungsaufwand zu digitalisieren und zu reduzieren. Hierzu werden Brücken zwischen den Protokollen benutzt und eine einheitliche Benutzerkennung für alle Protokolle vereinbart.

4. Anforderungen aus der Status Quo Erfassung

In diesem Kapitel werden die identifizierten Anforderungen, die sich u.a. aus Kapitel 3 ergeben, näher vorgestellt. Hierzu wurden alle Befragungsergebnisse ausgewertet und analysiert. Die erfassten Informationen wurden gemäß einem Clustering-Verfahren ausgewertet und werden im weiteren Verlauf näher beschrieben. Einige Kernaussagen wurden bereits in Kapitel 3

erläutert. Der Vollständigkeit halber werden diese für die Gesamtbetrachtung auch in diesem Kapitel aufgezeigt.

Eine Anforderung ist die Konzipierung einer Lösung für den verteilten Zugriff auf Nicht-Webdienste, wie z.B. den HPC-Cluster. Ein erster Schritt in die Richtung kann die Evaluation von neuen und herkömmlichen Technologien sein. Gemäß den Umfrageergebnissen lassen sich bestimmte Technologien, wie das AD, der LDAP oder Shibboleth in NRW als Basistechnologien kennzeichnen. Auch die innerhalb der Experteninterviews identifizierten Kompetenzen für Webschnittstellen (SOAP und REST) können hier eine Chance bieten, die Technologielücke zu füllen. Außerdem sind weitere Technologien wie OpenID, OAuth (Open Authorization), ADFS (Active Directory Federation Services), und SSH (Secure Shell) relevante Technologien, die näher betrachtet werden und eine zunehmend große Bedeutung erhalten sollten. Als weitere klare Anforderung haben die Hochschulen in NRW den Bedarf an Standard-Schnittstellen geäußert. Damit verbunden wurde der Wunsch nach Sicherheitsstandards (Passworte, Techniken auf dem aktuellen Stand, Best Practices, geregelte Sicherheitskonzepte, sichere Schnittstellen) genannt. Um diesen Bedarfen und Anforderungen nachzukommen werden im Rahmen des IDM.NRW Projekts, die u.a. oben genannten Technologien näher betrachtet und einer Evaluation unterzogen. Nur so können geeignete und sichere technische Lösungen konzipiert werden, die als Best-Practice und Empfehlung den Hochschulen in NRW zur Verfügung gestellt werden. Der Aufbau einer geeigneten Evaluation und ein möglicher Ansatz werden in Kapitel 5 näher beschrieben.

Eine weitere stark kommunizierte Anforderung ist der Bedarf von gemeinsamen Attributen in NRW. Dadurch sollen u.a. die zu übermittelnden Daten standardisiert und auf ein Minimum beschränkt werden (Datensparsamkeit). Durch Datensparsamkeit erhöht sich natürlich auch der Datenschutzaspekt, der in jedem Fall bedacht wird. In dem Zusammenhang wird in Kapitel 5 ein Attributset entwickelt, welches zunächst als Grobkonzept dienen soll. Eine Ausarbeitung der „Gemeinsamen Attribute in NRW“ und die Erprobung anhand von Use Cases wird im Hauptprojekt erfolgen.

Die dritte Anforderung, die sich aus den Befragungen ergab, ist der Bedarf einer Gruppen-/ Rollen-/ Rechteverwaltung. Eine Grundvoraussetzung für eine mögliche standardisierte Gruppenverwaltung, ist die Einigung über die Begrifflichkeit der zentralen Personengruppen in den Hochschulen. Welche zentralen Personengruppen es gibt und wie eine Homogenisierung der Begriffsdefinitionen erreicht werde kann, wird in Kapitel 5 beschrieben. Dort sind erste Erkenntnisse und Überlegungen zusammengefasst.

Die oben beschriebenen Bedarfe werden als zentrale Anforderungen betrachtet und erhalten dementsprechend große Aufmerksamkeit im Hauptprojekt. Daneben gibt es noch weitere vereinzelt genannte Anforderungen, die ebenfalls im Hauptprojekt betrachtet werden. Dazu

gehört das Thema Organisation und Technik, welches die gute Dokumentation von Lösungen und Technologien, ein geregeltes Supportkonzept und einen gemeinsamen Arbeitskreis beinhaltet, der sich kontinuierlich mit der Lösungsfindung der Anforderungen beschäftigt. Ein guter Ansatzpunkt bzgl. einer geregelten Supportstruktur ist die Erkenntnis, dass alle teilnehmenden Hochschulen in NRW über ein Ticket-System verfügen. Aufgrund dessen kann im Rahmen des Hauptprojekts eine hochschulübergreifende Supportstruktur konzipiert werden.

Ein weiteres wichtiges und klassisches IDM Thema stellt der Lifecycle von Identitäten dar. Im Rahmen des Vorprojekts kann festgehalten werden, dass bei einer hochschulübergreifenden Servicenutzung, Informationen über eine Person über die lokalen IDM-Systeme bereitgestellt werden sollen. Der Service solle im Nachgang selbst entscheiden, was er mit den Informationen tut und welche Berechtigungen vergeben werden. Dabei sollen sowohl die Abfragen als auch die Benachrichtigungen standardisiert ablaufen. Das Thema Deprovisionierung von Konten- und Benutzerdaten ist ebenfalls ein wichtiges Thema, dass Beachtung finden soll. Ob sich eventuell noch weitere Anforderungen aus parallellaufenden Initiativen oder Projekten, welche im Abschnitt 3.4 beschrieben sind, ergeben, wird sich im Verlauf des Hauptprojekts zeigen. Es ist jedoch festzuhalten, dass diese Projekte weiterhin beobachtet werden, um die Kompatibilität entwickelter Lösungen zu gewährleisten.

Nachdem die Anforderungen aus der Status Quo Erfassung der IDM-Systemlandschaft in NRW vorgestellt wurden, werden im weiteren Verlauf des Kapitels die Anforderungen aus der Status Quo Erfassung der Servicelandschaft in NRW beschrieben. In dem Zusammenhang wurden explizit drei wichtige Anforderungen genannt: Gemeinsame Gruppendefinition (zentrale Personengruppen-Definition), Erstellung von Sicherheits- und Betriebskonzepten und der Ticketaustausch bei einer hochschulübergreifenden Servicenutzung. Was mit der ersten Anforderung gemeint ist, wurde bereits im oberen Abschnitt näher erläutert. Die zweite Anforderung bezieht sich auf die Erstellung von Sicherheits- und Betriebskonzepten für ein föderiertes Identity Management. Dies ist ebenfalls ein Bestandteil des Hauptprojekts, welches unter den Punkt Datenschutz und Nachhaltigkeit fällt. Im Falle einer hochschulübergreifenden Servicenutzung in NRW müssen die hochschulübergreifenden Supportstrukturen feststehen, um einen reibungslosen Betrieb zu gewährleisten.

Es ist davon auszugehen, dass im Rahmen des Hauptprojekts tiefreichende Gespräche mit Servicebetreibern geführt werden und dass dementsprechend zusätzliche Anforderungen an IDM.NRW herangetragen werden.

5. Konzepterstellung

In diesem Kapitel werden gemäß den Anforderungen aus Kapitel 3 und 4 Grobkonzepte vorgestellt. Zunächst wird ein erster Ansatz für eine standardisierte Attributübermittlung in NRW vorgeschlagen. Im zweiten Abschnitt folgt ein erster Vorschlag für die Bestimmung und Definition zentraler Personengruppen in NRW. Im dritten Abschnitt wird dargestellt, wie eine Evaluation von neuen Technologien aussehen kann. Zudem werden erste Technologien benannt, die unter bestimmten Kriterien analysiert und bewertet werden. Im letzten Abschnitt wird beschrieben, wie der Konsens in NRW erreicht werden kann und welche Maßnahmen für eine erfolgreiche Zusammenarbeit notwendig sind.

5.1. Gemeinsame Attribute in NRW

Die hier vorgestellten Lösungen sind zunächst als erster Ansatz bzw. als Grobkonzept zu verstehen. Die detaillierte Bearbeitung und Erprobung erfolgt im Hauptprojekt. Die im Rahmen des Vorprojekts IDM.NRW erstelle Attributliste orientiert sich an den Best Practice Empfehlungen zur Verwendung von Attributen in der DFN-AAI [3]. Insbesondere die Konzepte eduPerson und SCHAC wurden näher betrachtet [4]. Zudem wurden Servicebetreiber in einem Experteninterview gefragt, welche Informationen über Nutzende ihres Services vorliegen bzw. übermittelt werden müssen, um den Zugriff auf den jeweiligen Service zu erhalten. Auf Grundlage der Informationen wurde eine Tabelle erstellt, die in der ersten Spalte erforderliche inhaltliche Informationen über Nutzende beinhaltet. In der zweiten Spalte finden sich die Services, welche die Informationen aus der ersten Spalte benötigen. In der dritten Spalte sind die möglichen, gängigen Shibboleth-Attribute hinterlegt, anhand dessen die Informationen über Nutzende übermittelt werden können. An einigen Stellen wurden mehrere Attributnamen genannt und an anderen Stellen, wie z.B. NRW-Zugehörigkeit, ist noch keine konkrete Festlegung gemacht. Diese Bestimmungen sind im Hauptprojekt nach Rücksprache mit den jeweiligen Servicebetreibern festzulegen und zu erproben. Die vierte Spalte gibt Information darüber, welche Attribute bzw. Informationen über Nutzende zu einem NRW Standard werden sollten und welche nur bei Bedarf übermittelt werden. Die fünfte Spalte zeigt, wie die technische Form des jeweiligen Attributwerts aussehen kann. Dies ist eine komplexe Aufgabe, die ebenfalls im Hauptprojekt nach Rücksprache mit dem jeweiligen Servicebetreiber geklärt werden muss. Die letzte Spalte gibt Information darüber, ob es sich bei dem jeweiligen Attribut, um ein single oder multi value Attribut handelt. Insbesondere die Festlegung auf ein Standard-Set von Attributen und eine möglichst homogene technische Form der Attributwerte versprechen eine deutliche Erleichterung der Implementierung für zukünftige Services in NRW

– sowohl auf Seiten der Service-Anbieter, als auch auf Seiten der konsumierenden Einrichtungen.

Informationen über Nutzenden	Services	Attribute	NRW Standard	Technische Form	Single/ multi value
Benutzername	Academic Groupware	upn (Benutzername im AD)		muss eindeutig sein, muss scope enthalten; darf nur als Login-Name verwendet werden	single
Eindeutige Benutzer ID	Backup und Restore, RWTH HPC	eduPersonTargetedID/ eduPersonUniqueId	x	https://www.switch.ch/aai/support/documents/attributes/edupersontargetedid/ https://www.switch.ch/aai/support/documents/attributes/edupersonuniqueid/	single
Nachname	Academic Groupware, Backup und Restore	sn	x	String, der alle Nachnamen wie im Ausweisdokument enthält	single
Vorname	Academic Groupware, Backup und Restore	givenName	x	wie die jeweilige Quelle den Vornamen erfasst und sendet oder Rufname	single
Anzeigename	Academic Groupware (optional)	displayName, cn	x	wie Uni sendet oder Nickname (Außendarstellung der Person), ggf. mit Titeln (keine separaten Titelfelder)	single
E-Mail Adresse	Academic Groupware, Backup und Restore	Mail (MA=dienstlich, Studierende=die von der Einrichtung vorgegebene)	x	xxx@[yyy.]uni.de veränderlich (!)	single
Rollen- und Gruppenzugehörigkeiten	RWTH HPC, AcademicGroupware, Backup und Restore, Datensicherung.nrw, (e-Akte), E-Learning, FD-Storage	eduPersonEntitlement	x	urn:mace:<uninamespace>:role:<source>: <version>:rid=<role id>:name=<role name>:context=<role context> urn:mace:<uninamespace>:group:<source>: <version>:id=<internerne stabile ID der Gruppe. Darf gerne menschenlesbar sein.>	multi

NRW-Zugehörigkeit		Muss noch geklärt werden.	*x*		
Kontext (Affiliation)	Backup und Restore, Daten-sicherung.nrw, E-Learning, FD-Storage, RWTH HPC, Backup und Restore, (e-Akte), PVP	eduPersonScopedAffiliation	x	student@uni-musterstadt.de	multi
Sub-Kontext (Einrichtung/Institut/ Fakultät)	Datensicherung.nrw	Da muss noch ein Standard geschaffen werden		Ein persistenter identifier für Einrichtungen wäre wünschenswert Könnte man als Gruppe abbilden urn:mace:<uninamespace>:OrganizationMembership: <source>:<version>:OrgId=<eindeutige ID der ranisation>:context=<context>	multi
Status	FD-Storage	schacUserStatus		urn:schac:userStatus:de:aai.dfn.de:idmStatus:disabled erlaubte Werte: Liste von URNs des Typs urn:schac:userStatus:<country-code>:<domain>:<iNSS>	multi
Level of Assurance (LoA) / Verlässlichkeitsklasse		eduPersonAssurance			

Zusätzlich zu der exakten Konkretisierung des Tabelleninhalts, sind weitere Festlegungen zu Formaten und Formatierungen notwendig. Diese werden im weiteren Verlauf des Abschnitts beschrieben. Um eine reibungslose Interpretation der Werte zu gewährleisten, sollte z.B. eine Festlegung der Zeichencodierung auf UTF-8 erfolgen.

Um Services für verschiedene Universitäten möglichst einfach zugänglich zu machen, ist es wünschenswert, dass alle Attribute insbesondere diejenigen die Berechtigungen (Rollen, Gruppen, etc.) enthalten, einem einheitlichen Aufbau unterliegen. Dies vermeidet Implementierungsaufwände und komplexe Mapping-Strukturen. Ein Vorschlag dazu ist die Repräsentierung in Form von URN-Strings. Der allgemeine Aufbau sollte wie folgt aussehen:

urn:mace:uninamespace:Type:Scope[:version:Key1[=Value1][:Key2[=Value2]…]].

Dabei sind diese URN-Strings durch Doppelpunkte in unterschiedliche Namensräume untergliedert. Die hier verwendeten Namensräume verstehen sich wie folgt:

Type

als Type wird für IDs id, für Gruppen group, für Rollen role usw. verwendet. „Welchen Datentyp beinhaltet der Wert?“

Scope

als Scope wird beispielsweise rero als Rechte- und Rollenverwaltung verwendet. „Woher stammt der Wert?“

Version

jede Version hat einen definierten Aufbau „Wie ist der Wert strukturiert?“

Key-Value-Paare

beinhaltet mögliche Key-Value-Paare. „z.B.: Welches Recht in welchem Kontext hat die Person?“

Erlaubte Zeichen

Keine der Komponenten Type, Scope, Key, Value darf einen Doppelpunkt oder ein Semikolon enthalten. Der Doppelpunkt gilt immer als Trenner der einzelnen Komponenten. Das Semikolon wird von Shibboleth Service Providern zur Abbildung von multi value Attributen genutzt.

Aufbau Type und Scope

Weder Type noch Scope dürfen Leerstrings sein.

Aufbau der Key-Value-Paare

- Es können beliebig viele Key-Value-Paare auftreten
- Die Key-Value-Paare sind durch Doppelpunkte voneinander getrennt
- Es ist optional welche Key-Value-Paare auftreten
- Die Reihenfolge der Key-Value-Paare ist nicht definiert und kann alternieren. Insbesondere ist die Möglichkeit vorbehalten, weitere Key-Value-Paare zwischen etablierten, also an beliebiger Stelle, einzufügen.
- Jeder Key darf nur einmal vorkommen. Multi value Objekte werden auf Anwendungsebene pro Key-Value-Paar definiert. Sie können durch ein weiteres Trennzeichen getrennt dargestellt werden, wie zum Beispiel key=value1,value2
- Ein Key-Value Paar besteht aus einem Key und optional einem Value.
- Sofern ein Value vorhanden ist, fungiert das erste Gleichheitszeichen als Trenner zwischen Key (links) und Value (rechts). Alle weiteren Gleichheitszeichen werden nicht interpretiert, sondern als Bestandteil des Values betrachtet.
- Sowohl Key als auch Value dürfen weder Doppelpunkte noch Semikolons enthalten.
- Keys dürfen niemals Leerstrings sein
- Es wird bei Values zwischen Leerstrings (Key2=) und null-Values (Key3) unterschieden.
- Die Keys sollen aus „sprechenden Namen“, also nicht aus Abkürzungen, bestehen.
- Es sollte mindestens ein Key-Value-Paar auftreten, da sonst die Versionsnummer nichts beschreiben würde. Sollte also kein Key-Value-Paar benötigt werden, so sollte die Versionsnummer weggelassen werden
- Der komplette URN-String sollte in Kleinschreibung übermittelt werden

Im Folgeprojekt sind diese Festlegungen zu bewerten und abzustimmen. Sie sollen in eine gemeinsame Festlegung münden, die die teilnehmenden Einrichtungen mit ihrem Beitritt zu einer IDM.NRW Föderation verpflichtend übernehmen.

5.2. Personen-/Gruppendefinition

Im Laufe der Evaluationsphase hat sich herauskristallisiert, dass wenn nicht ein Einvernehmen, doch zumindest eine Harmonisierung verschiedener Definitionen von Personengruppen getroffen werden sollte. Es ist im Rahmen der Freiheit von Forschung und Lehre nicht zu erwarten, dass alle beteiligten Institutionen sich langfristig auf eine vollkommen einheitliche Definition verständigen werden. Noch weniger ist dies in der verhältnismäßig kurzen Frist eines Einführungsprojektes zu erwarten. Für die gegenseitige Verständigung wäre

es jedoch unabdingbar, Konstrukte zu entwickeln um sich zumindest auf gewisse Grundtermini und ihre Bedeutung zu einigen.

Das Landeshochschulgesetz NRW unterscheidet zwischen zwei Statusgruppen, den Mitgliedern und den Angehörigen. [5] Darüber hinaus sind in den Identitätsmanagement-systemen weitere Personen verzeichnet, die weder Angehörige noch Mitglieder sind.

Die **Mitglieder** werden im Gesetz streng definiert mit einem Ermessensfall für die Hochschule, bzgl. beurlaubter und abgeordneter Professoren. Zwei Hochschulen machen von dieser Einzelfallentscheidung in ihren Grundordnungen Gebrauch. Darüber hinaus sind keine Veröffentlichungen auffindbar, ob dieser Paragraph angewendet wird. Ein Austausch hierüber unter den Universitäten wird zumindest angeregt.

Die **Angehörigen** werden im Gesetzt nur in Form einer Mindestmenge definiert. Über diese hinaus können die Hochschulen selbst Personen in diesen Kreis aufnehmen. Dies wird von allen Hochschulen mehr oder weniger praktiziert. Klassische Fälle sind beispielsweise:

An-Institute: Mitgliedschaft auf Antrag für die Dauer der voraussichtlichen Arbeitszeit. *Ehemalige Studenten:* Nur bei Abschluss oder einer minimalen Studienzeit, dann für x Jahre, unlimitierte Verlängerung um jeweils x Jahre möglich. (Vorschlag x=3)

Ehemalige Beschäftigte: Bei Ausscheiden aus Altersgründen: Für jeweils x Jahre, unbegrenzt verlängerbar. Begrenzung nur, um irgendwie an „Todeslisten“ zu kommen. Bei Ausscheiden aus anderen Gründen: Übergangsfrist ein Jahr, danach nicht mehr. (Vorschlag x=10) *Auszubildende:* Sollten als Angehörige geführt werden.

Lehrbeauftragte: Für die Dauer des Lehrauftrags.

Habilitanden (sofern keine Angestellten): Für die Dauer des Habilitationsverfahren. Problem des Mitbekommens des Abbruchs des Verfahrens. Daher Limitierung auf 6 Jahre, danach Verlängerungsmöglichkeiten.
Doktoranden sind hier nicht extra gelistet, weil sie meist entweder eingeschrieben und somit Studenten oder angestellt sind. Beides triggert den Mitgliederstatus

Medizinische Einrichtungen: Hier sind nicht nur die Angestellten der Unikliniken selbst und jene der medizinischen Fachbereiche gemeint, sondern auch Lehrbeauftragte aus anderen Lehrkrankenhäusern und Lehrpraxen. Hier sollten die Universitäten dringend angehalten werden, einen verlässlichen Datenfluss in den Kooperationsvereinbarungen festzuhalten. Das häufig praktizierte Verfahren der Statusgewährung “auf Zuruf” hat sich in der Praxis als aufwändig und inpraktikabel erwiesen.

Es wäre hier zur Reibungsminimierung sicher wünschenswert, wenn die Regelungen der Universitäten harmonisiert werden, da eine allzu große Abweichung ein großes Konfliktpotential und einen Koordinationsaufwand bewirkt.

Letztlich ist eine exakte Gleichförmigkeit der Bestimmungen jedoch nicht zwingend erforderlich. Was jedoch erforderlich ist (und die praktische Erfahrung lehrt, dass dies noch nicht überall der Fall ist) ist eine exakte Definition der Personengruppen innerhalb der einzelnen Hochschulen, sodass diese einen einheitlichen Status an das föderierte Identitätsmanagement zuverlässig weitergeben können. Einzelfallentscheidungen sind hier jedenfalls bestenfalls als Notbehelf anzusehen und zu vermeiden.

Nicht vom Hochschulgesetz erfasst ist die Gruppe der **Alumni**. Diese ist nur an der RWTH Aachen öffentlich definiert und zwar als Menge der ehemaligen Angehörigen und Mitglieder und umfasst damit insbesondere auch alle ehemaligen Studierenden. Die Definition erscheint zweckmäßig und daher zu empfehlen.

Die DFN-AAI verwendet für die Statusgruppen die Attribute eduPersonAffiliation und scopedEduPersonAffiliation. Es kennt folgende Werte:

faculty: Mitglied des Lehrkörpers
student: Studierende
staff: Mitarbeitende, die nicht zum Lehrkörper gehören
employee: faculty, staff und sonstige Angestellte
alum: Alumni
member: faculty, staff, student
affiliate: Partner der Organisation wie Gasthörer, Gastdozenten
library-walk-in: Mitarbeiter, die sich (physikalisch) in der Bibliothek befinden

Das Attribut bleibt leer, wenn alle Kategorien nicht passen. [6] Es ist ein Multivalue-Attribut. Der Wert *member* wird zusätzlich zu *faculty*. *staff*, *employee* oder *student* vergeben. An einigen Hochschulen erhalten alle Mitarbeitenden den Wert *staff*, sodass *employee* und *faculty* gar nicht verwendet werden. Der Wert *member* wird in der Föderation so verstanden, dass er sowohl Mitglieder wie auch Angehörige umfasst. Eine einheitliche Handhabung in NRW bei der Vergabe der Werte ist zu begrüßen.

5.3. Evaluierung von Technologien

Ein Ziel der Machbarkeitsstudie DH.NRW föderiertes Identity Management (IDM) war, die aktuellen technischen Möglichkeiten und Entwicklungen im Bereich der Authentifizierung und Autorisierung zu recherchieren, die heute, neben der bereits etablierten IDM-Föderation DFN-

AAI [7], an der alle NRW-Hochschulen partizipieren, eine weitere Lösung für DH.NRW darstellen könnten. Dabei wurde bereits in der Projekt-Kick-off-Veranstaltung durch den Impulsvortrag [8] von Herrn Dr. Nussbaumer vom KIT aus Baden-Württemberg klar, dass man zwei Kategorien betrachten muss, um die Anforderungen von Services an Authentifizierung und Autorisierung zu realisieren: Web- und Nicht-Web-Technologien. Um die Nachhaltigkeit der Recherche zu erhalten, wurde als Dokumentationsplattform ein Wiki [9] mit einheitlichen Fragestellungen etabliert, dass auch in Zukunft ein Einstiegspunkt für alle Interessierten in ganz NRW bleiben soll. Dabei war es nicht das Ziel jede einzelne Technologie im Detail zu beschreiben, sondern sinnvolle Verlinkungen zu Einstiegsseiten und Standardisierungen wie RFCs (Request for Comments) zu bündeln und mit nützlichen Informationen anzureichern wie zum Beispiel, welche Hersteller die Technologien unterstützen, weiterentwickeln oder auch erfolgreich einsetzen.

Begriffsverständnis Technologie

Die Arbeitsgruppe IDM.NRW hat bewusst den Begriff „Technologie“ gewählt, um eine hinreichende Abstraktionsebene zu einer konkreten Implementierung oder zu innerhalb einer Technologie verwendete Protokolle zu erreichen. Durch diesen hohen Abstraktionsgrad lassen sich Vergleiche zwischen Technologien ziehen, die in der konkreten Manifestierung sehr heterogen sind. So wurden zum Beispiel SAMLV2, Azure-AD oder LDAP auf eine Stufe gestellt. Dieses Verständnis erlaubt es, in einer späteren genaueren Evaluation bereits Kandidaten zu filtern, die auf einer abstrakten Ebene nicht die Anforderungen eines DH.NRW Services erfüllen. So eignet sich zum Beispiel eine Authentifizierungsmethode mit einem reinen LDAP-Server eher für lokale Authentifizierungen innerhalb einer Hochschule als über verschiedene Hochschulen hinaus.

Datenerfassung im Wiki

Die folgenden Fragenstellungen wurden für jede Technologie analysiert und als Wiki-Kapitel pro Technologie dokumentiert:

1. **Allgemeine Beschreibung**
   Grobe Beschreibung/Skizze oder Verlinkung auf Einstiegsseiten einer Technologie.

2. **Offizielle Standardisierung**
   Verlinkung auf RFCs oder Webseiten von Konsortien, die die genaue Spezifikation beinhalten

3. **Technologischer Kontext**
   Auslistung weiterer Kontexte und Protokolle, die im technologischen Kontext stehen wie zum Beispiel SAMLv2 zu http (Hypertext Transfer Protocol).

4. **Geeignet für**
   Was sind Stärken der Technologie? Ist sie beispielhaft für mobile Anwendungen geeignet? Dient sie für Benutzeranmeldungen oder eher zur Authentifikation auf Applikationsebene?

5. **Beteiligte Konsortien**
   Wer entwickelt die Technologie maßgeblich weiter, welche Teilnehmer stechen besonders hervor?

6. **Implementierungen**
   Gibt es kommerzielle oder nichtkommerzielle Software, die die Technologie bereits implementiert hat? Wenn ja, welche?

7. **Erfolgreich eingesetzt in**
   Gibt es erfolgreiche Projekte oder Services, die die Technologie einsetzen?

8. **Bekannte Probleme**
   Sind Probleme (mit einer bestimmten Version) der Technologie bekannt?

Betrachtete Technologien

Die folgenden Technologien wurden nach den genannten Fragestellungen ausgewertet:

SAMLv2

Die Standard Security Assertion Markup Language (SAML) definiert einen Rahmen für den Austausch von Sicherheitsinformationen zwischen Entitäten. Er wurde vom Security Services Technical Committee (SSTC) der Standardisierungsorganisation OASIS (Organization for the Advancement of Structured Information Standards) entwickelt. [10]

OAuth 2.0 mit OpenID-Connect 1.0

OpenID Connect 1.0 ist eine einfache Identitätsschicht auf dem OAuth 2.0-Protokoll. Sie ermöglicht es Clients, die Identität des Endbenutzers auf der Grundlage der von einem Autorisierungsserver durchgeführten Authentifizierung zu überprüfen und grundlegende Profilinformationen über den Endbenutzer auf interoperable und REST-ähnliche Weise zu erhalten.

OpenID Connect ermöglicht es Clients aller Art, einschließlich webbasierter, mobiler und JavaScript-Clients, Informationen über authentifizierte Sessions als auch Benutzer anzufordern und zu erhalten. Die Spezifikationssuite ist erweiterbar, sodass Teilnehmer optionale Funktionen wie die Verschlüsselung von Identitätsdaten, die Ermittlung von OpenID-Providern und die Sitzungsverwaltung nutzen können, wenn dies für sie sinnvoll ist. [11]

Kerberos

Kerberos bietet Mittel zur Überprüfung der Identität zwischen Entitäten, (z.B. einem Workstation-Benutzer und einem Netzwerkserver) auf einem offenen (ungeschütztem) Netzwerk. Dies wird erreicht, ohne sich auf Angaben des Host-Betriebssystems zu verlassen, ohne Vertrauen in die Adresse des Hosts, ohne physische Sicherheit aller Zugriffe auf das Netzwerk als auch unter der Annahme, dass Pakete im Netzwerk nach Belieben gelesen, verändert und eingefügt werden können. Kerberos führt unter diesen Bedingungen eine Authentifizierung als vertrauenswürdiger Dritter unter Verwendung konventioneller (shared secret) Kryptographie durch. [12]

ADFS

Active Directory Federation Service (ADFS) ermöglicht ein föderales Identitäts- und Zugriffsmanagement durch die sichere gemeinsame Nutzung digitaler Identitäts- und Berechtigungen über Sicherheits- und Unternehmensgrenzen hinweg. ADFS bietet die Möglichkeit, Single-Sign-on-Funktionalität, die sonst nur innerhalb einer einzigen Sicherheits- oder Unternehmensgrenze verfügbar ist, für internetfähige Anwendungen zu verwenden. [13]

FIDO

Basierend auf freien und offenen Standards der FIDO-Alliance ermöglicht die FIDO-Authentifizierung, sonst nur passwortgeschützte Anmeldungen durch sichere und schnelle Verfahren über Websites und Anwendungen zu ersetzen. [14]

FIDO2

FIDO2 ermöglicht es den Benutzern, gängige Geräte zur einfachen Authentifizierung bei Online-Diensten sowohl in mobilen als auch in Desktop-Umgebungen (statt Passwörter) zu nutzen. [15]

HTTP-Basic-Authentication

Das Basic-Authentifizierungsschema basiert auf dem Modell, dass sich der Benutzer mit einer Benutzerkennung und einem Passwort bei einem einzelnen Namensraum ("Realm"), z.B. einer Webseite, authentifiziert, [16] ein Gegensatz zu SSO-Verfahren. Die http-Basic-Authentifizierung sollte nur mit HTTPS verwendet werden.

HTTP-Digest-Authentication

Das Digest-Schema basiert auf einem einfachen Challenge-Response-Paradigma. Das Digest-Verfahren fordert die Nutzung eines einmaligen Wertes (nonce) und signalisiert, dass Benutzernamen-Hashing verwendet wird. Eine gültige Antwort enthält einen

unverschlüsselten Digest des Benutzernamens, des Passworts, des angegebenen Nonce-Wertes, der HTTP-Methode und der angeforderten URI. Auf diese Weise wird das Passwort niemals im Klartext gesendet. [17]

SCIM

Das SCIM-Protokoll ist ein HTTP-basiertes Protokoll auf Anwendungsebene zur Bereitstellung und Verwaltung von Identitätsdaten im Web und in domänenübergreifenden Umgebungen, wie z.B. bei Anbietern von Enterprise-to-Cloud-Diensten oder in Inter-Cloud-Szenarien. Das Protokoll unterstützt die Erstellung, Änderung, den Abruf und die Ermittlung von zentralen Identitätsressourcen wie Benutzern und Gruppen sowie von benutzerdefinierten Ressourcen und Ressourcenerweiterungen. [18]

CAS

CAS ist eine Single-Sign-On-Lösung für Webdienste. CAS bietet eine Open-Source-Community, die das Projekt aktiv unterstützt und dazu beiträgt. Das Projekt hat seine Wurzeln im Open Source-Bereich, ist aber inzwischen auf ein internationales Publikum angewachsen, das sich aus Fortune-500-Unternehmen und kleinen Spezialinstallationen zusammensetzt. [19]

Zertifikate

Digitale Zertifikate sind elektronische Berechtigungsnachweise, die verwendet werden, um die Online-Identitäten von Einzelpersonen, Computern und anderen Einheiten in einem Netzwerk zu bestätigen. Digitale Zertifikate funktionieren ähnlich wie Identifikationskarten wie z.B. Pässe und Führerscheine. Sie werden von Zertifizierungsstellen (Certification Authorities, CAs) ausgestellt, die die Identität des Zertifikatsinhabers sowohl vor der Ausstellung des Zertifikats als auch bei der Verwendung des Zertifikats überprüfen müssen. [20]

LDAP

Das Lightweight Directory Access Protocol (LDAP) ist ein leistungsfähiges Protokoll für den Zugriff auf Verzeichnisse. Es bietet die Möglichkeiten zum Suchen, Abrufen und Manipulieren von Verzeichnisinhalten und Zugriff auf eine reichhaltige Palette von Sicherheitsfunktionen.
Benutzerauthentifizierung erfolgt durch die BIND-Operation. Der BIND-Vorgang bietet anonyme, nichtauthentifizierte und Benutzername/Passwort-Varianten, sowie einen einfachen Zugriff auf die SASL (Simple Authentication and Security Layer) – Methode, die eine Vielzahl von weiteren Authentifizierungsmechanismen unterstützt. [21]

SSH

Das Secure Shell (SSH) Protocol ist ein Protokoll zur sicheren Anmeldung an entfernten Diensten und sicheren Netzwerkdiensten durch ein unsicheres Netzwerk. [22]
Dabei werden die Authentifizierungsmethoden „publickey, password, hostbased“ und „none“ unterstützt. [23]

Zwischenergebnis

Die Projektgruppe IDM.NRW hält einen Ansatz wie in Baden-Württemberg (bwIDM) für sinnvoll: für Authentifizierung an Webdiensten ist die wichtigste Strategie auf SAMLv2 in der DFN-AAI-Föderation zu setzen. Nach den bisherigen Umfrageergebnissen partizipieren nahezu alle Universitäten und Fachhochulen bereits in dieser Subföderation. Um die NRW-spezifischen Anforderungen der Services umzusetzen wird empfohlen, das Attributschema um NRW-spezifische Attribute zu erweitern, die nur innerhalb NRWs sichtbar sind und sehr dienstspezifisch ausfallen können. Dieses Modell bietet eine hohe Flexibilität - ohne Auswirkungen auf alle anderen Dienste in der Föderation zu haben. Das bwIDM ist damit sehr erfolgreich.
Auch bei allen weiteren zusätzlich erforderlichen Technologien soll die Prämisse gelten, dass sich die Benutzer möglichst ausschließlich an ihren Heimateinrichtungen authentifizieren, damit Passwörter nicht in der DH.NRW verteilt werden müssen.
Die weitere Anforderungsanalyse der DH.NRW Services hat ergeben, dass für Nichtwebdienste LDAP- und SSH-Authentifizierung (z.B. für Konsolenzugänge) erforderlich sein werden.
Gerade für die beiden letztgenannten könnte SCIM eine interessante Möglichkeit bieten, Identitätsinformationen innerhalb der DH.NRW auszutauschen.
Durch eine größere Verbreitung im kommerziellen Umfeld und großer Unterstützung namhafter Unternehmen (Akamai, Google, Microsoft, Verizon, etc.) ist es sinnvoll in einem Folgeprojekt zu analysieren, wie leistungsfähig OpenID-Connect im universitären Umfeld ist. Eine erfolgreiche Realisierung scheint nach heutigen Erkenntnissen auch die Möglichkeit zu schaffen, eine große Anzahl an kommerziellen Clouddiensten für die Universitäten und Fachhochschulen zu erschließen.
Etwas diffus ist die Lage bei Microsoft nahen DH.NRW Services. Hier waren die betroffenen Dienste noch nicht weit genug im jeweiligen Projekt, um klare Anforderungen zu formulieren. Dies könnte IDM.NRW noch vor eine größere Herausforderung stellen, da ein föderiertes ActiveDirectory für ganz NRW nach heutigen Erkenntnissen sehr komplex und auch (sicherheits-)risikobehaftet zu sein scheint.
Dieser Aspekt verdeutlicht auch, dass IDM.NRW ein dauerhaft angelegtes Projekt sein muss, da sich im Laufe der Zeit Änderungen an den Anforderungen ergeben und neue Services mit neuen Anforderungen hinzukommen werden. Um eine umfangreiche Technologieanalyse zu

gewährleisten, wird im Folgeprojekt IDM.NRW eine detaillierte Evaluierung der genannten Technologien erfolgen.

5.4. Schaffung eines landesweiten Konsenses in NRW

Um die in Kapitel 4 identifizierten Anforderungen und in den Abschnitten 5.1 – 5.3 beschriebenen Lösungsansätze bedarfsgerecht weiterzuentwickeln und im Nachgang in NRW zu etablieren, ist eine Herangehensweise zur Erreichung eines landesweiten Konsenses notwendig. Hierzu wurde ein 3-Phasen-Modell aufgestellt, dass im Weiteren näher erläutert wird.

Um eine langfristige und großflächige Einbindung lokaler IDM Systeme in die Föderation zu gewährleisten, ist es wichtig, die Einrichtungen in NRW bereits in den frühen Phasen des Hauptprojekts, einzubinden. Die erste Anlaufstelle sind Einrichtungen, die in den IDM- und Servicebefragungen konkrete Anforderungen, wie beispielsweise „Gemeinsame Attribute“ oder „zentrale Personengruppen-Definition“ an das Vorprojekt IDM.NRW gestellt haben. Diese werden in der ersten Phase zu Gesprächen eingeladen, um die gestellten Anforderungen zu spezifizieren und großflächig abdecken zu können. Nach intensivem Austausch werden die Grobkonzepte weiterentwickelt und zu fertigen Fachkonzepten ausgearbeitet. Diese werden in der zweiten Phase den Anforderungsstellern in Form eines landesweiten Workshops vorgestellt. Hierdurch soll zum einen Feedback eingeholt werden, um die Vorschläge zu perfektionieren und zum anderen soll die Möglichkeit gegeben werden an den Lösungskonzepten mitzuwirken. Je nach Rückmeldung werden die Fachkonzepte finalisiert und zur Verfügung gestellt. Nachdem die Anforderungssteller ihr schriftliches Kommittent abgeben und somit in die Föderation eintreten, startet die dritte Phase.

In der dritten Phase tritt die Föderation mit ihren Mitgliedern nach außen und stellt die fertigen Konzepte regelmäßig in Form von Workshops (z.B. im ZKI, IDM Techniktreff NRW, etc.) vor. In diesen Workshops sollen ebenfalls Services vorgestellt werden, die innerhalb des Hauptprojekts erprobt wurden und föderativ angeboten werden.

Gleichzeitig wird ein Rahmenwerk ausgearbeitet, dass die Teilnahmebestimmung an der IDM.NRW Föderation festlegt. Diese werden zur Sammlung von Kommittent verschriftlicht. Die inhaltlich finale Ausarbeitung des Rahmenwerks erfolgt im Hauptprojekt.

6. Umsetzungsplanung

Die Stärkung der Infrastruktur steht im Fokus des Projektvorhabens. Das Ziel des Projektvorhabens Machbarkeitsstudie föderiertes Identity Management war die Erarbeitung und Konzeptionierung einer gemeinsamen Vorgehensweise zur Etablierung eines föderierten Identity Managements zusammen mit allen Partnern für Nordrhein-Westfalen (NRW). Durch die Umsetzung der Machbarkeitsstudie soll durch die Bereitstellung einheitlicher IDM-Prozesse die Grundlage zur einfachen und einheitlichen Nutzung von Services diverser Hochschulen gewährleistet sein.

Aus der Machbarkeitsstudie föderiertes Identity Management ergaben sich neue Erkenntnisse zu relevanten Anforderungen an ein föderiertes Identity Management. Die Erkenntnisse der Studie wurden bereits bei der Entstehung der Daten auf eine nachhaltige Verwertbarkeit ausgelegt. Das generierte Konzept trägt wesentlich zur Weiterentwicklung und Vereinheitlichung bei Prozessen rund um das Identity Management bei. Prozesse werden ggfs. einmal entwickelt und können an allen Mitgliedseinrichtungen von DH.NRW genutzt werden. Das gemeinsame Verständnis erhöht die Durchlässigkeit bei der Prozessorganisation. Für die gegenseitige Serviceerbringung ist dies eine Voraussetzung. Von den Ergebnissen der Machbarkeitsstudie wurde ein Konzept in NRW entwickelt, welches im Folgeprojekt Föderiertes Identity Management.nrw umgesetzt werden soll. Die genauen Arbeitsfelder werden im Weiteren näher beschrieben.

Innerhalb des Projektvorhabens Föderiertes Identity Management.nrw werden die beschriebenen Aufgaben vornehmlich durch das IT Center der RWTH Aachen University koordiniert und mit Unterstützung der Partner durchgeführt. Wichtigstes Element ist daher die enge Zusammenarbeit der Mitarbeitenden mit entsprechender Expertise im Bereich Identity Management aller beteiligten Hochschulen. Zuzüglich wird das Arbeitspaket „Evaluierung von (neuen) Technologien“ in Kooperation mit der KIT-SCC im Rahmen der Allianz bwIDM-idm.nrw bearbeitet. Dadurch werden eine länderweite Kooperation und die Passfähigkeit beider Konzepte gewährleistet.
Die Umsetzung kann dabei in folgende Bereiche und Schwerpunkte gegliedert werden:

Projektmanagement und Kommunikation
In diesem Arbeitspaket wird die Vision des Folgeprojekts, mithilfe von Leitfragen, näher beschrieben. Des Weiteren werden Koordinations- und Kommunikationswerkzeuge festgelegt. Dazu gehört die Festlegung von Terminen für regelmäßige (virtueller) Treffen und die Bestimmung von Dokumentationstools. Die Projektgruppe wird hierzu von den positiven Erfahrungen aus dem Vorprojekt Gebrauch machen.

Erarbeitung der Konzepte

Innerhalb eines Jahres sollen, die im Vorprojekt skizzierten Grobkonzepte zu fertigen Fachkonzepten ausgearbeitet werden. Dazu gehören die Konzepte „Gemeinsame Attribute in NRW“, „Zentrale Personengruppen“ und „Evaluierung von Technologien“. Wie bereits erwähnt, wir Letzteres gemeinsam mit der Projektgruppe bwIDM aus Baden-Württemberg bearbeitet, um so zum einen von Wissensteilung zu profitieren und zum anderen einen ersten Schritt in bundesweite Kooperation zu machen.

Konsensschaffung in NRW

Dieses Arbeitspaket ist eine Daueraufgabe des Projektvorhabens und wird daher über die gesamte Projektlaufzeit betrachtet. Um die erarbeiteten Fachkonzepte in NRW zu etablieren ist eine Kommittmentphase unabdingbar. Hierzu wurde das 3 Phasenmodell entwickelt, welches in Abschnitt 5.4 näher beschrieben ist. Besonders wichtig ist, hierbei die Kommunikation nach außen und die geplanten regelmäßigen Workshops mit Einrichtungen aus NRW.

Erprobung der Konzepte anhand von Use Cases

Nachdem die Fachkonzepte fertiggestellt werden, soll innerhalb von 8 Monaten, dessen Erprobung erfolgen. Dazu werden Dienste aus dem Serviceportfolio ausgewählt, die sich gut als Use Case eignen. Pro Dienst findet eine Anpassung der Fachkonzepte statt, sodass nicht nur Themenfelder wie Sicherheit und Datenschutz Beachtung finden, sondern auch Schnittstellen und Datenmodelle ausgearbeitet werden. Am Ende des Arbeitspakets werden die Ergebnisse innerhalb eine Workshops im Konsortium diskutiert und bewertet.

Umsetzung und Partizipation

Innerhalb von 8 Monaten sollen die Lösungen im Konsortium umgesetzt werden. In dem Zusammenhang sollen Betriebsmodelle beschrieben und Dokumente zur Sicherung der Nachhaltigkeit der Ergebnisse erstellt werden. Dazu sollen Best Practice für Dienstanbietende festgelegt werden. Zuzüglich sollen an dieser Stelle die ersten Konzeptansätze für die Verstetigung von IDM.NRW in Form einer Geschäftsstelle erarbeitet werden. Des Weiteren sollen in dieser Phase die lokalen IDMs in die Föderation einbezogen und integriert werden. Im Nachgang werden in einem Abschlussworkshop alle Ergebnisse und Erkenntnisse aus dem Arbeitspaket diskutiert und bewertet.

Verstetigung IDM.NRW

Damit die Föderation IDM.NRW auch nach Projektende weiterhin aktiv bleibt, ist eine Verstetigung in Form einer Geschäftsstelle notwendig. Die letzten 8 Monate des Projektvorhabens dienen zur Konzepterstellung einer solchen Geschäfts- oder Beratungsstelle. Insbesondere die Struktur sowie das Aufgabenumfeld sollen näher beschrieben werden. Im Idealfall wird die Geschäftsstelle mit Ende des Projekts in Betrieb genommen. Die konkrete Beantragung kann jedoch erst mit einem gut durchdachten Konzept erfolgen.

7. Fazit und Ausblick

Das Ziel des Projektvorhabens ist die Erarbeitung und Konzeption einer gemeinsamen Vorgehensweise zur Etablierung eines föderierten Identity Managements in NRW, um zukünftig den Zugriff auf Webdienste sowie Nicht-Webdienste über Hochschulgrenzen hinweg möglich zu machen. Hierzu wurden alle Arbeitsschritte, die im Projektantrag skizziert wurden, nacheinander bearbeitet. Insbesondere die Datenerhebung für die Bedarfsanalyse erwies sich als sehr aufwendig. Zur Datenerhebung wurden die Methoden Onlinebefragung und Experteninterviews ausgewählt. Die Anwendung einer Onlinebefragung eignet sich sehr gut, da diese als häufigstes Befragungsinstrument in Unternehmen, Einrichtungen und Organisationen gilt. Dadurch kann eine breitere Zielgruppe erreicht werden, als wenn persönliche Befragungen durchgeführt werden. Gerade für Forschungsarbeiten eignet sich diese Methode sehr gut, weil zum einen sehr viel Zeit bei der Datenerhebung eingespart wird und zum anderen die Ergebnisse durch qualifizierte Analyse- und Darstellungsmöglichkeiten vorgestellt werden können. Als zweite Datenerhebungsmethode wurden Experteninterviews ausgewählt. Diese eignen sich ebenfalls sehr gut, um Daten zu erheben, da im Gespräch Aussagen vertieft werden können und eine gewisse Flexibilität im Gesprächsverlauf herrscht. Nachfolgend werden die zentralen Erkenntnisse aus der Bedarfsanalyse zusammengefasst.

Durch die Onlineumfrage sowie die Experteninterviews mit den Servicebetreibern kann festgehalten werden, dass für die Umsetzung eines FIDM, sowohl organisatorische wie auch technische Maßnahmen notwendig sind. Zu den Organisatorischen Maßnahmen zählt zum einen die Anforderung gemeinsame Attribute in NRW zu etablieren, um einen standardisierten Datenaustausch zu gewährleisten. Ein weiterer Grund ist die Datensparsamkeit, die dadurch erreicht werden kann. Insbesondere die Festlegung auf ein Standard-Set von Attributen und eine möglichst homogene technische Form der Attributwerte versprechen eine deutliche Erleichterung der Implementierung für zukünftige Services in NRW – sowohl auf Seiten der Service-Anbieter, als auch auf Seiten der konsumierenden Einrichtungen. Des Weiteren hat

sich das Thema zentrale Personengruppen als eine sehr wichtige Anforderung herauskristallisiert. Es ist zwar nicht zu erwarten, dass ein Einvernehmen verschiedener Definitionen von Personengruppen getroffen wird, aber zumindest eine Harmonisierung sollte erreicht werden. Es kann festgehalten werden, dass Institutionen sich langfristig nicht auf eine vollkommen einheitliche Definition verständigen werden, jedoch ist es für die gegenseitige Verständigung notwendig, Konstrukte zu entwickeln um sich zumindest auf gewisse Grundtermini und ihre Bedeutung zu einigen.

Des Weiteren wurde ein Überblick über existierende Verbünde erstell, um ggf. von bestehenden Lösungen zu profitieren. Hierbei wurden die Verbünde nach ihrer Technik, ihrer aufgebauten Struktur und ihrem Erkenntnisgewinn untersucht. Da es eine Vielzahl an Verbünden gibt, wurde eine Einschränkung auf in Deutschland verfügbare Verbünde gemacht. Andere europäische oder internationale Verbünde oder Projekte wurden betrachtet, wenn ein neuartiger oder vielversprechender Ansatz verfolgt wurde. Die dadurch gewonnenen Erkenntnisse werden im Hauptprojekt Anwendung finden. Insbesondere der Austausch mit bwIDM wird sich zu einer Zusammenarbeit weiterentwickeln.

Im Bereich der technischen Maßnahmen hat sich klar herausgestellt, dass Anforderungen der meisten DH.NRW Services, insbesondere derer, die stark auf Webtechnologien setzen, umsetzbar sind. Schwierigkeiten tauchen bei Services auf, die keine Möglichkeit bieten, an ein FIDM gekoppelt zu werden oder Fat-Clients dezentral benötigen.

Die größere Herausforderung wird darin bestehen, eine Vereinheitlichung der Gruppen in NRW zu erreichen und eine für alle IDMs und Services abgestimmte Syntax zu definieren, sowie über deren zeitliche Validität vertragliche Verpflichtung einzufordern. Ein weiteres Risiko besteht darin, wenn die Projektleitungen der DH.NRW-Services den IDM-Fragen nicht genug Projektzeit innerhalb eines Projektes lassen. IDM-Lösungen helfen in der Regel sehr, können aber eine, je nach Anforderung, hohe technische und prozessuale Komplexität aufweisen.
Die Projektgruppe IDM.NRW hält einen Ansatz wie in Baden-Württemberg (bwIDM) für sinnvoll: für Authentifizierung an Webdiensten ist die wichtigste Strategie auf SAMLv2 in der DFN-AAI-Föderation zusetzen. Wie in Abschnitt 5.3 bereits erwähnt, partizipieren fast alle Universitäten und Fachhochulen bereits in dieser Föderation. Um die Serviceanforderungen in NRW umzusetzen wird empfohlen, das aktuelle Attributschema um NRW-spezifische Attribute zu erweitern (siehe Abschnitt 5.1). Das bwIDM in Baden-Württemberg ist damit sehr erfolgreich. Bei weiteren erforderlichen Technologien wird festgehalten, dass sich die Benutzer ausschließlich an ihren Heimateinrichtungen authentifizieren, damit Passwörter nicht in der DH.NRW übermittelt werden. Weitere Ergebnisse aus der Anforderungsanalyse haben gezeigt, dass für Nicht-Webdienste LDAP- und SSH-Authentifizierung (z.B. für Konsolenzugänge) erforderlich sein werden. An dieser Stelle ist zu erwähnen, dass eine

umfängliche Evaluation von Technologien im Folgeprojekt notwendig ist, um auch hierfür Lösungen zu entwickeln.
Schlussendlich lässt sich festhalten, dass IDM.NRW ein dauerhaft angelegtes Projekt sein muss, da sich im Laufe der Zeit Änderungen an den Anforderungen ergeben und neue Services mit neuen Anforderungen hinzukommen werden. Aus diesem Grund ist im Rahmen der Verstetigung die Einführung und Inbetriebnahme einer Geschäfts- und Beratungsstelle IDM.NRW geplant, die sich auch zukünftig neuen Herausforderungen stellen und sowohl große als auch kleinere Einrichtungen unterstützen wird. Zudem hätten zukünftige Services einen direkten Ansprechpartner, wenn es um die Anbindung der Services in die Föderation geht. Die konkrete Umsetzung der Machbarkeitsstudie wird in dem Folgeprojekt, wie in Kapitel 6 beschrieben, realisiert.

8. Literaturverzeichnis

[1] DFN Verein, „Verlässlichkeitsklassen in der DFN-AAI,“ 28 April 2020. [Online]. Available: https://doku.tid.dfn.de/de:degrees_of_reliance. [Zugriff am 28.09.2020].

[2] H. Flanagan, Internet2, 13 August 2020. [Online]. Available: https://wiki.refeds.org/display/STAN/eduPerson+2020-01#eduPerson2020-01-eduPersonAffiliation. [Zugriff am 28 September 2020].

[3] https://doku.tid.dfn.de/de:aai:attributes_best_practice.

[4] https://doku.tid.dfn.de/de:elearning_attributes.

[5] https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=1&bes_id=28364&anw_nr=2&aufgehoben=N&det_id=462886

[6] https://doku.tid.dfn.de/_media/de:dfn-aai-attribute-v.1.0.pdf

[7] Deutsches Forschungsnetz (DFN), „DFN-AAI Dokumentation,“ 24 September 2020. [Online]. Available: https://doku.tid.dfn.de/de:aai:about. [Zugriff am 24.09.2020].

[8] M. Nussbaumer, Vortrag Projektkickoff IDM.NRW: bwIDM - hochschulübergreifendes Identitätsmanagement in Baden-Württemberg, Karlsruher Institut für Informatik KIT, 2020.

[9] N. Sand und N. V. Urbanczyk, „Authentifizierungs- und Autorisierungstechnologien,“ 24 September 2020. [Online]. Available: noch nicht öffentlich zugänglich. [Zugriff am 24.09.2020].

[10] H. Lockhart, B. Campbell, N. Ragouzis, J. Hughes, R. Philpott, E. Maler, P. Madsen und T. Scavo, „Security Assertion Markup Language (SAML) V2.0 Technical Overview,“ OASIS Security Services TC, 25 March 2008. [Online]. Available: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html. [Zugriff am 24.09.2020].

[11] The OpenID Foundation, „Welcome to OpenID Connect,“ February 2014. [Online]. Available: https://openid.net/connect/. [Zugriff am 24.09.2020].

[12] C. Neuman, T. Yu, S. Hartman und K. Raeburn, „The Kerberos Network Authentication Service (V5),“ July 2005. [Online]. Available: https://tools.ietf.org/html/rfc4120. [Zugriff am 24.09.2020].

[13] Microsoft, „AD FS Overview,“ Microsoft, 31 May 2017. [Online]. Available: https://docs.microsoft.com/de-de/windows-server/identity/ad-fs/ad-fs-overview. [Zugriff am 24.09.2020].

[14] FIDO Alliance, „What is FIDO,“ FIDO Alliance, 24 September 2020. [Online]. Available: https://fidoalliance.org/what-is-fido/. [Zugriff am 24.09.2020].

[15] FIDO Alliance, „What ist FIDO2,“ FIDO Alliance, 24 September 2020. [Online]. Available: https://fidoalliance.org/fido2/. [Zugriff am 24.09.2020].

[16] J. Reschke, „The 'Basic' HTTP Authentication Scheme,“ September 2015. [Online]. Available: https://tools.ietf.org/html/rfc7617. [Zugriff am 24.09.2020].

[17] R. Shekh-Yusef, D. Ahrens und S. Bremer, „HTTP Digest Access Authentication,“ September 2015. [Online]. Available: https://tools.ietf.org/html/rfc7616. [Zugriff am 24.09.2020].

[18] P. Hunt, K. Grizzle, M. Ansari, E. Wahlstroem und C. Mortimore, „System for Cross-domain Identity Management: Protocol,“ September 2015. [Online]. Available: https://tools.ietf.org/html/rfc7644. [Zugriff am 24.09.2020].

[19] Apereo Foundation, „CAS,“ 25 September 2020. [Online]. Available: https://apereo.github.io/cas/4.2.x/index.html. [Zugriff am 25.09.2020].

[20] Microsoft, „How Certificates Work,“ 08 September 2010. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc776447(v=ws.10)?redirectedfrom=MSDN. [Zugriff am 25.09.2020].

[21] R. Harrison, „Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms,“ Novell, June 2006. [Online]. Available: https://tools.ietf.org/html/rfc4513. [Zugriff am 25.09.2020].

[22] T. Ylonen und C. Lonvick, „The Secure Shell (SSH) Protocol Architecture,“ January 2006. [Online]. Available: https://tools.ietf.org/html/rfc4251. [Zugriff am 25.09.2020].

[23] T. Ylonen und C. Lonvick, „The Secure Shell (SSH) Authentication Protocol,“ January 2006. [Online]. Available: https://tools.ietf.org/html/rfc4252. [Zugriff am 25.09.2020].

[24] Géant: Federation Architectures, unter: https://wiki.geant.org/display/eduGAIN/Federation+Architectures [Zugriff am 05.10.2020].

[25] Metadata Flow in eduGAIN, unter: https://wiki.geant.org/display/eduGAIN/Metadata+Flow+in+eduGAIN [Zugriff am 05.10.2020].

Anhang

a. Fragenkatalog aus der Onlineumfrage

1. IST-Analyse

1.1. IDM-Konzept

1.1.1.Ist IDM als Konzept vorhanden? (ankreuzen)

ja	nein

1.1.2. An welcher Stelle ist das IDM strategisch in der Hochschule verankert?

1.1.3. Wie stark ist der Rückhalt von IDM durch strategische Unterstützung gewährleistet? (ankreuzen)

sehr stark	stark	weniger stark	gar nicht stark

1.1.4. Wer ist strategischer/organisatorischer/technischer Ansprechpartner? (für Rückfragemöglichkeit)

Strategisch:

Organisatorisch:

Technisch:

1.1.5. Welche Ressourcen werden dafür bereitgestellt, welche fehlen? Ggf. bitte ergänzen (ankreuzen)

Ressourcen	bereitgestellt	fehlt
Geldmittel		
Zeit		
Personal		

1.2. IDM-System

1.2.1. Gibt es ein IDM-System? (ankreuzen)

ja	nein

1.2.2. Welches IDM ist im Einsatz (Hersteller, Eigenentwicklung, …)?

1.3. IDM-Schnittstellen

1.3.1. Welche Systeme sind an das IDM-System angebunden/angeschlossen (Art des Systems und Herstellers)? Welches davon sind Quell- oder Zielsysteme und welches sind beides? (ankreuzen)

System	Art des Systems	Hersteller	Kommentar	Q	Z
Bsp. RWTHonline	Datenbank	TU Graz			
…					

1.3.2. Bewerten Sie die Systeme nach ihrer Datenqualität und geben Sie an, wie der Datenaustausch geregelt ist. (ankreuzen)

System	sehr hohe Qualität	hohe Qualität	weniger hohe Qualität	gar keine hohe Qualität	täglich	stündlich	on demand	x-Minuten Takt
Bsp. RWTHonline								
…								

1.3.3. Gibt es Sicherheitsbedenken Schnittstellen nach außen anzubieten? (Werden an Ihrer Hochschule z.B. Firewalls/Zwangsproxys/Portfilter eingesetzt, die möglicherweise den Zugriff von außen über Authentifikationsprotokolle (z.B. AD/LDAP) behindern?) (ankreuzen)

ja	nein

1.3.4. Ist das IDM ein zentraler Datenverteiler oder gibt es noch andere Möglichkeiten Daten zu beziehen bzw. zu verteilen? Wenn ja, welche?

1.3.5. Gibt es Prozesse im IDM, die regelmäßiges händisches Eingreifen durch den Support oder das IDM-Team erfordern? (ankreuzen)

ja	nein

Wenn ja, wie sieht der Arbeitsablauf aus (grobe Beschreibung):

1.4. IDM-Daten

1.4.1. Wird die Eindeutigkeit von Identitäten gewährleistet? (ankreuzen)

ja	nein

Wenn ja, wie:

1.4.2. Gibt es eine Identität pro Menschen oder pro Rolle? (ankreuzen)

pro Mensch	pro Rolle

Falls pro Rolle, sind die Identitäten untereinander verknüpft?

ja	nein

1.4.3. Gibt es Funktionsidentitäten? (ankreuzen)

ja	nein

Werden diese von einer oder mehreren Personen genutzt?

eine Person	mehrere Personen

1.4.4. Ermöglichen Sie den Nutzenden für ihre Accounts separate Kennwörter zu setzen? (ankreuzen)

ja	nein

1.4.5. Wie findet die Registrierung bzw. die Identitätsüberprüfung statt (Personalausweiskontrolle, …etc.)?

1.4.6. Wie ist der Lifecycle geregelt (Wie werden Identitäten aus dem IDM-System gelöscht)?

1.4.7. Werden Uni-Kennungen an Drittsysteme weitergegeben? (ankreuzen)

ja	nein

1.5. IDM-Authentifizierung

1.5.1. Welche Authentifizierungssysteme gibt es und welche werden als AaaS (= Authentification as a Service) angeboten? (ankreuzen)

Authentifizierungssysteme	vorhanden?	Kommentar
AD		
LDAP		
IdP: SAML		

IdP: SAMLv2		
IdP: OpenID		
IdP: OAuth		
IdP: Kerberos		
IdP: CAS		
Account WS		
Etc.		

1.6. IDM-Autorisierung

1.6.1. Welche zentralen Personengruppen werden hinsichtlich ihrer Rechte im IDM-System unterschieden?

1.6.2. Gibt es eine Rollen-/Rechte-/Gruppenverwaltung? (Bsp.: zu welchem Lehrstuhl gehörend, zu welchem Projekt, zu welcher Nutzendengruppe gehört jemand, etc.)? (ankreuzen)

ja	nein

Wenn ja, wie ist die technische Realisierung:

1.6.3. Werden Anfragen abgelehnt, die mittels dieses Konzepts nicht unterstützt werden können? (ankreuzen)

ja	nein

1.7. Hochschulübergreifende Kooperationen

1.7.1. Gibt es an Ihrer Hochschule bereits hochschulübergreifende Kooperationen als Anbieter/Nutzender (z.B. E-Learninganwendungen)? (ankreuzen)

ja	nein

Wenn ja, wie werden die Identitäten dort übermittelt und wie ist der Support des anbietenden Service geregelt?

Übermittlung der Identitäten:

Supportregelung:

1.7.2. Gibt es an Ihrer Hochschule ein Konzept „nicht Web-Dienste“ föderativ zugreifbar zu machen (insbesondere bezieht sich die Frage auf Apps und Shellaccounts)? (ankreuzen)

ja	nein

Wenn ja, wie ist die technische Umsetzung (grobe Beschreibung):

1.7.3. Gibt es Dienste, bei denen die Anbindung an das IDM bisher gescheitert ist? (ankreuzen) Wenn ja, welche und was war der Grund?

ja	nein

Welche:

Grund:

1.7.4. Wie sehen Ihre Anforderungen an einen Service aus, damit man diesen gut über das eigene IDM-System nutzen kann? Welche davon würden Sie als Mindestanforderung bzw. spezifische Anforderung klassifizieren? (ankreuzen)

Anforderungen	Mindest-anforderung	spezifische Anforderung

1.7.5. Sehen Sie den Bedarf hochschulübergreifend Services zu nutzen bzw. anzubieten?

(ankreuzen) (Hinweis: Ggf. ist für die Beantwortung dieser Frage ein anderer Ansprechpartner notwendig)

ja	nein

Wenn ja, wer ist an Ihrer Einrichtung der geeignete Ansprechpartner hierfür?
(Hinweis: wichtig für Rückfragen um Wünsche zu berücksichtigen)

Ansprechpartner:

b. Fragenkatalog aus der IDM-Nacherfassung

1. Planen Sie die Einführung eines anderen neuen IdM Systems? Wenn ja, welches und warum / was erhoffen Sie sich vom neuen System?

2. Haben/Betreiben Sie Shibboleth?

   ☐ ja
   ☐ nein

3. Haben Sie ein Trouble Ticket System? (ankreuzen)

   ☐ ja
   ☐ nein

   Wenn ja, ist dieses ans IdM angeschlossen?

4. Von wem wird händisch in IDM Prozesse eingegriffen und in welchem Umfang? (ankreuzen und prozentuale Gewichtung)

☐ …% IT ServiceDesk
☐ …% IDM-Fachabteilung
☐ …% sonstige

5. Welche Prozesse sind nicht zu 100% durchautomatisiert?

6. Liegen Kompetenzen/Know-How zu Webservices vor? (ankreuzen)

☐ SOAP
☐ REST
☐ Sonstiges

7. 95,7 % der Universitäten wollen Services hochschulübergreifend nutzen/anbieten, aber haben Sicherheitsbedenken bei Schnittstellen nach außen. Können Sie Ihre Bedenken spezifizieren?

8. Wenn Sie Funktionsidentitäten haben, sind sie von normalen Identitäten unterscheidbar?

9. Warum sind hochschulübergreifende Anbindungen ans IdM gescheitert? Detailliertere Antwort.

10. Weitere Anmerkungen/Anregungen

c. Fragenkatalog aus der Servicebefragung

1. Allgemeine Fragen an den Service

1.1. Wie heißt Ihr Service und was leistet er?

1.2. Wer ist verantwortlicher Betreiber?

1.3. Auf welche Zielgruppe (Kunden) zielt der Service ab?

1.4. Wird der Service bereits von anderen Hochschulen genutzt? Wenn ja, von wie vielen?

1.5. Wie viele Nutzende (Einzelkunden) hat der Service?

1.6. Wie schätzen Sie die weitere Entwicklung der Nutzerzahlen und teilnehmenden Hochschulen ein?

1.7. Für welchen Bereich soll der Service erbracht werden?

1.8. Welche Endgeräte sollen den Service nutzen können?

1.9. Muss der Service besonderen gesetzlichen Anforderungen genügen? Wenn ja, welchen?

1.10. Wie lange ist die Betriebslaufzeit des Service geplant?

☐ für max. 1 Jahr

☐ zwischen 1 und 5 Jahren

☐ mehr als 5 Jahren

1.11. Ist ein Support (ServiceDesk, Anwenderberatung) für diesen Service erforderlich? Wenn ja, wie wird er realisiert (zentral, dezentral, etc.)?

1.12. Wie ist der aktuelle Stand des Service? Stehen (große) Veränderungen an?

1.13. Gibt es ein Betriebskonzept/Sicherheitskonzept?

☐ ja

☐ nein

2. Welche Funktionalitäten erwarten Sie vom IDM?

☐ Gruppenbildung?

☐ Hochschulübergreifende Gruppenbildung?

☐ LifeCycle?

☐ Allgemeine Rollen, Shibboleth affiliations

☐ über welche Schnittstelle/Protokolle soll/kann Ihr Dienst/Service kommunizieren?

☐ Wie können sich die Nutzer an dem Service authentifizieren?

- ☐ über Shibboleth
- ☐ nicht webbasierter Zugriff, über Outlook
- ☐ ….

☐ Sonstige

2.1. Welche Funktionalitäten sind unverzichtbar, welche optional?

2.2. Soll das IDM Autorisierungsinformationen übermitteln? Wie werden diese gepflegt/auditiert?

2.3. Wie und welche Konten-/Nutzerdaten werden (de-)provisioniert?

3. Ressourcen

3.1. Sind finanzielle und personelle Ressourcen für die Umsetzung und den Betrieb vorhanden/eingeplant?

3.2. Welche Mitarbeiter aus dem anfordernden Fachbereich/der Fakultät/der Einrichtung oder anderen Bereichen/Externe müssen noch eingebunden werden?

4. Haben Sie noch Anregungen/Anmerkungen?

5. Einschätzung des Interviewers

☐ machbar
☐ problematisch
☐ risikoreich
☐ kein Plan

d. IDM-ZKI angeschlossene Systeme (bundesweit)

Würzburg

(NetIQ Identity Manager 4.5.3)

HIS SOS, SAP HR, Gästeverwaltung RZ (Oracle), Studierenden- und Mitarbeiterverwaltung HfM (csv), IDM Uni-Klinik Zielsysteme: File und Print (eDirectory), AD (Uni und HfM), UB (Datenbank direkt), Emailsysteme (Groupwise, Cyrus), Web-Server, Datenbanken, VoIP, HIS SOS, eLearning (moodle), LDAP-Authentifizierungs-Server (eDirectory), Schließsystem, Datenbanken für Chipkarte, Gästeverwaltung, Webshop, E-Mail-Und Telefonverzeichnis, IDM Uni-Klinik, Applikation-Server (Linux)

Hagen

(Microsoft Forefront Identity Manager 2010 R2)

HIS SOS (Studierendenverwaltung), SAP HR (Personalverwaltung), SAP OM (Verwaltung der Organisationsstruktur), Microsoft Active Directory, Microsoft Exchange (Mailsystem für die Beschäftigten), Microsoft AD LDS (Zentraler Verzeichnisdienst), Zertifikatsserver (Oracle Datenbank), Communigate Pro (Mailsystem für die Studierenden), Home-Folder Verwaltung für Beschäftigte

---

Ilmenau

(NetIQ/Novell Identity Manager, Version 4.0x)

HISSOS, HISSVA, THUAPOS (Gäste), LDAP-Authentifizierungssystem (eDirectory), E-Mail-System (OpenLDAP), MS Exchange/SharePoint (AD), NDS, Windows-Domain (AD), Zeiterfassung/Zutritt (Primion), TYPO3, Shibboleth IdP, IP-Telefonie (Avaya), ...

Weimar

(NetIQ/Novell Identity Manager, Version 4.0x)

HISSOS, HISSVA, THUAPOS (Gäste), LDAP-Authentifizierungssystem (eDirectory), E-Mail-System (OpenLDAP), MS Exchange (AD), eDirectory, Windows-Domain (AD), Zutritt (Primion), Shibboleth IdP, HISLSF, E-Learning (metacoon), Mitarbeiter-/Studentenkarte (thoska), ...

Jena

(NetIQ/Novell Identity Manager, Version 4.0x)

- Studentenverwaltung (HISSOS)
- Personalverwaltung (HISSVA)
- Gästeverwaltung (THUAPOS)
- E-Mail-System (OpenLDAP)
- div. Authentifizierungssysteme (OpenLDAP, Active Directory, eDirectory, RADIUS)
- Andrew File System
- Zentrales Universitätsdateisystem (EMC Isilon)
- MS Exchange (Active Directory)

- Förderatives Authentifizierungssystem (Shibboleth IdP)
- Telephonverwaltung (Integrationsserver für DeTeWe CMG)
- Portal (Liferay)
- Bibliothek (LBS via OCLC IDM-Connector)
- Registrierungsdienst für MS-Office-365-ProPlus-Abo (thuEdu365 in Ilmenau)

Erfurt

(NetIQ/Novell Identity Manager, Version 4.0x)

HISSOS (Studierendenverwaltung), HISSVA (Personalverwaltung), THUAPOS (Gästeverwaltung), Sun One Directory (E-Mail-System), NDS, OAS (Operatives Auskunftsportal), eDirectory (LDAP-Authentifizierungssystem), Shibboleth IDP (Förderatives Authentifizierungssystem), thoska+ (Chipkarte: Dienst- und Studierendenausweis)

Chemnitz

(Eigenentwicklung auf Basis von Open-Source-Software (Python/Django))

- Quellsysteme:
  - HIS-SVA
  - HIS-SOS
  - HIS-Bau
  - Kartenverwaltung
  - TucEd Studierendenverwaltung
- Zielsysteme:
  - Account: 2 Active Directory Domains, LDAP Cluster, Kerberos, RADIUS, Shibboleth
  - Storage: AFS Home, CIFS, AFS Projektverzeichnisse, Dateiaustauschdienst, Versionsverwaltungsdienst
  - Mail: MTA (exim), Cyrus, Exchange
  - Datenbankdienst: MySQL, PostgreSQL
  - Sync & Share-Dienst
  - VoIP Telefonanlage
  - Türzugang
  - Gruppen: Verwaltung von AD-, AFS-, LDAP und Exchange-Gruppen
  - Virtuelle Server
  - Papercut Abrechnung
  - Software-Verwaltung/Lizenz-DB
  - OTRS Helpdesk
  - Admin-Dienste
  - WebDNS
  - Fax/UMS

Darmstadt

(NetIQ/Novell Identity Manager, Version 4.x)

SAP/HCM via LDAP Container, Campusnet (TUCaN) via FileImport, Gäste über LDAP-Container, LDAP-Authentifizierungssystem (eDirectory), Active Directoty, MS Exchange in Arbeit, NDS, ...

Bamberg

(OGiTiX Unimate 2013)

Quellsysteme:

- Personalverwaltungssysteme Universität, Kooperationseinrichtungen und Aninstitute
- Studierendenverwaltung HIS-SOS
- Promovierendeverwaltung in Vorbereitung
- Gästeverwaltung in Vorbereitung
- Kartensystem
- Raumverwaltung

Zielsysteme:

- ActiveDirectory
- Shibboleth mit OpenLDAP als Attributspeicher
- Exchange mit automatisierten Verteilergruppen
- Telefonanlage (Siemens) über Zwischen-LDAP im Testbetrieb

Erlangen-Nürnberg

(Open Source Eigenentwicklung)

Quellsysteme:

- VIVA (SAP - Personalverwaltung)
- HIS GX
- HISinOne
- docDaten (Promovierendenverwaltung)
- aim (Sonstigenverwaltung)
- LOGA - Personalverwaltung des Uniklinikums Erlangen

Zielsysteme:

- OpenLDAP
- Microsoft Active Directory (inkl. MS Exchange)
- HIS GX
- HISinOne

Hohenheim

(NetIQ/Novell Identity Manager, Version 4.x)

- Quellsysteme:
  - HIS-SVA
  - HISInOne-STU
- Zielsysteme:
  - Univention
  - AFS
  - Dovecot Mailserver

  - Ilias
  - Shibboleth IdP
  - Microsoft ActiveDirectory

Bonn

(Open Source Software GOsa (PHP, LDAP))

- Quellsysteme:
  - HIS-SVA
  - HIS-SOS
- Zielsysteme:
  - Kerberos
  - GPFS Speicherdienst
  - Communigate Pro Mailserver
  - Ilias
  - Shibboleth IdP
  - Open LDAP

Wuppertal

(Eigenentwicklung auf einer PostgreSQL - Datenbank mit Shell-, PHP- und Perl-Skripten, sowie einigen Triggerfunktionen auf DB-Ebene)

Quellsysteme:

- HIS-SVA
- HIS-SOS

Zielsysteme:

- CSV
- Open LDAP

Passau

(NetIQ/Novell Identity Manager, Version 4.x)

Quellsysteme:

- Studierendendaten: HIS-SOS
- Personaldaten: VIVA
- Dienstadresse/Funktion: HIS-BAU
- CampusCard: Kartenportal
- Buchungssystem für Sport-Kurse

Zielsysteme:

- PC-Anmeldung, Fileserver: NetIQ eDirectory/Microsoft Active Directory
- E-Mail: Novell GroupWise/Microsoft Exchange
- Authentifizierung: LDAP/Shibboleth

- Netzzugang: eduRoam, openVPN
- Universitätsbibliothek: OCLC IDM-Connector
- Campusmanagement, Vorlesungsverzeichnis, Veranstaltungsanmeldung: Stud.IP
- E-Learning: ILIAS
- VoIP-Telefonanlage: Cisco
- Elektronisches Zutritts- und Schließfachsystem

Dresden

(NetIQ/Novell Identity Manager, Version 4.0.2 (Umstieg auf 4.5 in Planung))

Quellsysteme:

- SAP_HCM
- HIS-SOS
- SAP_HCM Uniklinik
- Dezentrale Organisationsverwaltung (Pilotphase)
- Dezentrale Gruppenverwaltung (in Entwicklung
- Dezentrale Gastverwaltung (in Entwicklung)

Zielsysteme:

- Open LDAP: Authentifizierung/Attributspeicher
- Active Directory Pool: reine Authentifizierung
- Active Directory User: Authentifizierung/Attributspeicher
- Shibboleth mit OpenLDAP als Attributspeicher
- MS Exchange: Auth über AD User
- MS Sharepoint: Auth über AD User
- Unix-Mailer
- Radius
- Projektdatenbank für HPC
- Fileserver
- indirekt diverse weitere Dienste und Systeme

Bielefeld

(Quest One Identity)

Quellsystem ist konzeptionell das IDM, bidirektionale Systeme sind:

- SAP_HCM
- HIS-SOS (wird HISinOne)
- SIAS (Ausleihsystem d. Bibliothek)
- InterCard smartLife (UniCard-Verwaltung)
- Moodle
- Shibboleth
- Bluecat
- Provisionierungssoftware BenVW (Eigenentwicklung in TCL/TK => wird von Quest One Identity funktional abgelöst). Daran sind unidirektional u.a. angebunden:
    - Oracle Mail
    - Radius für VPN/WLan
    - Microsoft ActiveDirectory
    - Cisco Call Manager

- StudIP
- BMC Remedy Helpdesk
- Perimeter-Firewall

Freiberg

(NetIQ/Novell Identity Manager, Version 4.x)

;Quellsysteme: HIS-SOS (Studierendenstammdaten), HIS-SVA (Mitarbeiterstammdaten), Kartenmanagement Pro Services (Chipkartendaten), HIS-COB (Kostenstellen), User Application (Stammdaten Externe; Telefondaten); Zielsysteme: MS AD, Zentrale Nutzerdatenbank (notwendiger Zwischenschritt Shibboleth, kleinere lokale Anwendungen), HIS-POS, Mailserver, Zutrittssystem, Zeiterfassung, Bibliothekssystem Libero

---

HS Köln-Gummersbach

(ForgeRock OpenIDM, Version 2.1)

Quellsystem: AIX NIS (einmalig), Benutzeranträge; Zielsystem: MS Active Directory, ForgeRock openDJ (LDAP)

TU München

(TUMonline (CAMPUSonline) als zentrales IDM, NetIQ/Novell Identity Manager, Version 4.5 als Verzeichnisdienst)

TUMonline Quellen

- SAP/XML TUM (Personendaten, Dienstverhältnisse, Gebäude/Räume, Kostenstellen)
- SAP/CSV MRI (Personendaten, Dienstverhältnisse des Klinikums)
- Studierenden-Import LMU

TUMonline Zielsysteme

- IntegraTUM Directory (DirXML)
- myTUM Directory (DirXML)
- SAP-BW (Statistiken, ...)
- diverse Webschnittstellen (XML/JSON) zu Typo3, OpenERP, Alumni-Community, Karten-Drucker/Validatoren, DMS, ...

IntegraTUM Directory Zielsysteme

- Shibboleth IDP / Authentifizierungsserver
- ActiveDirectory des LRZ (Exchange/Groupware, NAS, VPN)
- Bibliotheks-Directory
- Lokale Verzeichnisse der Fakultäten
- ...

Braunschweig

Quellsysteme: HIS/SOS, SAP/HCM sowie manuelle Erfassung über Antragsformular.
Zielsysteme: LDAP, AD, Ticketsystem (OTRS), CMS-Redaktionssystem (Fiona), Druckkostenabrechnung (PaperCut).

Leipzig

(NetIQ/Novell Identity Manager, Version 4.0.2)

Quellsysteme:

- HIS-SVA (via CSV)
- SAP HR (via CSV)
- CampusNet (via Intermediate Table)
- Dezentrale Gastverwaltung (UserApplication)
- Kostenstellenbaum (via CSV)

Zielsysteme:

- Active Directory (via RemoteLoader)
- Unix-Mailer (via CSV)
- CampusNet (via Intermediate Table)
- Kartendrucksystem ICMS (via Intermediate Table)
- Libero (via CSV)
- indirekt diverse weitere Dienste und Systeme

Marburg

(Eigenentwicklung auf Basis von OpenLDAP als zentraler Datenbank, Python-Skripten zum Datenabgleich sowie AngularJS-basiertem Webinterface; später evtl. HIS-PSV zur Dateneingabe sowie "evolveum midPoint" oder "Pentaho Kettle" zum Datenabgleich)

Datenquellen "Studierende":

- reguläre Studierende (bislang HIS-SOS)
- Gasthörer (bislang Textdatei)
- Teilnehmer sonstiger Programme (z.B. Internationale Sommeruniversität - bislang Excel)
- studentische Gruppen (z.B. AStA, Fachschaften, Uni-Chor... - bislang formlos)
- Tagungs- und sonstige Gäste (bislang formlos durch Tagungsleiter)
- Studierende anderer Hochschulen (bislang Papierformular)
- externe Kursteilnehmer (bislang Excel)
- Bibliotheksnutzer / "Laufkunden" (PICA - geplant)

Datenquellen "Beschäftigte":

- Professoren und Mitarbeiter (bislang SAP via Textdatei)
- apl. Professoren (bislang Papierantrag)
- Lehrbeauftragte (bislang HIS-LSF)
- Landesbedienstete am Klinikum (Klinikums-SAP via CSV-Datei)
- Doktoranden (mit/ohne Vertrag - bislang Papierantrag)
- Gästehaus-Bewohner (bislang Excel)
- Mitarbeiter von Partner-Einrichtungen (bislang Papierantrag)

- Firmen und sonstige Kooperationspartner (bislang Papierantrag)

Quellsysteme:

- HIS-PSV (aus HISinOne)
- Excel-Tabellen (bislang weit verbreitet, Einsatz sollte minimiert und durch HIS-PSV abgelöst werden)
- ...

Zielsysteme

- HISinOne
- OpenLDAP
- Active Directory
- diverse Webanwendungen (Shibboleth, ILIAS, ...)
- ...

Gießen

(Eigenentwicklung auf Basis von X500 und OpenLDAP mit als zentraler Datenbank für ChipKarten, Python-Skripten zum Datenabgleich)

Quellsysteme

- HIS-SOS
- SAP

Zielsysteme:

- OpenLDAP
- ...

Osnabrück

(Drupal 6 (PHP))

Quellsysteme

- HIS-SOS

Zielsysteme:

- OpenLDAP
- Stud.IP

Stuttgart

(Oracle Waveset, Version 8.1 im Betrieb; Migration auf ForgeRock OpenIDM, Version 4.5 in Arbeit)

Quellsysteme

- C@MPUS (CAMPUSonline) - Studierendenverwaltung / Campus Management
- HIS-SVA - Personalverwaltung
- SIAM-DB (Eigenentwicklung) - Gäste- und "Sonstige"-Verwaltung

Zielsysteme

Kaiserslautern

(in Vorbereitung: OpenIdM)

Quellsysteme: HIS-SVA, HIS-SOS, in Vorbereitung: Datenlotsen, MACH. Zielsysteme: OpenLDAP, ActiveDirectory, Communigate, diverse CSV.

LRZ München

(NetIQ/Novell Identity Manager, Version 4.5; Frontend IdM-Portal: Eigenentwicklung (Perl))

Quellsysteme:

- TUMonline via TUM-Directory (NetIQ-Treiber)
- CampusLMU via LMU-Directory (NetIQ-Treiber)
- Hochschule München (JSON)
- LRZ IdM-Portal (delegierte Kennungs- und Projektverwaltung) für übrige Hochschulen und Einrichtungen
- LRZ Personaldatenbank
- diverse LRZ-Dienste für Verbrauchsdaten, Plattenbelegung, Nutzungsstatus

Zielsysteme:

- LRZ Authentifizierungsserver OpenLDAP und eDirectory (NetIQ-Treiber) für die meisten am LRZ betriebenen Dienste (insb. VPN, HPC, Mail außer Exchange, Webhosting, WebDNS, Netzportal etc.)
- LRZ Mail-Directory (NetIQ-Treiber)
- MWN-ADS Active Directory (für Exchange, Online-Speicher, PC-Pools, VMware-Cluster)
- Service Management iET ITSM (NetIQ-Treiber)
- HPC mySQL-DB (Perl)

HS Osnabrück

(NetIQ Identity Manager 4.0.2)

Quellsysteme:

- CampusNet über CIF (NetIQ Treiber) für Studierendendaten
- SAP für Mitarbeiter und Professoren
- ILeGS für Lehrbeauftragte und Gäste (Eigenentwicklung)
- Alumni und Promovierende werden manuell per ldif eingepflegt

 Zielsysteme:

- Active Directory, ein zentrales und für Fakultäten, inklusive Exchange Provisionierung
- Shibboleth

- Text Driver für Türschließsysteme und PICA (in Planung Siemns und Voss)
- Datenbanken, wie z.B. InterCard
- Logik Treiber für Versenden von Emails, Loopback, WorkOrder , FHOS-Entitlement
- eDirectory Verzeichnis Treiber

TU Hamburg-Harburg

(Eigenentwicklung auf Basis von Open-Source-Software: Java (Spring, Hibernate, ICEfaces) + PostgreSQL-Datenbank)

Quellsysteme:

- HIS (Studierende)
- Personalreferat (Beschäftigte)
- LDAP (Kontaktdaten)
- Lehrveranstaltungsplanung (externe Lehrbeauftragte)
- Anbindung weiterer Quellen ist in Planung

Zielsysteme:

- LDAP
- Active Directory
- Mailing
- ... (insgesamt ca. 20)

Münster

Quellen:

(Eigenentwicklung auf Basis einer Oracle-Datenbank. Frontends und Geschäfts-Logik mittels PL/SQL, Java EE, Perl, PHP, APEX.)

- Studierende Uni (HIS-SOS)
- Personal Uni (SAP HCM)
- Personal Klinikum
- Kunstakademie Studierende und Personal
- Studierende mehrerer Weiterbildungseinrichtungen
- Organisationstruktur Uni
- Organisationsstruktur Klinikum
- Studiengänge
- Alumni
- Self-Service

Ziele:

- Open-Source-Mail
- Active Directories (zentrale und in Fachbereichen)
- Web-Server-Park
- SSO
- Netzzugangs-Systeme (Radius)
- Kerberos
- IdP für DFN-AAI
- Forschungsdatenbank

- Druck-Abrechnungssystem
- HPC-Systeme
- Elektronisches Telefonbuch

Augsburg

(Eigenentwicklung auf Basis von Open-Source-Software (OpenLDAP, Python, Perl))

Quellsysteme:

- HIS-SOS
- VIVA (SAP - Personalverwaltung)
- Gästeverwaltung (Eigenentwicklung)

 Zielsysteme:

- OpenLDAP
- MIT Kerberos
- Microsoft Active Directory
- Campus Filesystem
- Digicampus (Stud.IP)
- Mail-System
- Karten-Management-System
- IdP für DFN-AAI

Duisburg-Essen

(Eigenentwicklung (Perl, DB2, Apache, Openldap))

Quellen:

- HISinOne-STU
- SAP-HCM für Mitarbeiter
- Online-Gästeregistrierung
- HIS-LSF (für Kontaktinformationen)
- Grouper (Handpflege von Gruppen)

Ziele:

- LDAP
- AD
- Postfachserver(Exchange und Cyrus)
- Mail-Annnahme und Routing (Ironport und Sendmail)
- Fileserver (Homedirs)
- Mailverteiler (rollenbasierte Mailinglisten)
- TSM-Kontenverwaltung
- Troubelticket-System
- SAP-Benutzerverwaltung

FH Dortmund

(NetIQ/Novell Identity Manager, Version 4.0.2 (Umstieg auf 4.5 teilweise umgesetzt))

Quellsystem:

- HIS-SOS
- HIS-SVA

Zielsysteme:

- NetIQ eDirectory
- openLDAP
- Microsoft AD
- Novell Groupwise 2014
- Listserver (mailman)
- Bibliothek (via OCLC IDM-Connector)

LDAP-Cluster Authentifizierung für:

- CMS (Infosite)
- ILIAS
- DFN-AAI
- Freeradius
- LSF
- Kopierdienst
- OTRS

Düsseldorf

(NetIQ Identity Manager 4.0.2)

Quellsysteme:

- HIS-SOS
- MACH PM
- LSF
- Klinikpersonal-Import
- Gästeschnittstelle des Dozierendenportals
- ZIM-LDAP
- Telefonie-LDAP
- Wählerverzeichnis-Import
- ULB-Aleph

Zielsysteme:

- HIS-SOS
- LSF
- Dozierendenportal
- AD
- ZIM-LDAP
- Telefonie-LDAP
- Shibboleth-LDAP
- Cobra-Alumni-Datenbank

- Typo3

Köln

(MicroFocus/NetIQ/Novell Identity Manager, Version 4.0.2 (demnächst Umstieg auf 4.5))

Quellsysteme: SAP, CampusOnline -Studierendenverwaltung (Oracle Datenbank), UniKlinik (Text-Import),Dispatch für sonstige accounts (MySQL DB) Zielsysteme: AD, LDAP (Telefonie, Shibboleth, Jobserver für Skriptbearbeitung, Kerberos, Ilias und weitere Dienste), , Text-Export (Mail, Export für Campus-Online), MS-SQL (Org-Baum), MySQL(WLAN-Gast)

Bochum

(Eigenentwicklung auf Basis einer Oracle-Datenbank)

Quellsystem:

- HIS-SOS
- HIS-SVA

Zielsysteme:

- LDAP (Oracle Virtual Directory)
- AD
- Bibliothek

Aachen

(Microsoft Forenfront Identity Manager 2010 R2)

Quellsysteme: SAP, SOS, Bibliotheksdaten, div. Coupon-verfahren Zielsysteme: AD, LDAP, div. Exporte, Rollenverwaltung etc.