Einführung eines Identitätsmanagement-Systems an Hochschulen des Landes NRW

hier

Vorabuntersuchung zum Datenschutz

Erstellt von

W. Held (Ms), B. Lix (Dui-E) und

L. Dierking, Forschungsstelle Recht des DFN, Universität Münster

sowie unter Mitwirkung von

G. Bunsen (Ac), R. Conradshaus (Dui-E), M. Fersen (Dui-E), F. Klapper (Bi), R. Mersch (Ms), C. Müller-Böhm (Ms), M. Neuheuser (IuK K) und H. Stenzel (K)

September 2005

Inhalt

1. Bedeutung des Identitätsmanagements

1.1 Was ist Identitätsmanagement

Untersuchungen[1] haben gezeigt, dass an Hochschulen eine gut zweistellige Anzahl in der Regel nicht miteinander verbundenen Benutzerverwaltungen mit je eigenen Benutzerverzeichnissen existieren, mit denen unterschiedliche Einrichtungen[2] die jeweils von ihnen betriebenen IT-Systeme und -Anwendungen[3] verwalten. Identitätsmanagement soll diese historisch gewachsene Vielfalt durch eine einheitliche Verwaltung von Personen einschließlich zugehöriger Kontaktinformationen, Rollen und (Zugriffs-)Rechten ablösen. Dies geht über die reine Identifikation in einem übergeordneten Verzeichnis deutlich hinaus, indem es dafür sorgt, dass dem Nutzer auf allen Systemen, auf denen ihm Rechte zustehen, diese Rechte ohne weitere Anträge und Verwaltungsvorgänge automatisch eingerichtet und ggf. auch wieder entzogen werden (Provisioning). Damit erst schafft sich die Hochschule die Möglichkeit, auf der Basis moderner IT-Infrastrukturen ein zeitgemäßes und konkurrenzfähiges Angebot an integrierten Diensten und Informationen für ihre Mitglieder und Partner sicher und kosteneffizient bereitzustellen und neuen Herausforderungen zu begegnen, mit denen sie sich ständig konfrontiert sieht.

Der Landesrechnungshof NRW hat ein solches Vorgehen nachdrücklich empfohlen[4].

1.2 Identitätsmanagement ist unverzichtbar in einer IT-Infrastruktur

Eine ganze Reihe sich gegenseitig verstärkende Entwicklungen haben nunmehr einen Reifegrad erreicht, bei dem die alten Organisationsformen der *Benutzer*verwaltungen sich als hinderliche und kostenaufwendige Bremse für moderne Dienste erweisen und insbesondere einem sicheren Betrieb des immer komplexer gewordenen IT-Gesamtsystems entscheidend entgegenstehen.
Zu nennen sind vor allem

- Zunahme an Digitalisierung wichtiger Prozesse in Verwaltung, Lehre, Studium und Forschung
- Anstieg der Leistungsfähigkeit und Verfügbarkeit von Netzen und Netzzugängen
- Verbreitung mobiler Endgeräte
- Zunahme der Prozessorientiertheit von IT-Anwendungen, d. h. vollständige, netzbasierte Verarbeitung, bei der bisher getrennte (Teil-)Prozessen aufeinander bezogen und mit Schnittstellen versehen werden
- Informationen, die nicht gut zugänglich aus dem Netz zu beziehen sind, werden von Nutzern oft ignoriert, was zu fatalen Folgen führen kann
- Zunahmen der Bedeutung von Sicherheitsmaßnahmen zur Abwehr immer häufigerer und immer gefährlicherer Angriffe von außen und innen und zur sachgerechten Be-

---

[1] z. B. bei der Erstellung der Feinkonzepte für das Identity Management an den Universitäten Duisburg-Essen, Bielefeld und Aachen

[2] wie z. B. Bibliothek, Rechenzentrum, Verwaltungsdatenverarbeitung, Technische Betriebszentrale, Fachbereiche, Institute, Lehrstühle

[3] wie E-Mail, Web, Backup und Archiv, Fileserver, HIS-Systeme der Verwaltung, BSCW-Server, Telefon, Fax, Zugang zu Räumen und Computern, Zugriff auf das Hochschulnetz und Teilnetze, auch von mobilen und weit entfernten Endgeräten aus,…..

[4] „Prüfung von IT-Services und IT-Schulungen an den Hochschulen“ vom 28. April 2005, Seite 16

wältigung der aus funktionalen Gründen unerlässlichen Integration ehemals getrennter Prozesse der wissenschaftlichen und administrativen Informationsverarbeitung
- Herausforderungen, die von außen durch zunehmenden Wettbewerb um Ressourcen und Studierende sowie Bologna-Prozesses an die Hochschulen herangetragen werden.

Die Autonomie der Hochschule, die Einführung neuer Studienabschlüsse und die damit verbundenen administrativen Detail-Aufgaben im Studienablauf und Prüfungswesen sind konkrete Beispiele der wachsenden Bedeutung der IT-Unterstützung. Diese und viele der anderen Aufgaben zur Steuerung und Verwaltung einer Hochschule, zur Qualitätssicherung sowie zur Steigerung der Leistungen in der Wissenschaft machen einen weiter stark wachsenden IT-Einsatz in vernetzten Umgebungen erforderlich, wie das in den Erläuterungen zum § 30 des Hochschulgesetzes vom Jahre 2000 vorhergesehen wurde.

1.3 Anwendungsbereiche des Identitätsmanagements

Integriertes Servicemanagement und Servicequalität

Viele IT-Aufgaben sind personenbezogen. Personen muss im erlaubten Umfang Zugang zu vielfältigen IT-Ressourcen gewährt werden und andere Mitglieder der Hochschulen benötigen für ihre tägliche Arbeit verlässliche und sichere, den Missbrauch ausschließende Zugänge zu personenbezogenen Daten. Die notwendige Basis für derartige Zugangssteuerungen und Services kann manuell nicht geleistet werden. Wirtschaftliche Zwänge gebieten ohnehin den IT-Einsatz. Ein Basiselement dieser IT-Services ist das Identitätsmanagement. Es ist Mittelpunkt aller kontrollierten und kontrollierbaren Zugänge zu Ressourcen und Informationen. Integriertes Servicemanagement bietet jedem Mitglied der Hochschule zur wirksamen Unterstützung von Forschung, Lehre, Studium, Verwaltung und Öffentlichkeitsarbeit und unter Berücksichtigung seiner Rolle(n), Aufgaben und persönlichen Berechtigungen einen einheitlichen, direkten und vollständigen Zugang zu allen Diensten, Informationsquellen und Kommunikationspartnern an. Das Identitätsmanagement gewährleistet die Verlässlichkeit, die im Sinne der Gesetze, insbesondere der Datenschutzgesetze, zwingend notwendig ist. Das Identitätsmanagement ist Voraussetzung dafür, dass personalisierte Portale für unterschiedliche Gruppen eingerichtet werden können, die den Hochschulmitgliedern entsprechend ihren Rollen und Rechten die notwendigen Arbeitsumgebungen mit Software und Informationen erschließen. Über das Identitätsmanagement ist ein Single-Sign-On zur Arbeitserleichterung und zur Verbesserung der Sicherheit erforderlich. Auf diese Weise wäre ganz offensichtlich eine erhebliche Verbesserung der Servicequalität erreicht, die noch gesteigert werden kann, wenn die einzelnen IT-gestützten Dienste über ein gemeinsames Portal zugänglich werden.

Effizientere Organisation und Wirtschaftlichkeit

Die heute noch üblichen kleinteiligen Benutzerverwaltungen mit eigener, in der Regel immer wieder neuer manueller Aufnahme der Nutzer bei jeder Einrichtung und nachfolgender Zuordnung von Berechtigungen auf den dort verwalteten IT-Systemen[5] (Accounts) sind höchst ineffizient. Diese Vielfalt paralleler Administrationsprozesse für dieselben Daten derselben Person auf unterschiedlichen Systemen soll im Identitätsmanagement abgelöst werden durch eine einmalige Erfassung bei Eintritt in die Hochschule (in der Regel durch das Personal- bzw. Studierendenverwaltungssystem der Hochschulverwaltung), die dadurch ausgelöste Einrichtung einer eindeutigen Identität, die automatisierte, rollenbasierte Erteilung von Zugangs-

[5] Ausnahmen haben sich erst in letzter Zeit in Einzelfällen ergeben: Benutzerverwaltungen von Bibliotheken und Rechenzentren übernehmen in festgelegten Abständen Daten aus der Studierendenverwaltung. Für alle anderen Nutzer bleibt es weiterhin beim manuellen Verfahren.

berechtigungen (Accounts) auf den wichtigsten IT-Systemen und die Einrichtung von Abläufen (Workflows), die sicherstellen, dass Änderungen des Status (wie z B. Ausscheiden) oder der Daten (wie z. B. Adressänderungen) an der geeignetsten Stelle einmal eingegeben und dann zeitnah, vollständig und synchronisiert in allen angeschlossenen Systemen nachvollzogen werden. Die o. a. Empfehlungen des Landesrechnungshofs gehen ausführlich auf die so zu erwartenden Effizienzgewinne ein.

Datenqualität

Es ist unvermeidlich, dass dieselben Daten, die in unterschiedlichen Systemen mehrfach erfasst und separat verwaltet werden, in vielen Fällen nicht übereinstimmen und im Laufe der Zeit immer weiter auseinender driften, weil kein Mechanismus existiert, der Änderungen (Adressen, Namen, Raumnummern, Status, Telefon….) den jeweils anderen Systemen mitteilt. Solchermaßen im Systemdesign angelegte schlechte Datenqualität führt zu Irrtümern, fehl laufenden Prozessen, aufwendigen Korrekturverfahren mit zweifelhaftem Erfolg. Managementinformationen als Basis für die Planung und Entscheidungsfindung der Leitungsorgane sind dadurch nur mit eingeschränkter Zuverlässigkeit erhältlich.
Wer auf persönliche Merkmale in den IT-Verfahren zurückgreifen muss, die mehr und mehr etwa im Prüfungswesen rechtsverbindlich sein müssen, benötigt zuverlässige Daten zur Beschreibung der Identitäten, Rollen und Rechte. Diese können nur aus den zentralen Datenbanken (z. B. HIS-Datenbanken) der Verwaltung bereitgestellt werden, wenn sie Basis für IT-Verfahren sein sollen. Diese Daten müssen daher im Identitätsmanagement gepflegt und für weitere Nutzungen bereitgestellt werden. Sie müssen nicht eindeutige und nicht fehlerfreie Identitätsmerkmale ausschließen.

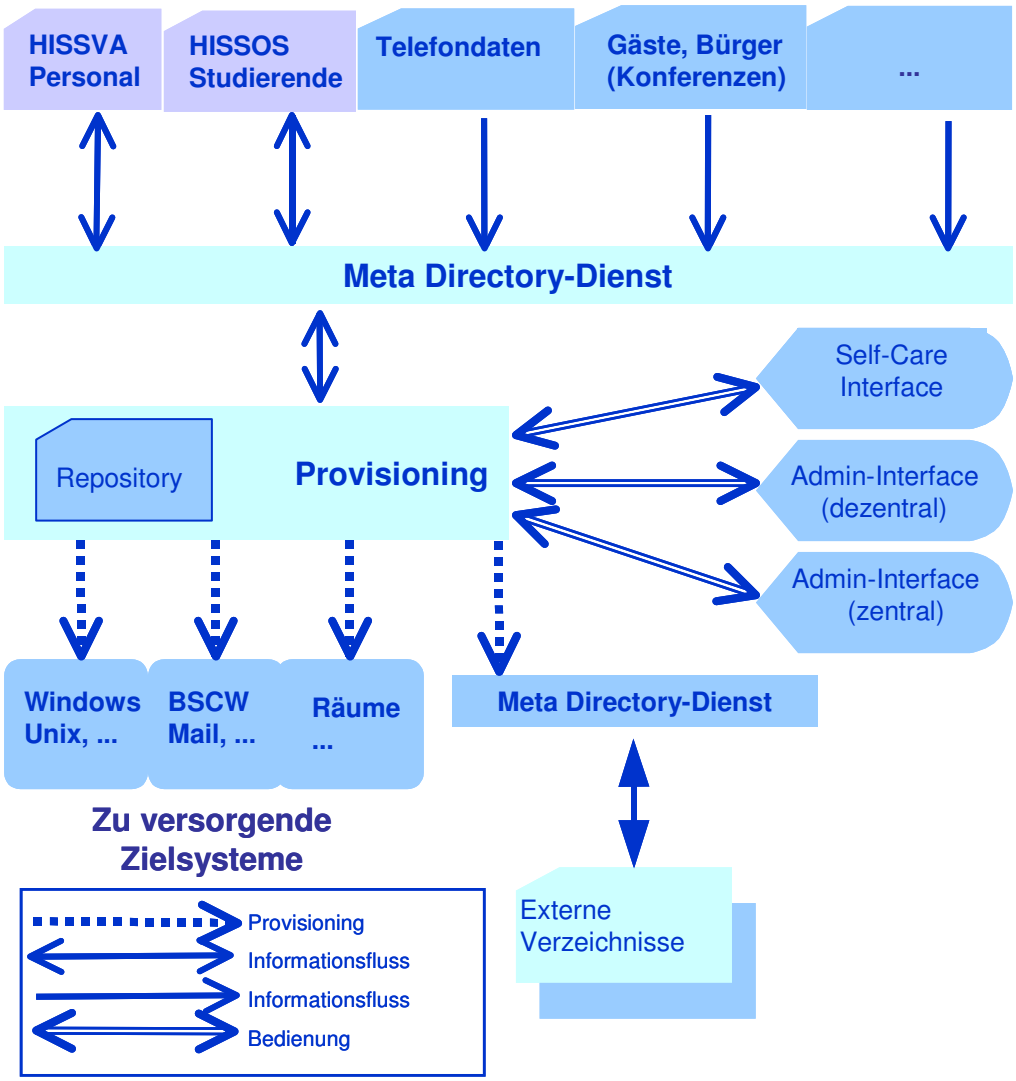
Sicherheit, Datenschutz, informationelle Selbstbestimmung

Fehlendes Identitätsmanagement führt dazu, dass komplexe, vernetzte Systeme nicht sicher betrieben werden können. Gefahr geht von Accounts aus, die nicht zuverlässig bestimmten Personen zugeordnet werden können, insbesondere von *verwaisten* Accounts, die noch ihre Rechte haben, obwohl der legitime Rechteinhaber die Hochschule schon längst verlassen hat. Sie stellen ein weit offenes Eingangstor für kriminelle oder auch nur mutwillige Machenschaften dar. Ein Problem sind auch mehrfache Accounts für ein und dieselbe Person: Ohne Identity Management besteht nirgendwo eine Übersicht, welche Accounts welcher Person zugeordnet sind, so dass in keiner Weise sichergestellt werden kann, dass bei Ausscheiden, Statusänderungen oder Sperrungen die erforderlichen Änderungen an allen Accounts vorgenommen werden.
In einem Identitätsmanagement ist jederzeit nachvollziehbar (Auditfähigkeit) und genau dokumentiert, welche Daten aus welchen Quellsystemen in das Identitätsmanagementsystem hineingeflossen sind, wo diese systemintern mit welchen Zugriffsrechten gespeichert werden und welche Daten zu welchem Zweck an welche Anwendungssysteme übermittelt worden sind. Alle Transaktionen mit Daten werden im System dokumentiert (geloggt). Es ist somit jederzeit nachvollziehbar, ob Grundsätze des Datenschutzes beachtet sind.
Dem Recht auf informationelle Selbstbestimmung wird Geltung verschafft, weil jeder Berechtigte jederzeit vollständige Auskunft darüber erhalten kann, welche persönlichen Daten wo und zu welchem Zweck von wem gespeichert oder verarbeitet worden sind. Darüber hinaus sehen die Systeme in der Regel Schnittstellen (*self care*) vor, die in vorher rechtlich einwandfrei festgelegtem Rahmen jedermann die Möglichkeit geben, selbst über die Art der Veröffentlichung seiner Daten zu entscheiden und bestimmte Änderungen (z. B. Adressen) vorzunehmen.
Die dem Identitätsmanagement zugrundeliegenden Server können redundant und damit ausfallsicher sowie dem Stand der Technik entsprechend abgesichert werden

Basis für hochschulübergreifende Dienste
Qualitätsverbesserung bei sinkenden Ressourcen und zunehmenden Herausforderungen wird ohne Intensivierung der Kooperation von Hochschulen bei der Erbringung gemeinsamer Dienste, der Nutzung gemeinsamer Ressourcen und bei der Realisierung gemeinsamer Studiengänge nicht möglich sein. Eine eindeutige Zuordnung von Personen und Accounts ist zwingende Vorraussetzung dafür, dass an anderen Hochschulen online in zurechenbarer Weise Dienste und Ressourcen nachgefragt oder Studien- und Prüfungsleistungen nachgewiesen bzw. erbracht werden können. Das Identitätsmanagement bietet auch dafür eine solide Basis, da von den Verantwortlichen wohldefiniert festgelegt werden kann, welche Daten gemeinsam genutzt werden sollen und dürfen.

2. Funktionsweise

Anhand der nachstehenden Skizze kann die Funktionsweise eines Identitätsmanagement-Systems wie folgt beschrieben werden.[6]



Verzeichnisse zur Gewinnung von Identitätsdaten

Als Quelle der Identitätsdaten sind vor allem die besonders verlässlichen Personenverzeichnisse der Universitätsverwaltung für Studierende und Bedienstete (HISSOS und HISSVA) zu sehen. Es kommen aber auch Daten aus Telefonverzeichnissen, Daten für Gäste der Universität, Alumni-Daten und Bürger als Nutzer der Universitäts- und Landesbibliothek in Frage. Aus den HIS-Datenbanken werden pro Person nur die Datenextrakte benötigt, die in Abschnitt 4 beschrieben werden. Dabei ist es unverzichtbar, dass für jede Identität ein eindeutiges Merkmal festgelegt wird. Einer eindeutigen Identität können dann jedoch ein oder mehrere Accounts zugeordnet werden. Die Festlegung einer eindeutigen Identität für Personen aus verschiedenen Datenquellen wird als Mapping der Extrakte für Studierende und für Bediens-

[6] Die Beschreibung orientiert sich am zunächst einzusetzenden Produkt TIM der Firma IBM. Sie dürfte aber weitgehend zutreffen für Produkte andere Firmen mit Provisioning-Komponente.

tete bezeichnet. Beim Mapping muss zur Herstellung der eindeutigen Kennung überprüft werden, ob z. B. eine Person, die als Studierender geführt wird, auch Bediensteter ist. Diese eindeutige Kennung ist aus Gründen der IT-Sicherheit unverzichtbar, gleichzeitig bietet sie dem IT-Nutzer einen sehr viel leichteren Umgang mit der IT als das bisher der Fall sein konnte. Beim Mapping werden gleichzeitig auch die Daten - soweit das notwendig ist - zu konsolidieren sein: Unterschiedliche Schreibweisen im Namen von ein- und derselben Person oder andere Fehler werden beseitigt.
In einem späteren Schritt sollen Datenelemente, die im Identitätsmanagement verändert wurden (etwa durch die unten beschriebenen Administrationen und Selbstbedienungen), in die Datenbanken HISSVA und HISSOS zurückfließen, damit die Pflege der ausdrücklich für dezentrale Änderungen zugelassenen Items nicht an mehreren Stellen vorgenommen werden muss und damit leicht zu Fehlern führen kann.

Mit der Verwendung verlässlicher Daten, mit denen auch verwaiste Accounts ausgeschiedener Mitarbeiter/innen vermieden werden, ist ein deutlicher Sicherheits-Zuwachs beim Zugang zu Ressourcen und Informationen verbunden.

Meta Directory mit Provisioning und Repository
Im Meta Directory werden aus verschiedenen Quellen stammende Datenextrakte zusammengeführt.
Das Provisioning-System steuert alle Prozesse, die mit Erzeugung, Modifikation und Entzug von Accounts und Berechtigungen zusammenhängen. Es enthält ein konsolidiertes Verzeichnis (Repository) der Identitätsdaten, die Rollendefinitionen und das Regelwerk, an Hand dessen die Nutzerberechtigungen auf den Zielsystemen bereitgestellt, modifiziert und entzogen werden. Über Rollen, die eine Person wahrnimmt, und Rechte wird also zukünftig der Zugang zu allen Zielsystemen, d. h. Ressourcen wie Rechner und Räume, aber auch zu Anwendungen und Informationen sicher steuerbar, zugelassen oder verweigert. Die Rollen können aus der Organisationsstruktur der Universität übernommen oder aber über Administratoren eingetragen werden. Die Änderungen werden auf den Zielsystemen mit Hilfe von „Agenten“ direkt durchgeführt. Während die Versorgung der Zielsysteme durch das Provisioning-System Teil des täglichen Geschäfts ist, müssen zu Beginn auch Eintragungen mit den bereits vorhandenen Accounts auf den Zielsystemen und dem Repository des Provisioning-Systems abgeglichen werden.

Interfaces für Administratoren und Selbstbedienung
Keine Anwendung (und damit natürlich auch kein Anwender) hat direkten Zugang zu den Daten im Repository des Provisioning Systems, der Datenaustausch erfolgt in festgelegten Richtungen für festgelegte Datenfelder im Rahmen festegelegter und geprüfter Workflows. Direkter Zugang ist ausschließlich ausdrücklich zugelassenen Administratoren vorbehalten. Dabei wird unterschieden zwischen zentralen und dezentralen Administratoren. Zentrale Administration wird auf einige wenige, namentlich benannte Mitarbeiter des Rechenzentrums und der Verwaltung beschränkt sein. Einige wenige Administratoren aus Fachbereichen, die natürlich auch benannt sein müssen, werden nur solche Eintragungen vornehmen können, die keine Auswirkungen über Fachbereichsgrenzen hinaus haben. Im noch eingeschränkteren Umfang wird man eine Selbstbedienung (Self Care Interface) zulassen. Auf diesem Weg der Selbstbedienung wird ein Nutzer auf gesichertem Weg z. B. sein Passwort zurücksetzen oder ändern können oder andere Eintragungen, die nur für ihn selbst relevant sind, vornehmen dürfen. Die Selbst-Administration wird für die informelle Selbstbestimmung nutzbar, da sich jeder Nutzer darüber selbst einen Überblick über die über ihn gespeicherten Daten verschaffen kann. Die zu Personen gehörenden Rollen und Rechte und die damit verbundenen Nutzungsmöglichkeiten können dem Nutzer auf Wunsch angezeigt und mitgeteilt werden.

Alle Zugriffe von Administratoren und in der Selbstbedienung werden automatisch protokolliert und sind somit nachvollziehbar.

Meta Directory-Dienst und Externe Verzeichnisse
Als Ergebnis des Identitätsmanagements können von befugten Administratoren externe Verzeichnisse erstellt werden, die jeweils maßgeschneiderte Informationen zur weiteren individuellen Nutzung innerhalb von Fakultäten (z. B. für die Administration von PC-Pools) enthalten.

Single-Sign-On
Als Bestandteil eines Identitätsmanagements wird für alle Zielsysteme, soweit das technisch schon möglich ist, ein Single-Sign-On eingerichtet, mit dessen Hilfe die Nutzer unterschiedliche Anwendungen starten können, ohne sich stets erneut anmelden zu müssen. Damit wird die IT-Sicherheit verbessert.

Rollen
Rollen werden u. a. sein: Rektoratsmitglieder, Dekane, Instituts- und Seminarleiter, Hochschullehrer, Wissenschaftliche Mitarbeiter, Studierende, Studentische Hilfskräfte, Wissenschaftliche Hilfskräfte, Mitglieder von Gremien. Man wird wegen des Aufwandes mit einer kleinen Zahl von Rollen beginnen und diese dem Bedarf folgend ausweiten.

Zu versorgende Zielsysteme
Zu den zu versorgenden Zielsystemen gehören Rechner- und Betriebssysteme (ADS für Windows-Domänen, Solaris, Linux usw.), Netzsysteme (Netzdatenbank, Netzmanagementsystem, Radius-Server usw.), Kommunikationssysteme (BSCW, Web, E-Mail usw.), E-Learning-Systeme und Systeme zur Administration der Lehre (Kursbuchungssystem, Vorlesungs-Evaluation usw.), Bibliothekssysteme, Raum-Schließsysteme (Haustüren, Abteilungs- und Zimmertüren, Server- und Poolräume usw.). Diese Zusammenstellung ist nicht abschließend.

Vom Identitätsmanagement fließen in der Regel folgende Daten zu den Zielsystemen:

1. Account (Name des Accounts)
2. Passwort
3. Einige Rollen und Rechte aus dem Provisioning (in Münster werden diese in der bisherigen Nutzerverwaltung z. B. noch durch eine sogenannte Gruppenzugehörigkeit beschrieben)
4. Real World Name und organisatorische Informationen (dazu gehören der Nutzername im Volltext und z. B. die Bezeichnung des Ausgabefaches, in dem die Druckergebnisse abgelegt werden
5. Technische Informationen, dazu gehören Informationen zur Shell und dem Home-Filesystem des Nutzers. Diese technischen Informationen können durch den Nutzer vorgegeben werden (self care) oder es werden Standardparameter systemseitig gesetzt werden.

In einzelnen Zielsystemen können die Daten noch anders aussehen.

Im Active Directory System können z. B. zusätzlich vielfältige Daten aufgeführt werden, die Namen, Anschrift, Telefonnummer, Institut etc. umfassen. Diese Daten muss der Nutzer selbst eintragen (self care). Sie werden nicht vom Identitätsmanagement eingetragen. Allenfalls würde dies nach ausdrücklicher Zustimmung der Nutzer automatisiert werden.

Dieser letzte Satz gilt generell für alle anzuschließenden Zielsysteme: Über die Ziffern 1. bis 5. hinausgehende Datenflüsse vom Identitätsmanagement zu den Zielsystemen werden grund-

sätzlich vom Nutzer selbst einzutragen sein (self care) oder nach dessen ausdrücklicher schriftlicher Zustimmung automatisiert übertragen.

3. Ganzheitliche Betrachtung des Identitätsmanagements

Aus den bisherigen Darlegungen zur Bedeutung und Funktionsweise des Identitätsmanagements ist deutlich geworden, dass ein Identitätsmanagement wesentlicher Kernbestandteil zeitgemäßer Aufgabenerfüllung der Hochschule nach § 3 und nach §30 HG NRW ist. Dieser Kern einer IT-Infrastruktur stellt ihren Mitgliedern Dienste auf dem aktuellen Stand der technischen Entwicklung zur Verfügung. Das Identitätsmanagement spielt auf allen Ebenen dieser Infrastruktur eine zentrale Rolle, vom sicheren Zugang zu Systemen und Netzen über die Sicherung der Datenqualität bis hin zu integrierten und gesicherten Dienstzugängen über Portale. Identitätsmanagement ist die zwingende Konsequenz aus dem flächendeckenden Einsatz, d. h. einer sehr großen Anzahl an Nutzern und einer großen Zahl von personalisierten IT-Verfahren, die nicht auf einem monolithischen Ansatz beruhen. Ohne Identitätsmanagement, das Gesamtsystem der Informationsverarbeitung nicht beherrschbar.

Die Anforderungen an das Identitätsmanagement können also nur in einer solchen Gesamtbetrachtung richtig eingeschätzt werden. Eine wichtige Konsequenz aus dieser Gesamtbetrachtung ist, dass für alle Teilnehmer im System eine eindeutige Identität vorzusehen ist. Die Forderung nach einer eindeutigen Identität folgt vor allem aus Sicherheitsüberlegungen. Mehrfache Identitäten können zu erheblichen Problemen bei der IT-Sicherheit führen, was nachstehend an vier Beispielen erläutert werden soll.

Ein Benutzer, der mehrere Identitäten hat und durch sein Verhalten gegen die Sicherheit der IT verstößt, kann zunächst nur mit der einen zufällig bekannten Identität gesperrt werden. Unter den anderen Identitäten kann der Missbrauch weitergehen, weil nirgendwo gespeichert ist, dass diese verschiedenen Identitäten zu ein und derselben Person gehören. Dies ist eine reale Annahme, die wir wiederholt beobachtet haben. Mit dem Identitätsmanagement müssen z. B. die administrativen Aufgaben im Zusammenhang mit Studierenden sicher behandelt werden. Einem Studierenden, der mehrere Identitäten hat, werden leicht wichtige Informationen (z. B. Studienkonten) an mehreren Stellen zugeordnet, was sehr leicht zu erheblichen Schäden führen kann. Ein Professor, der als Prorektor eine 2. Identität bekommen hat, die er versehentlich oder wider besseres Wissen auch für wissenschaftliche Arbeiten nutzt und die ihm aber am Ende seiner Amtszeit automatisch entzogen wird, weil kein Mapping der Identitäten stattgefunden hat, verliert u. U. seine wissenschaftlichen Daten. Der Schaden kann dadurch beträchtlich werden. Verschiedene Dienste, z. B. in Bibliothek oder Rechenzentrum sind kostenpflichtig. Personen, die diese Zahlungen nicht leisten, müssen vorübergehend von der weitern Nutzung dieser Dienste ausgeschlossen werden, um weiteren finanziellen Schaden zu vermeiden. Dafür ist eine eindeutige Identität notwendig.
Allein diese Beispiele zeigen, dass das Identitätsmanagement infolge seiner grundlegenden Bedeutung und den damit verbundenen Sicherheitsproblemen ganzheitlich zu betrachten ist. Die Bedeutung des Identitätsmanagements ist so weitreichend, dass das Mapping lediglich ein kleines, allerdings bei unsachgemäßer Einführung ein wichtiges Element ist. Ein automatisiertes Mapping ist darüber hinaus dauernd notwendig: Wenn etwa einem Bürger als Kunde der Bibliothek eine Identität zugeordnet werden soll, muss auch geprüft werde, ob diese Person schon als Gast oder Mitglied der Universität über eine Identität verfügt. Auch hier sind Duplikate zu verhindern.
Nicht zuletzt ist im Zusammenhang mit dem Mapping auch auf die Handhabbarkeit durch den Nutzer hinzuweisen. Provisioning heißt, dass automatisiert Accounts angelegt werden, sobald die jeweilige Rolle dies hergibt. Eine neu eingestellte studentische Hilfskraft bekommt damit z. B. eine weitere Email-Adresse, weitere Zugänge zu Servern, ohne dass die Historie, d.h. die für ihn als Studierender bereits angelegten Daten/Konfigurationen zu übernehmen. Dafür sind

die neuen Accounts als Mitarbeiter/in aber in der Regel mit weitergehenden Rechten ausgestattet. Nun beginnt entweder das manuelle Mapping oder ein Hin und Her zwischen *alter Umgebung* und *neuen Rechten*. Das ist aus Sicht der Nutzer aber sicher nicht akzeptabel, weil nicht praktikabel.

Die in Abschnitt 5 diskutierten Varianten zur ganzheitlichen Betrachtung des Identitätsmanagements können also nicht akzeptiert werden.

4. Feinanalysen

4.1 Datensynchronisation zwischen den Quellsystemen

Die hier dargestellten Daten und Datenflüsse beschreiben den Zustand, wie er nach der Grundinstallation sein wird. Diese Daten werden sich natürlich ändern, sobald Funktionalitäten zwischen den Systemen wechseln.

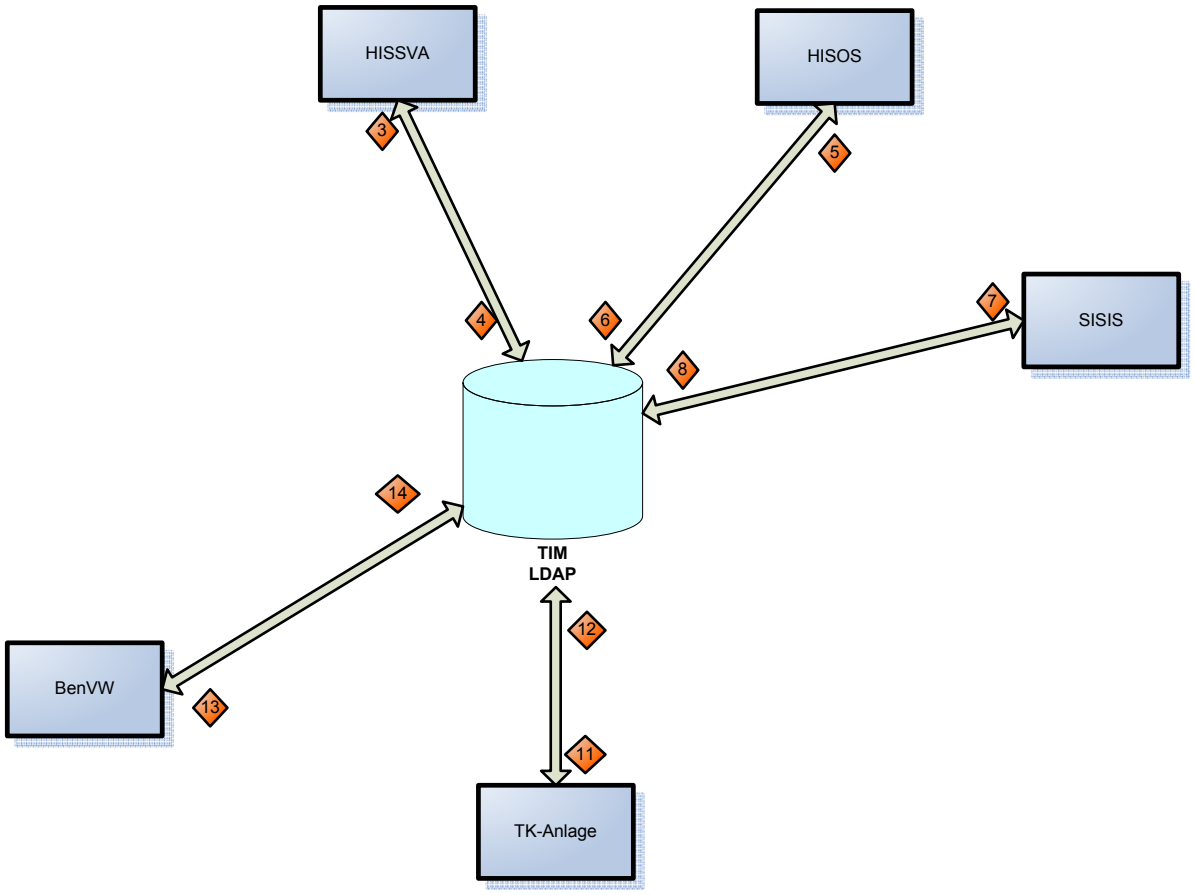


Abbildung 1: Datenflüsse zwischen Quellsystemen

Die Nummern in der Abbildung verweisen auf die im Anschluss aufgeführten Tabellen, in denen die jeweiligen Attribute, die übertragen werden, definiert sind.

In dem gesicherten TIM LDAP sind sämtliche Personen vorhanden, die in einem der anderen Systeme auftreten. Damit nicht Personendaten in Systeme übertragen werden, in denen sie nicht zwingend notwendig geführt werden, ist ein Personenattribut mit dem Namen „PERSONENSTATUS“ definiert worden. Dieses Attribut stellt dar, wie diese Person in Beziehung zur Universität steht (Studierende, Mitarbeiter/in, Externe, Gast, Ehemaliger. Das Feld kann mehrere dieser Werte führen, so zum Beispiel gleichzeitig Mitarbeiter und Student. Anhand dieser Werte kann nun festgestellt werden, zu welchen Systemen die Daten übertragen werden dürfen.
Bei anderen Systemen wird ein wenig abweichend vorgegangen, so wird für die TK-Anlage nochmals eine separate Rolle *Telefonberechtigt* geführt, die angibt, ob eine Person mit einer Telefonnummer bestückt werden darf und dementsprechend der Personensatz der TK-Anlage zur Verfügung gestellt wird.

4.2 Daten TIM-HISSVA

Voraussetzung dafür, dass die Daten in diese Richtung verteilt werden, ist:
Personenstatus = Mitarbeiter-Universität

Daten TIM → HISSVA (3)
Uni-ID
Personen Status
Nachname
Vorname
Titel
Geburtsdatum
Geschlecht
Telefonnummern (Dienstl., multival. Incl. Raum)
Telefonnummer (Privat)
Strasse, Hausnummer
Postleitzahl
Ort
Land / Wohnort
Kontakt e-mail
Einrichtung
Bankverbindung
Bankleitzahl
Kontonummer

Dieser Datentransport (3) ist für eine spätere Variante vorgesehen.

Daten HISSVA → TIM (4)
Uni-ID
Personen Status (nur Mitarbeiter)
Nachname
Vorname
Geburtsdatum
Titel
Geschlecht
Strasse, Hausnummer
Postleitzahl
Ort
Land / Wohnort
Einrichtung
Kostenstelle
Bankverbindung
Bankleitzahl
Kontonummer

4.3 Daten TIM-HISSOS

Voraussetzung dafür, dass die Daten in diese Richtung verteilt werden, ist:
Personenstatus = Studierender-Universität

Daten TIM → HISSOS (5)
Uni-ID
Nachname
Vorname
Titel
Telefonnummer (Privat)
Strasse, Hausnummer
Postleitzahl
Ort
Kontakt e-mail
Sichtbarkeit

Dieser Datentransport (5) ist für eine spätere Variante vorgesehen.

Daten HISSOS → TIM (6)
Uni-ID
Personen Status (nur Studierender)
Nachname
Vorname
Geburtsdatum
Geschlecht
Matrikelnummer
Studierendenstatus
Titel
Telefonnummer (Privat)
Strasse, Hausnummer
Postleitzahl
Ort
Kontakt e-mail
Studiengang (multivalue)
Einrichtung

4.4 Daten TIM-SISIS

SISIS ist die Datenstruktur für das gleichnamige Bibliothekssystem, das an einigen Standorten eingesetzt wird.
Voraussetzung dafür, dass die Daten in diese Richtung verteilt werden dürfen, ist:

Personenstatus = Bibliothek (dieser Status wird bei Studierenden, wissenschaftlichen Mitarbeitern (Universität) und externen automatisch gesetzt; alle anderen müssen im Self-Service diesen Flag beantragen – Prozess „Beantragung Account“)

Daten TIM → SISIS (7)
Uni-ID
Studierenden Status
Personen Status

Nachname
Vorname
Geburtsdatum
Geschlecht
Raumnummer (multival.)
Strasse, Hausnummer
Postleitzahl
Ort
Kontakt e-mail

Damit wird die Bibliothek lediglich als Zielsystem eingebunden. Aufgrund der Anforderungen bzgl. der Stadtbenutzer, die als externe in das System neu aufgenommen werden, wird allerdings die Bibliothek hier im Datenfluss der Quellsysteme mit aufgenommen.

4.5 Daten TIM-TK-Anlage

Die Verbindung zwischen TK-Anlagen und Identitätsmanagement wird an unterschiedlichen Standorten leicht voneinander abweichen; die Datenelemente werden aber wesentlich einheitlich sein.
Voraussetzung dafür, dass die Daten in diese Richtung verteilt werden, ist:

Personenstatus = Person hat die Rolle TK-berechtigt

Daten TIM → TK-Anlage (11)
Uni-ID
Nachname (SN)
Common Name (CN)
Vorname
Anrede
Titel
Dienstbezeichnung
Kontakt e-Mail

Daten TK-Anlage → TIM (12)
Uni-ID
Telefonnummer GUID
Telefonnummer
Raum
Kostenstelle
Berechtigung
Telefonbucheintrag
Anschlussinfo
Rechnungsempfänger
Liste der GUID's, die der TN zugeordnet werden
Ressource

Dieser Datentransport (12) ist für eine spätere Variante vorgesehen.

4.6 Daten TIM-BenVW

Die bisher in den Hochschulen vorzufindenden Benutzerverwaltungen für den Zugang zu den IT-Ressourcen, werden in einzelnen Datenelementen voneinander abweichen. Unterschiede von grundsätzlicher Bedeutung sind dies aber nicht. Voraussetzung dafür, dass die Daten in diese Richtung verteilt werden, ist:

Personenstatus = ALLE

Daten TIM → BenVw (13)
Uni-ID
Studierenden Status
Personen Status
Matrikel Nummer
Nachname
Vorname
Geschlecht
Telefonnummern (Dienstl., multiv. Incl. Raum)
Kontakt e-mail
Einrichtung

Daten BenVw → TIM (14)
Uni-ID
eMail Adresse (Uni-Bi)
Uid

4.7 Datenflüsse aus der Provisionierung in die Zielsysteme

Datenflüsse aus dem Provisioning in typische Zielsysteme (z. B. Windows, Unix, BSCW, E-Mail) umfassen Accounts und Passwörter. Weitere Einzelheiten sind dazu oben am Ende von Abschnitt 2 beschrieben.

5. Datenschutzrechtliche Würdigung gemäß DSG NW

Gemäß § 3 HG NW hat die Universität für die Pflege und Entwicklung der Wissenschaften durch Forschung, Lehre und Studium zu sorgen und den Wissens- und Technologietransfer sowie die internationale Zusammenarbeit zu fördern. Um diese Aufgaben zu erfüllen, bietet die Hochschule eine große Vielfalt von Informationen und Dienstleistungen für und durch ihre Mitglieder (Wissenschaftler, Studierende, Mitarbeiter der Verwaltung und der Zentralen Einrichtungen), aber auch für Gäste und externe Partner an. Wie oben dargetan wurde, hat sich mit der Entwicklung der Informations- und Kommunikationstechnik unausweichlich ergeben, dass ein immer größerer Teil dieser Dienstleistungen und Informationen über Hochschulnetz und Internet angeboten und nachgefragt werden. Dem trägt auch die Begründung zu § 30 HG Rechnung, die explizit das *Betreiben von Netzwerken* vorsieht (*MSWWF NRW*, Hochschulgesetz mit Begründungen, 2000, S. 160). Weil Angebot und Nachfrage von Dienstleistungen und Informationen über Netzwerke einen wesentlichen und immer größeren Teil dieser Kernaufgabe der Hochschule bestimmen, müssen dabei strenge Sicherheitsanforderungen eingehalten werden. Die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Nachrichten und Dienstleistungen müssen gewährleistet sein. Durch das einzuführende Identitätsmanagement kann dies in sehr viel zuverlässigerer Weise sichergestellt als mit den bisherigen Verfahren – allerdings nur dann, wenn alle Teilnehmer an diesem Betrieb eindeutig identifizierbar und autorisierbar sind. Wie ebenfalls im ersten Kapitel dargetan, ist dies nur auf der Basis eines funktionierenden Identitätsmanagements möglich. Wie die folgenden Erwägungen zeigen werden, sind für die Datenerhebung und -verarbeitung die Vorraussetzungen der §§ 12 ff. DSG NW gegeben.

5.1 Automatisiertes Einrichten von Identitäten

Für das geplante Identitätsmanagement werden jedem Studierenden und jedem Bediensteten der Universität eine eindeutige Identität und ein oder einige Accounts zugeordnet. Hierfür werden personenbezogene Daten benötigt, die eine eindeutige Zuordnung ermöglichen (z.B. Name, Matrikelnummer und Geburtsdatum). Dies betrifft zum einen Studie-

rende und Angestellte die neu an die Hochschule kommen und zum anderen diejenigen, die bereits immatrikuliert bzw. angestellt sind.

a) Einwilligung

Wird beim Einrichten einer Identität hierfür eine **Einwilligung** der betroffenen Person erteilt, so ist die von der Einwilligung umfasste Datenverarbeitung zulässig (§ 4 Abs. 1 b) DSG NW). Es ergeben sich also dann keine weiteren datenschutzrechtlichen Bedenken. Eine Einwilligung i. S. d. § 4 DSG NW muss widerruflich, freiwillig und eindeutig sein. Grundsätzlich muss die Einwilligung **schriftlich** erteilt werden, eine **elektronische Erklärung** ist jedoch auch zulässig, wenn sichergestellt ist, dass die Erklärung

1. nur durch eine eindeutige und bewusste Handlung der handelnden Person erfolgen kann
2. sie nicht unerkennbar verändert werden kann
3. ihr Urheber erkannt werden kann
4. die Einwilligung bei der verarbeitenden Stelle protokolliert wird und
5. der betroffenen Person jederzeit Auskunft über den Inhalt ihrer Einwilligung gegeben werden kann.

b) Zulässigkeit auch ohne Einwilligung

Das Landesdatenschutzgesetz sieht darüber hinaus die Möglichkeit vor, dass Datenverarbeitungen auch ohne Einwilligung des Betroffenen vorgenommen werden können (§ 4 Abs. 1 a) DSG NW). Erforderlich ist für diesen Fall, dass eine Vorschrift des DSG oder eines anderen Gesetzes dies erlaubt.

aa) Datenerhebung

Bei Studenten und Angestellten, die **neu** an die Hochschule kommen, geht es zunächst um eine Erhebung der Daten. Für die **Datenerhebung** gilt **§ 12 DSG**, wonach die Kenntnis der Daten für die rechtmäßige Aufgabenerfüllung erforderlich sein muss. Die Aufgabe der Hochschule, die sie mit der Bereitstellung des Identitätsmanagements erfüllt, ist oben ausführlich geschildert.

Erforderlich i. S. d. § 12 DSG NW ist die Datenerhebung dann, wenn die Kenntnis der Daten zur Erreichung des konkreten Zwecks **objektiv geeignet** und im Verhältnis zum angestrebten Zweck auch **notwendig** ist – hier sind strenge Maßstäbe anzulegen. Die Datenerhebung sollte sich auf das ***unerlässliche Minimum*** beschränken (*Stähler/Pohler*, Datenschutzgesetz Nordrhein-Westfalen, 2003, § 12 Rn. 2). Mittelbar ist in dieser Vorschrift auch der **Zweckbindungsgrundsatz** enthalten (Rossnagel/*v. Zezschwitz*, Handbuch Datenschutzrecht, 2003, 3.1. Rn. 21 f.), wonach Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie auch erhoben wurden. Die Datenerhebung darf daher allein in einer dem Zweck angemessenen Art und Weise und in entsprechendem Umfang erfolgen. Nach § 12 Abs. 2 S. 1 DSG NW ist über Sinn und Zweck der Erhebung, insb. die beabsichtigte Verwendung der personenbezogenen Daten aufzuklären. Eine besondere Form ist hierfür jedoch nicht vorgeschrieben.

Es ist vorgesehen, für Studierende eine entsprechende Änderung der Einschreibordnung vorzunehmen. Neu einzustellenden Mitarbeitern wird bei Einstellung mitgeteilt, in welcher Weise ihre Daten im Rahmen des Identitätsmanagements verwendet werden sollen.

bb) Übermittlung von Daten

Daten von Studenten und Mitarbeitern, die bereits immatrikuliert bzw. angestellt sind, befinden sich bereits in den Datenbanken der Universitätsverwaltung (im Wesentlichen HIS-Daten). Die im Identitätsmanagement benötigten Daten stellen lediglich Auszüge aus den umfassenderen Daten dar. Sinnvoll wäre es daher, wenn diese Daten nicht wie unter aa) beschrieben neu erhoben werden müssten, sondern unmittelbar in das neue Identitätsmanagement-System übertragen werden könnten. Eine solche **Übermittlung** von Daten regelt **§ 14 DSG NW**. Gem. § 14 Abs. 4 DSG NW gilt die Vorschrift ausdrücklich auch für eine Weitergabe von Daten innerhalb einer öffentlichen Stelle wie der Universität. Genau wie die Erhebung von Daten ist auch die Weitergabe ohne Einwilligung des Betroffenen dann zulässig, wenn die Kenntnis der Daten zur Erfüllung einer eigenen Aufgabe erforderlich ist. Entgegen dem Wortlaut ist dabei auf die Kenntnis und nicht auf die Datenübermittlung abzustellen (*Stähler/Pohler*, Datenschutzgesetz Nordrhein-Westfalen 2003 § 14 Rn. 4). Dabei ist jedoch wiederum der Grundsatz der **Zweckbindung** zu berücksichtigen, der durch **§ 13 DSG NW** festgelegt ist. Hiernach dürfen personenbezogene Daten nur zu dem Zweck weiterverarbeitet werden, zu dem sie erstmals gespeichert worden sind. Erforderlich ist also eine **Zweckidentität** zwischen der Erhebung der Daten und der weite-

ren Verwendung. Die Daten müssen dabei jedenfalls auch zum Zweck der Übermittlung gespeichert worden sein (*Stähler/Pöhler*, Datenschutzgesetz Nordrhein-Westfalen 2003 § 14 Rn. 4). So können z.B. personenbezogene Daten, die von Studenten und Angestellten bei ihrer Immatrikulation bzw. Einstellung zum Zweck der Nutzung eines E-mail-Accounts und Uni-Netzzuganges erhoben wurden, zu diesem Zweck auch im Rahmen des neuen Identitätsmanagement-Systems übermittelt und genutzt werden.

Ist eine Zweckidentität nicht gegeben, so kann eine Übermittlung dennoch zulässig sein, wenn die Zweckänderung nach den Voraussetzungen des **§ 13 Abs. 2 S. 1 lit. a-i DSG NW** legitimiert ist. Dies ist nach **Abs. 2 a)** der Fall, wenn eine Rechtsvorschrift dies erlaubt oder eine Zweckänderung zur Aufgabenerfüllung zwingend erforderlich ist. Für die zwingende Erforderlichkeit gilt das oben Gesagte. Nach **Abs. 2 e)** ist eine Zweckänderung aber auch dann zulässig, wenn eine Einwilligung unverhältnismäßig hoher Aufwand wäre und die Zweckänderung offensichtlich im Interesse d. Betroffenen liegt. Hierbei ist insofern auch auf das hypothetische subjektive Interesse abzustellen, es zählt also nicht allein, was für den Betroffenen „das Beste" ist. Ein offensichtliches – subjektives – Interesse pauschal aller bereits immatrikulierten Studenten und aller Angestellten an der automatisierten Einrichtung eines Accounts wird wohl sehr schwer zu begründen sein.

In „Altfällen" ist eine Übermittlung der Daten daher grundsätzlich möglich, soweit der Zweck mit dem der erstmaligen Datenerhebung identisch ist. Im Falle einer Zweckänderung ist gemäß den o. a. Ausführungen die gesetzliche Aufgabe heranzuziehen, deren Erfüllung die Übermittlung zwingend erforderlich macht.

5.2 Verknüpfen von Daten („Mapping")

Im Rahmen eines Identitätsmanagement-Systems können Daten, die zu verschiedenen Zwecken erhoben worden sind, miteinander verknüpft werden. So muss ein Student, der gleichzeitig Angestellter der Hochschule ist, nicht zwei Identitäten führen. Seine Daten können in einer einzigen Identität zusammengeführt werden. Die Verknüpfung bezieht sich also lediglich darauf, dass Doppelungen und Inkonsistenzen in semantisch gleich bedeutenden Datenfeldern, die für eine Person in unterschiedlichen Systemen gespeichert sind, beseitigt werden. Eine darüber hinaus gehende Verknüpfung findet in keiner Weise statt.

a) Datenzusammenführung mit Einwilligung

Erhalten bisher getrennt gespeicherte Daten durch Verknüpfung einen anderen Informationsgehalt, so liegt ein „Verändern“ i. S. d. § 3 DSG NW vor (*Stähler/Pohler*, Datenschutzgesetz Nordrhein-Westfalen 2003, § 3 Rn. 12). Der Vorgang ist damit Datenverarbeitung i. S. d. § 4 DSG NW und zulässig, wenn die betroffene Person eingewilligt hat. Die erforderliche Form der widerruflichen, freiwilligen und eindeutigen Einwilligung richtet sich erneut nach den unter 1 a) genannten Kriterien. Denkbar und datenschutzrechtlich vollkommen unproblematisch wäre es damit, eine Zusammenführung der Daten erst nach erfolgter **elektronischer Einwilligung** durchzuführen.

b) Datenzusammenführung ohne Einwilligung

Das Verändern von Daten ist gem. § 4 Abs. 1 a) DSG NW auch ohne Einwilligung zulässig, wenn das DSG oder eine andere Rechtsvorschrift dies erlaubt. In Frage kommt hier **§ 13 DSG NW**. Danach muss die Verknüpfung zur rechtmäßigen Erfüllung von Aufgaben **erforderlich** sein. Es stellt sich somit die Frage, ob zur Aufgabenerfüllung tatsächlich eine Verknüpfung der Daten erforderlich ist oder ob nicht das gesamte System auch ohne eine solche Datenveränderung funktionieren kann. Denkbar ist, dass die Betroffenen so lange mit zwei Identitäten, denen jeweils unterschiedliche Rollen zugeordnet sind, am Netz teilnehmen, bis sie ihre elektronische Einwilligung zur Zusammenführung abgegeben haben. Das gesamte System würde hierdurch in seiner Funktion nicht vollständig lahmgelegt. Allerdings führt die Verwendung mehrerer Identitäten für dieselbe Person zu Uneindeutigkeit, Unübersichtlichkeit und beträchtlichen Sicherheitsrisiken. Dies wird vor allem deutlich, wenn man in den Blick nimmt, dass es nicht nur um zwei Systeme geht, sondern um Identitäten in einer Vielzahl von Zielsystemen, die unter ganz unterschiedlicher Verwaltung stehen.

aa) Gesamtbetrachtung

Möglich ist daher, die Datenzusammenführung als notwendigen Bestandteil der gesamten Einführung des Identitätsmanagements zu betrachten. Die Einführung des Identitätsmanagements ist erforderlich (s. o.). Bei einer solchen Gesamtbetrachtung käme man somit zu dem Ergebnis, dass die Datenzusammenführung als Bestandteil der Systemeinführung erforderlich und damit auch ohne Einwilligung zulässig ist.

bb) Einzelbetrachtung

Andernfalls ist eine Einzelbetrachtung der Datenzusammenführung vorzunehmen. Dann könnte sich eine Erforderlichkeit der Zusammenführung z.B. unter dem Aspekt der Einführung eines universitären **PKI-Sicherheits-Zertifikates** ergeben. Sollte eine solche Zertifizierung nur dann möglich sein, wenn jedem Teilnehmer lediglich eine einzige Identität zweifelsfrei zuzuordnen ist, könnte eine automatische Verbindung zweier Identitäten hierfür erforderlich sein. Das Zertifikat als solches erfordert zunächst nur, dass der Benutzer des Zertifikates eindeutig als eine bestimmte Person identifizierbar ist. Dies ist aber dann nicht mehr ausreichend, wenn Zertifikate auch als Logon-Ersatz Verwendung finden müssen, um das Ausspähen von Passworten endgültig zu vermeiden und damit die IT-Sicherheit abermals deutlich zu erhöhen. Ein Zertifikat muss also eindeutig einer Person zugeordnet werden. Diese Sicherheit kann aber nicht gewährleistet werden, wenn ein Nutzer zwei Identitäten und damit u. U. auch zwei Zertifikate nutzt. Ein Nachteil wäre bei zwei Zertifikaten darüber hinaus wirtschaftlicher Art, da die Ausstellung eines Zertifikats Kosten verursacht. Die zwingende Notwendigkeit für stärkere Identifikationsmechanismen, z. B. durch die Ausstellung von Zertifikaten, ergibt sich dadurch, dass Anpassungen an den Bologna-Prozess und die damit verbundenen prüfungsrelevanten Verwaltungsvorgänge elektronisch zu erledigen sind.

Die Erforderlichkeit einer einheitlichen Identität ergibt sich jedoch auch aus **§ 10 DSG NW** unter dem **Aspekt der Datensicherheit**. So könnte sich eine Sicherheitsgefährdung daraus ergeben, dass ein Nutzer mit zwei oder mehr Identitäten nicht effektiv durch eine Sperrung ausgeschlossen werden kann. Sollte ein Nutzer die Datensicherheit etwa durch ein Ausspähen von Passwörtern gefährden und als Konsequenz dessen seine Identität gesperrt werden, so könnte dieser Nutzer einfach auf eine weitere Identität ausweichen. Das „Mapping“ kann in diesem Zusammenhang als eine eigenständige technische Maßnahme zur Gewährleistung der Datensicherheit i. S. d. § 10 DSG NW angewandt werden.

cc) Zweckbindung

Daneben stellt sich das Problem der **Zweckbindung** aus § 13 Abs. 1 DSG NW. Auch bei Erforderlichkeit darf eine Verarbeitung der Daten nur dann stattfinden, wenn die Daten auch zu diesem Zweck erhoben wurden. Etwa bei den Personaldaten eines Studenten ist dies in Bezug auf eine spätere Angestelltentätigkeit nicht der Fall. Es müsste also in diesem Fall eine der Ausnahmen nach § 13 Abs. 2 DSG NW eingreifen. In Frage kommt auch hier Abs. 2 a). Nach § 13 Abs. 2 a) DSG NW müsste die Erlaubnis durch eine

Rechtsvorschrift oder die zwingende Notwendigkeit zur Wahrnehmung einer gesetzlich erteilten Aufgabe vorliegen.
Im Falle einer Gesamtbetrachtung ergibt sich die zwingende Notwendigkeit aus den Ausführungen zu Anfang dieses Abschnitts 5.
Bei der Einzelbetrachtung der Datenzusammenführung zur Herstellung einer einheitlichen Identität ist eine zwingende Notwendigkeit anzunehmen, weil diese einheitliche Identität eine zwingende Notwendigkeit unter dem Aspekt der IT-Sicherheit ist und somit das Zusammenführen als eigenständige erforderliche technische Maßnahme zur Gewährleistung der Datensicherheit anzusehen ist . (gemäß § 10 DSG NW).

dd) Zusammenfassung

Hinsichtlich des sog. „Mappings“ ist somit zwischen einer Gesamt- und einer Einzelbetrachtung zu differenzieren. Sieht man im Sinne einer **Gesamtbetrachtung** die Datenzusammenführung als notwendigen Bestandteil des gesamten Identitätsmanagement-Systems an, das zur Aufgabenerfüllung erforderlich ist, so ist nach § 13 DSG NW ein „Mapping“ auch ohne Einwilligung möglich.
Auch bei einer **Einzelbetrachtung** ist die Datenzusammenführung ohne Einwilligung zulässig, weil eine zwingende Notwendigkeit unter dem **Aspekt der Datensicherheit** gegeben ist.
Als weiterer möglicher Weg käme in Frage, die Zusammenführung der Daten von einer **Einwilligung** des Betroffenen abhängig zu machen, die auch (nach den unter 1. a) aufgeführten Voraussetzungen des § 4 DSG NW) elektronisch abgefragt werden kann. Dabei ist denkbar, dass bei der Einrichtung eines Accounts für Mitarbeiter automatisch über ein elektronisches Formular, das anhand der Notwendigkeit eines „Einloggens“ auch eindeutig zugeordnet werden kann, eine entsprechende Einwilligung abgefragt wird.

5.3 Übertragen von Daten („Roaming“)

Das Identitätsmanagement-System bietet neben der hochschulinternen Nutzung auch die Möglichkeit einer **hochschulübergreifenden Datenverwaltung**. So könnten für die Nutzer einer Hochschule auch Programme oder Geräte anderer Hochschulen mit Identitätsmanagement zur Verfügung gestellt werden. Dies erforderte zunächst eine Abfrage der Berechtigung und anschließend eine **Datenübertragung** aus dem System der einen an das System der anderen Hochschule. Für die Datenübertragung gilt § 14 DSG, wonach auch ohne Einwilligung des Betroffenen eine Datenübertragung dann zulässig ist, wenn sie zur

Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist. Die in diesem Rahmen zu erfüllenden Aufgaben beider Hochschulen ergeben sich aus § 30 HG NW. In der amtlichen Begründung hierzu heißt es, dass die Regelung sowohl eine gemeinsame Wahrnehmung von Aufgaben durch mehrere Hochschulen als auch die Nutzung hochschulexterner Einrichtungen ermögliche (*MSWWF NRW*, Hochschulgesetz mit Begründungen, 2000, S. 160). Ohne eine entsprechende Datenübertragung, die aber evtl. auf Elementardaten wie Name und Adresse zu beschränken ist, kann diese Aufgabe nicht wahrgenommen werden, so dass auch in diesem Fall **keine Einwilligung erforderlich** ist.

5.4 Datensicherheit

Wenn eine Erhebung oder Verarbeitung von Daten nach dem DSG NW zulässig ist, muss die Hochschule sicherstellen, dass die Durchführung datenschutzgerecht erfolgt und ein Missbrauch der Daten ausgeschlossen ist. Gem. § 10 Abs. 1 DSG NW haben die Hochschulen durch **technische und organisatorische Maßnahmen** sicherzustellen, dass die Vorschriften über den Datenschutz eingehalten werden. Die Landesbeauftragte für den Datenschutz empfiehlt daher auch aus Gründen der Transparenz, bereichsspezifische Regelungen in die Einschreibeordnungen aufzunehmen, in denen Art, Umfang und Verantwortlichkeiten der Verarbeitung personenbezogener Daten unter Berücksichtigung des Zweckbindung- und Erforderlichkeitsgrundsatzes klargestellt und festgelegt werden (*Sokol*, Datenschutz und Informationsfreiheit, Bericht 2005, 121 f.). Die Universität Münster etwa hat in ihrer Einschreibungsordnung in § 1 Nr. 6 a) nur Art und Umfang der Datenverarbeitung festgelegt.

a) Administration

Das Identitätsmanagement-System bietet sowohl die Möglichkeit einer **zentralen** als auch einer **dezentralen Administration**. Während bei einer zentralen Administration eine geringe Anzahl an Personen mit der Administration des Gesamtsystems befasst ist, können bei der dezentralen Administration einzelne Systemteile (etwa die Verwaltung eines Fachbereichs) mit bestimmten Änderungsbefugnissen auf eine Vielzahl dezentraler Administratoren aufgeteilt werden. Zwar bietet ein dezentrales System den Vorteil der Arbeitserleichterung und der Übersichtlichkeit – Fragen, die einen solchen Teilbereich betreffen, können intern geklärt werden. Nachteile der dezentralen Verwaltung sind aber vor allem in der Datensicherheit zu sehen. Je mehr Personen als Administratoren Zugriff auf die Daten haben, desto größer ist die **Gefahr eines Missbrauchs**. Die in § 10 DSG NW geforderte Datensicherheit ist beispielsweise dann nicht mehr gewährleistet, wenn für den dezentralen Administrator mit beschränkter Änderungsbefugnis durch die Anwen-

dung verschiedener technischer Tricks die Möglichkeit besteht, auf sämtliche Übergabedaten zuzugreifen. Ist den Systementwicklern eine solche Möglichkeit bekannt, so kann etwa eine Dienstanweisung, die das Unterlassen dieser Tricks anordnet, nicht ausreichen, um den Erfordernissen aus § 10 DSG NW gerecht zu werden. Kann ein solcher Missbrauch technisch nicht ausgeschlossen werden, so ist auf die „sichere" zentrale Administration zurückzugreifen.

b) Endsysteme

Die an das Identitäts-Management angeschlossenen Endsysteme lesen die ihnen zur Verfügung gestellten Daten aus. Wenn die dem einzelnen Nutzer zugewiesene Rolle einen Zugriff zu diesem Endsystem erlaubt, gewähren sie einen Zugang (etwa zu einem bestimmten Programm oder auch zu einem Raum), andernfalls nicht. Unter Datenschutzaspekten sind hier keine Schwierigkeiten ersichtlich, das Auslesen von Daten bezieht sich bei den Endgeräten ja lediglich auf die vom System zugewiesene Rolle. Im Hinblick auf die zu gewährleistende **Datensicherheit** ist jedoch darauf zu achten, dass keine veralteten Endsysteme verwendet werden, die einen missbräuchlichen Zugriff auf die Daten des Identitätsmanagement-Systems zulassen könnten.

c) Externe Verzeichnisse

Das Identitätsmanagement-System ermöglicht es, externe Verzeichnisse anzufertigen mit deren Hilfe etwa die Email-Adressen einer bestimmten Gruppe von Nutzern (z.B. alle Studenten des Professors X im 2. Semester) aufgelistet werden können. Sollen an all diese Adressen Mails versendet werden, so besteht zum einen die Möglichkeit, die jeweilige Liste zugänglich zu machen, zum anderen könnte die Mailversendung über den Administrator erfolgen, so dass außer diesem niemand die Adressen erfährt. Je nach Einzelfall kann etwa eine Kommunikation der Empfänger untereinander **erforderlich** sein, so dass das Zugänglichmachen der Liste angezeigt ist. Andernfalls ist im Sinne der Datensicherheit vom Veröffentlichen eines solchen externen Verzeichnisses abzusehen und die Verarbeitung externer Datenverzeichnisse **zentral vorzunehmen.**

5.5 Technische und Organisatorische Maßnahmen nach § 10 Abs. 2 DSG NRW

In diesem Abschnitt wird dargestellt, wie ein in der bisher beschriebenen Weise aufgebautes und funktionierendes Identitätsmanagement den Forderungen nach § 10 Abs. 2 Ziff. 1

bis 6 DSG NW genügt und ihnen in einigen wichtigen Punkten deutlich besser Rechnung trägt als die bisherigen Verfahren.

Ziff 1: Vertraulichkeit

Es ist sicherzustellen, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können.

Keine Anwendung und kein Anwender hat Zugriff zu den Daten im Repository und im Provisioning-System. Der Datenaustausch mit Ziel- und Quellsystemen erfolgt durch festgelegte automatische Workflows, deren Regeln im System dokumentiert und jederzeit überprüfbar sind. Direkter Zugriff ist nur für wenige zentrale, ausdrücklich benannte Administratoren möglich, die entsprechend geschult und auf die erforderlichen Geheimhaltung verpflichtet sind.

Ziff. 2: Integrität

Es ist sicherzustellen, dass Daten während, der Verarbeitung unversehrt, vollständig und aktuell bleiben

Unversehrtheit und Vollständigkeit sind gewährleistet, weil keine Zugriffe von außen möglich sind (siehe Ziff. 1). Aktualität wird in der Regel dadurch gefährdet, dass zum einen Änderungen mit großer zeitlicher Verzögerung eingetragen werden und zum anderen dann nur in einem System wirksam werden, weil es sich in der Praxis als außerordentlich schwierig und kaum realisierbar erweist, solche Änderungen (z. B. der Adresse oder Telefonnummer) allen (in der Regel nicht miteinander verbundenen) Systemen mitzuteilen, die diese Datenfelder ebenfalls führen. Genau das ist im Identitätsmanagement wesentlich besser gelöst: Eine Änderung wird einem Quellsystem (z. B. HIS-Daten) mitgeteilt, mittels automatischem Workflow an das Identitätsmanagement weitergegeben und von dort an alle Zielsysteme verteilt, die gemäß den festgelegten Regeln dieses Datenfeld ebenfalls führen. Diese Lösung setzt allerdings voraus, dass im Identitätsmanagement eine einheitliche Identität definiert ist, auf deren Basis erst die erforderlichen Zuordnungen vorgenommen werden können.

Ziff. 3: Verfügbarkeit

Es ist sicherzustellen, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.

Durch die automatische Provisionierung der Endsysteme sorgt das Identitätsmanagement sehr viel besser als die jetzige Organisationsform dafür, dass einmal eingegebene Daten und die daraus abgeleiteten Berechtigungen sehr zeitnah an all den Stellen zur Verfügung stehen, denen sie durch die festgelegten Regeln zugewiesen sind. Da der Datentransport nur automatisiert gemäß den im System festgelegten Regeln erfolgt und protokolliert wird, ist die ordnungsgemäße Verarbeitung sichergestellt, sofern diese jederzeit nachprüfbaren Regeln den entsprechenden Ansprüchen genügen.

Ziff. 4: Authentizität

Es ist sicherzustellen, dass personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können.

Dazu gilt einerseits das unter Ziffer 3 zur ordnungsgemäßen Verarbeitung (Regeln und Protokollierung) Gesagte, zum anderen sind die wenigen mögliche Quellsysteme, aus denen personenbezogene Daten stammen können, genau festgelegt. Somit können gar keine Daten im System sein, deren Ursprung nicht jederzeit zuverlässig festgestellt werden kann.

Ziff. 5: Revisionsfähigkeit

Es muss jederzeit festgestellt werden können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat

Die Revisionsfähigkeit im gesamten Bereich der IT-Benutzerverwaltungen wird erst mit der Einführung des Identitätsmanagements in verlässlicher und tatsächlich praktikabler Weise hergestellt, weil alle Eingriffe und alle Datenbewegungen zwischen Quell- und Zielsystemen zuverlässig und langfristig protokolliert werden und Vorgänge, die sich dem entziehen wollen, technisch nicht möglich sind.

Ziff. 6: Transparenz

Die Verfahrensweisen bei der Verarbeitung personenbezogener Daten müssen vollständig, aktuell und in einer Weise dokumentiert sein, dass sie in zumutbarer Zeit nachvollzogen werden können.

Dies gehört geradezu zur Definition eines Identitätsmanagements, wie in den vorstehenden Erläuterungen ausführlich dargetan ist und entscheidet es grundlegend von den vielen unterschiedlichen Nutzerverwaltungen, die dieser Forderung einzeln in ganz unterschiedlicher Weise, in ihrer Gesamtheit aber nur äußerst unvollkommen genügen.

5.6 Datenvermeidung

Gemäß §4 Abs. 2 DSG NW haben sich die Planung, Gestaltung und Auswahl informationstechnischer Produkte und Verfahren an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben und weiterzuverarbeiten.
Dieser Forderung wird Rechnung getragen, weil aus den Quellsystemen nur diejenigen Daten in das Identitätsmanagement übernommen werden, die für die Verwaltung von Rechten auf Zielsystemen und die Sicherstellung einer eindeutigen Identität tatsächlich erforderlich sind. Insbesondere aber werden an die Zielsysteme nur diejenigen Daten übermittelt, die diese ihrerseits für ihre Rechteverwaltung benötigen. Das sind in der Regel wesentlich weniger Daten, als dort bisher gespeichert sind. So sind beispielsweise in den Benutzerveraltungen der Rechenzentren Namen, Anschriften, Geburtsdaten gespeichert, die für die eigentliche Administration der dortigen IT-Systeme gar nicht direkt erforderlich sind, aber gleichwohl zur Unterscheidung bei Namensgleichheiten oder für Anschreiben zu Zwecken der Missbrauchsahndung oder der Gebührenerhebung erforderlich sind. Diese Speicherung kann unterbleiben, wenn die eindeutige Identitätsklärung im Identitätsmanagement bereits erfolgt ist bzw. wenn im Bedarfsfall über definierte Workflows auf solche im Identitätsmanagement gespeicherten Daten zurückgegriffen werden kann, wenn sie benötigt werden. Somit lässt sich diese Forderung des Datenschutzgesetzes durch Einsatz von Identitätsmanagement-Systemen wesentlich besser erfüllen als mit den bisherigen Verfahren.

5.7 Auskunft

Gemäß § 18 Abs. 1 DSG NW ist betroffenen Person von der verantwortlichen Stelle auf Antrag Auskunft zu erteilen über

1. die zu ihrer Person verarbeiteten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung,
3. die Herkunft der Daten und die Empfänger von Übermittlungen sowie
4. die allgemeinen technischen Bedingungen der automatisierten Verarbeitung

der zur eigenen Person verarbeiteten Daten.

Solche Auskünfte verlässlich, zeitnah und vollständig zu erteilen, ist bei einer zweistelligen Zahl voneinander unabhängiger Benutzerverwaltungen eine außerordentlich schwieri-

ge und unverhältnismäßig aufwendige Aufgabe. Das ändert sich grundlegend zum Positiven, wenn ein funktionierendes Identitätsmanagement Kernbestandteil der IKM-Infrastruktur ist. Wiederum ist allerdings eine einheitliche Identität im Identitätsmanagement Vorrausetzung dafür, dass dies möglich wird.