Flexible dezentrale Administration überschneidender Benutzergruppen – Informationelle Selbstbestimmung durch benutzerkontrollierte Provisionierung

Andreas Brennecke, Stefan Finke, Jerome König, Gudrun Oevel

Zentrum für Informations- und Medientechnologien (IMT)
Universität Paderborn
Warburger Str. 100
33098 Paderborn
brennecke@uni-paderborn.de
stefan.finke@uni-paderborn.de
jerome@uni-paderborn.de
gudrun.oevel@uni-paderborn.de

Abstract: Dieser Beitrag stellt Aspekte des im Zentrum für Informations- und Medientechnologien (IMT) der Universität Paderborn entwickelten Identitätsmanagements vor. Dabei gehen wir speziell auf die dezentrale (d. h. nicht vom IMS-Betreiber selbst vorgenommene) Administration sowie die benutzerkontrollierte Provisionierung vom Identitätsmanagementsystem in die angeschlossenen Zielsysteme ein. Desweiteren erläutern wir das Konzept des benutzerkontrollierten Matchings, bei dem der Dateninhaber im Sinne der Informationellen Selbstbestimmung die volle Kontrolle über die Integration seiner Personendaten behält.

Einleitung

Fast jede Hochschule steht infolge der zunehmenden Durchdringung mit elektronischen Diensten sowie knapper werdender Personalressourcen aktuell vor der Aufgabe, ihre Vielzahl gewachsener dienstspezifischer Nutzerverwaltungen in ein *hochschulweites Identitätsmanagement* zu überführen. Darüber hinaus haben die verschiedenen Anbieter elektronischer Dienste ein großes Interesse am Zugriff auf aktuelle, verlässliche und redundanzfreie Personendaten.

Wenngleich sämtliche Identitäten zentral verwaltet werden, sollen verschiedene Bereiche der Hochschule diese dennoch administrieren können. Beispielsweise werden die Identitäten der Studierenden zentral erstellt, während einzelne dezentrale Bereiche jeweils autonom Identitäten für ihre Gäste anlegen können sollen. Des Weiteren muss berücksichtigt werden, dass Personen überschneidende Rollen ausüben bzw. gleichzeitig verschiedenen Bereichen der Hochschule zugeordnet sein können. Das trifft ebenso für Studierende zu, die in mehreren Fakultäten studieren, wie für Gäste, die neben dezentralen Ressourcen in den für sie zuständigen Bereichen auch zentrale Dienste (bspw. das WLAN) nutzen sollen. Wünschenswert ist außerdem eine weit reichende *delegierte Administration*, um die Nutzer bedarfsgerecht an verschiedenen Stellen zu betreuen.

Dabei sind umfangreiche rechtliche Bestimmungen einzuhalten und für die Nutzer *Transparenz* und *Mitbestimmungsmöglichkeiten* zu schaffen. Unabhängig davon, welcher Bereich seine Identität angelegt hat, soll der Inhaber der Identität entscheiden, welche Dienste welcher Bereiche er „abonnieren" möchte. Wir beschreiben im Folgenden einen Ansatz der sowohl den Nutzern eine hohe *informationelle Selbstbestimmung* ermöglicht, als auch den besonderen Strukturen an Hochschulen gerecht wird.

Identitätsmanagement

Unter einer *Identität* verstehen wir im Folgenden eine Sammlung personenbezogener Daten. Beim Identitätsmanagement werden diese Daten erhoben, gespeichert, verwaltet und zur Nutzung durch verschiedene andere Systeme, insbesondere zur *Authentifizierung* und *Autorisierung*, bereitgestellt. Gegenüber den häufig anzutreffenden lokalen Benutzerverwaltungen ermöglicht ein zentrales Identitätsmanagement innerhalb einer Organisation konsistente und verlässliche Datenbestände. Hochschulen weisen gegenüber klassischen rein hierarchischen Organisationsstrukturen jedoch auch bezüglich ihrer IT-Struktur einige Besonderheiten auf.

IT-Struktur an Hochschulen

Die Binnenorganisation von deutschen Hochschulen erfolgt über wissenschaftliche Bereiche (Institute, Fachbereiche, Fakultäten), zentrale Betriebseinheiten (Bibliotheken, Medien- oder Rechenzentren) sowie zentrale Hochschulverwaltungen.

Bedingt durch die Entwicklungen im Bereich der Mikroprozessortechnik erfolgten vor 20 Jahren die Abkehr vom klassischen Mainframe und die Einführung von Client-Server-Strukturen. Damit einher ging der Trend zum Aufbau vieler kleiner und kleinster dezentraler IT-Betriebsgruppen, die die Clients/Desktops vor Ort betreuten sowie der Abbau der bis dahin zentralen Funktionen der Rechenzentren (siehe Moog 2005). In Folge dieses Dezentralisierungstrends findet man an Hochschulen üblicherweise nicht nur eigene IT-Betriebsgruppen in den Instituten und Fakultäten sondern auch eigene Rechenzentren in Bibliotheken und Verwaltungen. Diese betreiben Rechner sowie Serveranwendungen für ihren Bereich. Jede dieser Anwendungen beinhaltet standardmäßig eine eigene Benutzerverwaltung. Als Folge verfügen Benutzer und Benutzerinnen in unterschiedlichen Bereichen der Hochschule über unterschiedliche Benutzerkennungen und Passwörter, was sowohl für die Anwenderinnen und Anwender als auch für die Betreuenden einen erheblichen Verwaltungsaufwand beinhaltet. Hinzu kommt, dass die Erlangung von Zugriffsrechten mit unterschiedlichen Verwaltungsvorgängen behaftet ist, in denen häufig ähnliche Daten erhoben werden. Dies entspricht mittlerweile nicht mehr dem Anspruch, den Kunden an einer Hochschule an die Nutzung von IT-Systemen stellen. Für die Administratoren ergibt sich ein zusätzlicher Verwaltungsaufwand durch regelmäßiges Überprüfen der Gültigkeit von Berechtigungen. Insgesamt sind die unterschiedlichen Nutzerverwaltungssysteme kundenunfreundlich und wartungsintensiv.

Darüber hinaus ergeben sich neue Anforderungen aus der Koppelung von bislang eigenständigen IT-Systemen und der Vereinheitlichung und Personalisierung des Informationszugriffs über so genannte Webportale. Es ist einleuchtend, dass für die Verdichtung und Personalisierung von IT-Diensten die entsprechenden Benutzer und Benutzerinnen eindeutig über alle beteiligten IT-Systeme hinweg identifiziert werden müssen.

Konzepte des Identitätsmanagements

Ein *Identitätsmanagementsystem (IMS)* stellt eine Infrastruktur für das *Identitätsmanagement (IdM)* bereit. Aus vorhandenen Personendatenbeständen *(Quellsystemen)* können Identitäten automatisch generiert und aktualisiert werden. Auf diese Weise sind sämtliche Daten einer Person beim *IMS-Betreiber* zentral gebündelt, auch wenn sie faktisch von verschiedenen Stellen verwaltet werden. Aus diesen organisationsübergreifenden Identitäten können dann – in Abhängigkeit bestimmter Attribute – Zugänge und Zugriffsrechte für die verschiedenen elektronischen Dienste der Organisation *(Zielsysteme)* erzeugt werden.

Historisch durchlief die Entwicklung hin zu Identitätsmanagementsystemen verschiedene Stufen, die sich auch heute noch als deren Komponenten erkennen lassen. In den 1990er Jahren wurden dezentrale Benutzerverwaltungen erstmalig durch die Einführung zentraler *Verzeichnisdienste* abgelöst, gegenüber denen nun eine standardisierte Authentifizierung (bspw. per LDAP) möglich war (vgl. Knop, Bode 2002). *Metaverzeichnisse* ermöglichten im Folgenden den automatisierten Abgleich mit Verzeichnissen und Datenbanken (siehe Klapper, Oevel 2003). Für den „Anschluss“ unterschiedlichster Zielsysteme und die differenzierte Vergabe von Berechtigungen spielt in den letzten Jahren die *Provisionierung* eine zunehmende Rolle.

Ein Identitätsmanagementsystem kann aus unterschiedlichen Komponenten bestehen (vgl. König 2005, Abschnitt 2.4.1):

- *Identity Repository:* Speicherung und Administration von Identitäten in einer Datenbank oder einem Verzeichnisdienst
- Ein *Metaverzeichnis / Meta Directory* synchronisiert verschiedene Datenbanken und Verzeichnisdienste über so genannte *Konnektoren,* die z. B. auch die Konvertierung verschiedener Datenformate vornehmen.
- Ein *Virtual Directory* arbeitet wie ein Meta Directory, allerdings ohne eigene Datenhaltung. Alle Anfragen werden daher an die verschiedenen beteiligten Systeme weitergeleitet. Auf diese Weise sind die Daten aktuell und redundanzfrei.
- *Provisionierung / Provisioning:* Erstellung, Sperrung, Entfernung von Zugängen *(User Provisioning)* und die Synchronisation der Passwörter und Zugriffsrechte *(Ressource Provisioning).*
- *Workflow-Automatisierung,* d. h. die Abbildung von Geschäftsprozessen wie z. B. die Beantragung oder Kündigung eines Dienstzugangs, kann als einzelne Komponente oder als Teil eines Provisioning-Systems realisiert sein.

- Benutzerschnittstellen zur Administration und Selbstadministration *(Self Care)*

Identitätsmanagementsysteme werden kommerziell von verschiedenen Herstellern (BMC, Siemens, Novell, IBM, SUN, …) angeboten, wobei diese jeweils unterschiedliche Ausprägungen bei den einzelnen Komponenten besitzen.

Informationelle Selbstbestimmung

Verzeichnisdienste und Identitätsmanagementsysteme sind datenschutzrechtlich durchaus ambivalent zu sehen. Einerseits steigen durch eine Zusammenführung von Daten für den Betrieb unterschiedlicher IT-Systeme die Missbrauchmöglichkeiten, andererseits werden aber auch die Verfügbarkeit und Transparenz der gespeicherten Daten erhöht (vgl. Dessler 2002). Grundsätzlich muss ein Identitätsmanagementsystem viele datenschutzrechtliche Grundsätze berücksichtigen, beispielsweise die Prüfung der Zulässigkeit der Datenspeicherung, deren Zweckbindung, die Minimalität der erhobenen Daten sowie technische und organisatorische Maßnahmen zur Datensicherheit. Erschwerend kommt hinzu, dass es sich beim Identitätsmanagement nicht um ein einzelnes System handelt, sodass auch sämtliche angeschlossene Systeme (Datenbanken, Verzeichnisse, Zielsysteme) denselben Anforderungen genügen müssen. Anders als bei den meisten Gesetzen wird mit den Datenschutzgesetzen nicht erst der Missbrauch geahndet sondern der *ordnungsgemäße Gebrauch* von Daten geregelt (siehe Holl 1997), wofür Betreiber von Systemen, die personenbezogene Daten verarbeiten, geeignete Maßnahmen ergreifen müssen.

Neben der Einhaltung einzelner datenschutzrechtlicher Bestimmungen, stellt die Verbesserung der informationellen Selbstbestimmung ein übergeordnetes Handlungskriterium für den Umgang mit personenbezogenen Daten dar. In der Datenschutzliteratur ist die Informationelle Selbstbestimmung bereits ein wesentlicher Bestandteil von Identitätsmanagement, das „die grundsätzliche Kontrolle des Nutzers über seine eigenen Daten“ ermöglicht (Hansen et al. 2003, S. 552). Dies schließt auch die anonyme Nutzung von Diensten sowie den Gebrauch von verschiedenen Pseudonymen ein (siehe Köhntopp, Pfitzmann 2001). Im Kontext unseres universitären Identitätsmanagementsystems steht jedoch die Zuordnung von Aktionen im Rahmen des Studiums und der Arbeitsprozesse im Vordergrund. Die einzelnen angeschlossenen Systeme benötigen in der Regel verlässliche Daten. Dazu werden beispielsweise auf Grundlage der Einschreibungsordnung Daten der Zentralverwaltung an die Benutzerverwaltung der Bibliothek übermittelt, sodass eine Person über einen Ausweis einer Identität mit definierter Rolle (immatrikulierter Student) zugeordnet werden kann.

Es sollen nicht mehr Daten als erforderlich in die verschiedenen auch dezentralen Systeme verteilt werden. Hierzu ermöglicht das Identitätsmanagementsystem eine zentrale Steuerung der Nutzung persönlicher Daten in den verschiedenen Diensten und Abteilungen. Zur Wahrung der Informationellen Selbstbestimmung erhalten nur diejenigen Dienstanbieter Identitätsdaten, deren Dienste vom Identitätsinhaber *tatsächlich* genutzt werden (Zweckbezogenheit). Jeder Dienst erhält ferner ausschließlich die *für diesen Dienst benötigten* Daten (Minimalitätsprinzip). Um welche Daten es sich dabei handelt, ist für den Benutzer bereits bei Beantragung des Dienstes ersichtlich (Transparenz),

indem die Anbieter von Diensten ihre *Policy* im IMS einsehbar hinterlegen. Die Nutzer behalten so einen umfassenden Überblick, an welchen Stellen welche Daten über sie gespeichert sind und können einzelne nicht (mehr) benötigte Dienste jederzeit auch wieder kündigen und dadurch die weitere dortige Nutzung ihrer Daten untersagen. Mit Kündigung der Dienstnutzung endet auch das entsprechende Datenzugriffsrecht des Anbieters im IMS. Über ein Protokoll lässt sich für jeden Benutzer auch nachträglich einsehen, welcher Dienstanbieter in welchem Zeitraum welche Daten von ihm bezogen hat. Der Dienstanbieter erhält auf diese Weise stets aktuelle und redundanzfreie Daten, während der Dienstnutzer die Kontrolle über die Verbreitung seiner Personendaten hat. Dadurch werden sowohl eine *Benutzerkontrollierte Provisionierung* als auch eine *Revisionsfähigkeit* (die Nachvollziehbarkeit der Urheberschaft der erfolgten Dateneinträge und Verarbeitungsschritte) ermöglicht.

Das Paderborner Identitätsmanagement

Das Zentrum für Informations- und Medientechnologien der Universität Paderborn betreibt seit einigen Jahren einen zentralen Verzeichnisdienst, der Studierenden, Personal und Gästen eindeutige Identitäten zur Nutzung elektronischer Dienste zur Verfügung stellt. Über die Zugangsverwaltung für hochschulweite Dienste (bspw. WLAN-Zugang, E-Mail) hinaus ist diese Lösung als weitergehendes Identitätsmanagement konzipiert, um beispielsweise Datenflüsse zu steuern und dezentrale Dienste zu provisionieren. Die Bedienung erfolgt webbasiert über ein Self-Care-Interface für die Nutzer sowie ein Administratoren-Interface.

Für die Benutzer erlaubt die Self-Care-Interface neben der Einsicht und der partiellen Änderungsmöglichkeit für die Daten insbesondere auch die Steuerung der Aktivierung sowie einer eventuellen Zusammenlegung (Matching) von verschiedenen Identitäten einer Person (bspw. als Student und Mitarbeiter) sowie die Steuerung der Nutzung dezentraler Dienste, die mit einer Datenweitergabe verbunden ist.

Benutzerkontrolliertes Matching

Eine wichtige Aufgabe bei Einführung und Betrieb eines Identitätsmanagements ist die Integration von Personendaten aus verschiedenen Datenquellen in den Attributen einer Identität, nachfolgend als *Matching* von Personendaten bezeichnet. Dieses Matching muss, innerhalb der Rahmenvorgaben der Organisation, sowohl auf die technische Realisierbarkeit als auch auf besondere datenschutzrechtliche Fragestellungen hin untersucht werden.

Beim Matching werden die Einträge der beteiligten Personendatenquellen zunächst auf eine *gemeinsame* Menge von Schlüsselattributen überprüft. Diese Schlüsselattribute sollen Datensätze derselben Personen in allen Datenquellen eindeutig identifizieren. Datensätze, die in allen Schlüsselattributen identische Werte haben, werden dann unter einer Identität zusammengefasst. Sind die Werte der Schlüsselattribute nicht identisch, wird davon ausgegangen, dass die Daten sich auf verschiedene Personen beziehen, und

sie werden unter verschiedenen Identitäten abgelegt. Die Identität der Schlüsselattribute kann hierbei auch durch Wahrscheinlichkeitswerte bestimmt werden.

Folgende Fragestellungen gilt es bei diesem Ansatz des Matchings zu beachten:

- Erfüllt die postulierte gemeinsame Schlüsselmenge die Schlüsselkriterien in allen beteiligten Datenquellen wirklich hinreichend?
- Ist die Qualität aller beteiligten Datenquellen für die Integration in einem Datensatz ausreichend? Wie reagiert das Matchingverfahren auf fehlerhafte Daten?
- Wie sind unterschiedliche Konventionen[1] der Datenquellen zu beachten?

	Datenquelle 1	*Datenquelle 2*
Vorname	Frank	Frank-Uwe
Nachname	Neumann	Neumann
Geburtsdatum	3.6.1967	6.3.1967

Tabelle 1: Matchingproblem

Tabelle 1 verdeutlicht diese Probleme anhand eines Beispiels. Es werden Personendaten aus zwei Datenquellen aufgrund der gemeinsamen Schlüsselattribute Vorname, Nachname und Geburtsdatum integriert. Obwohl es sich hierbei um Datensätze derselben Person handelt, wird ein Matching fehlschlagen. Die verschiedenen Vornamen (Datenquelle 2 speichert Doppelnamen, Datenquelle 1 nicht) lassen sich vermutlich auflösen. Kommt aber zusätzlich der Zahlendreher beim Geburtsdatum hinzu, wird selbst ein Matching das mit Wahrscheinlichkeitswerten arbeitet scheitern.

Grundsätzlich können zwei Ereignisse zu einem fehlerhaften Matching führen:

1. Die postulierten Schlüsselattribute sind *identisch*, aber die Daten beziehen sich auf verschiedene Personen.
2. Die postulierten Schlüsselattribute sind *nicht identisch*, die Daten gehören trotzdem derselben Person.

Dem ersten Punkt wird bei der Entwicklung geeigneter Matchingverfahren viel Aufmerksamkeit geschenkt. Da es hier zu einer Zuordnung von Personenattributen zu der falschen Person kommen kann, muss ein fehlerhaftes Matching dieser Art ausgeschlossen sein. Dieser Fehlerfall lässt sich bei der Verwendung von nicht idealen Schlüsselattributen für ein automatisches Matching jedoch niemals hundertprozentig vermeiden. Der zweite Punkt wird hingegen oft vernachlässigt. Auch er lässt sich in der Regel nicht ausschließen und kann zu einer Verletzung der beim IdM häufig geforderten 1:1-Beziehung zwischen Person und elektronischer Identität führen.

[1] Eine Konvention ist z.B. die Festlegung, ob und wie Doppelnamen einer Person gespeichert werden.

Neben den dargelegten technischen Problemen des Matchings sind hier die Maßgaben des Datenschutzes besonders zu beachten. Das Zusammenführen von Personendaten aus verschiedenen Verzeichnissen ermöglicht eine komplette Sicht aller gespeicherten Daten einer Person an zentraler Stelle. Der Vorgang der Integration von Nutzerdaten und anschließender Weitergabe an diverse Dienstanbieter sollte demnach, bei Einhaltung der Prinzipien der Informationellen Selbstbestimmung, mit Zustimmung und Kontrolle des Dateninhabers geschehen. Auch aus Sicht des Matchingverfahrens macht eine Einbeziehung des Dateninhabers in den Integrationsvorgang durchaus Sinn, denn der Nutzer kennt die eigenen Daten und ist demnach der eigentliche „Experte" für die Kontrolle des Matchingvorgangs.

Paderborner Matching-Ansatz

Der Entwurf des Identitätsmanagements der Universität Paderborn wurde im Hinblick auf das Matchingverfahren im Wesentlichen von zwei Zielvorgaben bestimmt:

1. Die bestehenden Systeme zur Registrierung von Nutzerdaten (HISSOS für Studierende und HISSVA für Mitarbeiter) sollen weiterhin führende Systeme für diese Aufgabe bleiben. Personen, die dort nicht erfasst sind, wie etwa Tagungsgäste oder Honorarprofessoren, sollen durch ein gesondertes Verfahren registriert werden.
2. Aus Gründen der Informationellen Selbstbestimmung soll kein automatisches Matching durchgeführt werden.

Die erste Zielvorgabe führt dazu, dass auch nach der Einführung des IdM mehrere verschiedene Registrierungsverfahren im Einsatz sind. Da die Registrierungsdaten nicht untereinander abgeglichen sind[2], sich aber dieselbe Person bei verschiedenen Stellen unabhängig registrieren kann (z. B. als Studierender aber auch als Mitarbeiter), muss eine Integration dieser Daten in einer Identität auch zur Laufzeit des IMS möglich sein. Wir sprechen hier von einem *Online-Matching-Verfahren*, im Gegensatz zum klassischen *Offline-Matching*, bei dem eine Integrationsphase *vor* Einführung des IdM durchgeführt wird, um danach alle Personen mit einem einheitlichen Verfahren zu registrieren.

Zur Wahrung der Informationellen Selbstbestimmung sehen wir uns verpflichtet, den Benutzer über ein Matching seiner Daten zu informieren. Weiterhin soll der Dateninhaber an dieser Stelle die Möglichkeit des Widerspruchs haben, ohne dass ihm dadurch die Nutzung einzelner Dienste verweigert wird.

Die Idee eines Ansatzes, der diesen beiden Zielvorgaben entspricht, besteht nun darin, das Matching nicht vom IMS automatisch ausführen zu lassen. Stattdessen wird dem Benutzer die Entscheidungsmöglichkeit gegeben, seine Registrierungsdaten einer bereits vorhandenen Identität hinzuzufügen, oder diese alternativ zum Anlegen einer neuen Identität zu nutzen

---

[2] Die an unserer Universität eingesetzte Software der HIS GmbH verfügt derzeit über keine Identitätsmanagement-Komponente

Zur Realisierung dieses Ansatzes werden die bei der Registrierung erhobenen Personendaten in einer so genannten *Identitätsquelle* abgelegt. Bei der Identitätsquelle handelt es sich um ein Datensatz, der Registrierungsdaten zunächst getrennt von einer Identität speichert und zusätzlich mit Authentifizierungsdaten[3] versehen wird. Die Identitätsquelle ermöglicht so eine Trennung des Vorgangs der Registrierung vom Vorgang der Aktivierung einer Identität, so dass die Aktivierung zu einem späteren Zeitpunkt vom Inhaber der Identität selbst durchgeführt werden kann.

Ein einfaches Beispiel veranschaulicht den Vorgang der benutzerkontrollierten Aktivierung von Identitätsquellen. Eine Person ist zunächst Studierender unserer Universität und wird dann zusätzlich als Mitarbeiter eingestellt. Bei der Immatrikulation wurde aus den dort erhobenen Personendaten automatisch eine Identitätsquelle erzeugt, welche die Person dann zum Anlegen einer Identität verwendet hat. Um nun auch Dienste für Mitarbeiter nutzen zu können, lässt sie sich manuell als Mitarbeiter registrieren. Die Registrierungsdaten werden in eine weitere Identitätsquelle aufgenommen. Sie hat nun zwei Möglichkeiten, mit dieser neuen Registrierung zu verfahren:

Abbildung 1 stellt den bewussten Verzicht des Identitätsinhabers auf das Matching seiner Personendaten dar. Die neue Identitätsquelle wird zum Anlegen einer zweiten Identität genutzt, die von der ersten Identität völlig unabhängig verwaltet wird. Mit der einen Identität kann der Inhaber Dienste für Mitarbeiter nutzen, mit der Anderen Dienste für Studierende. Steht ein Dienst beiden Rollen zur Verfügung, kann dieser Dienst alternativ mit beiden Identitäten genutzt werden.

Abbildung 2 verdeutlicht die Integration zweier Identitätsquellen innerhalb einer Identität. Nach der Registrierung als Mitarbeiter wird die daraus hervorgehende Identitätsquelle in eine bereits vorhandene Identität integriert. Dieser Vorgang wird vom Benutzer selbst durchgeführt, der Inhaber sowohl der Identität als auch der zusätzlichen Identitätsquelle ist. Diese Inhaberschaft wurde zuvor durch entsprechende Authentifizierungsverfahren nachgewiesen.

[3] Wir erzeugen bspw. bei der Registrierung eine alphanumerische Transaktionsnummer, die dann in der Identitätsquelle verschlüsselt gespeichert und dem Nutzer ausgehändigt wird.

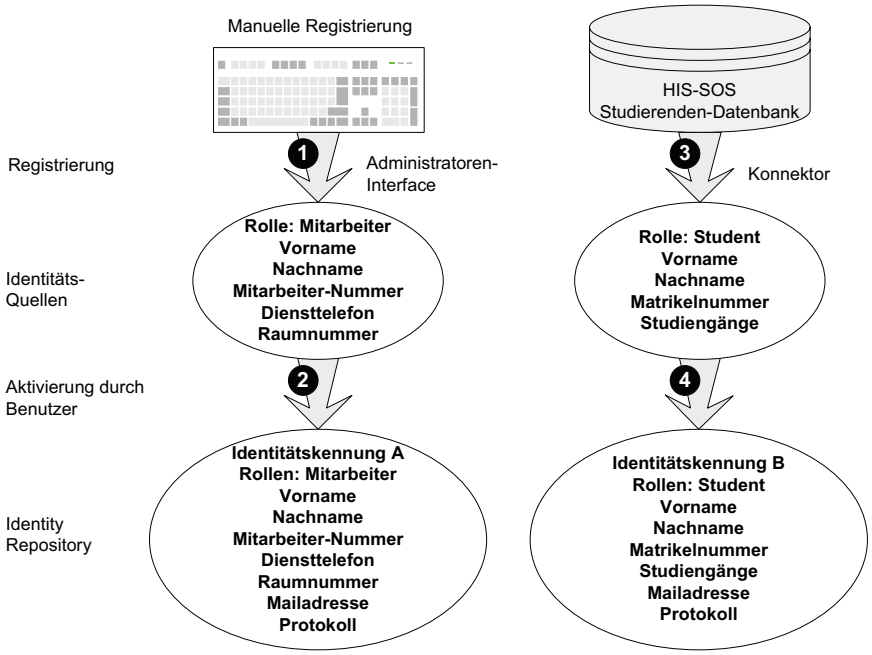

Abbildung 1: Zwei unabhängige Identitäten derselben Person

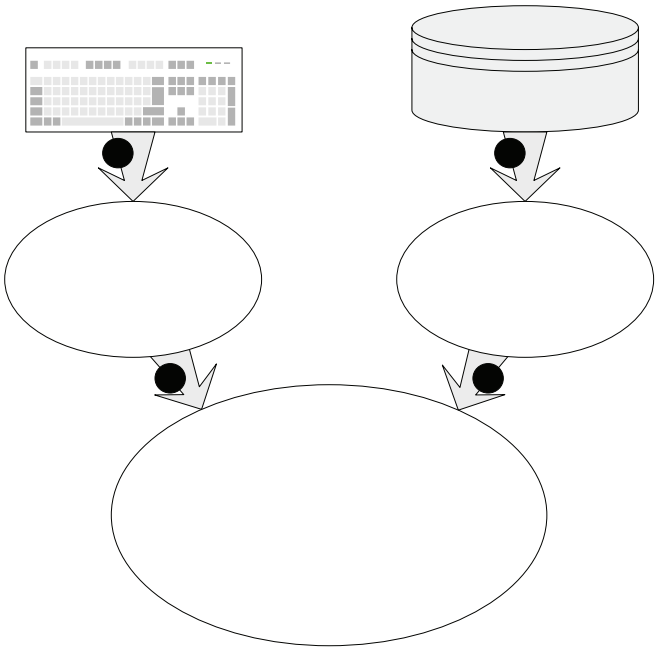

Abbildung 2: Integrierte Identität

Benutzerkontrollierte Provisionierung

Bei einer *automatischen* Provisionierung werden die jeweils benötigten *Teilidentitäten* an sämtliche Zielsysteme übermittelt, zu denen der jeweilige Benutzer entsprechend seiner Rollen Zugang haben soll. Hierbei hat der Benutzer im besten Falle die *Übersicht*, nicht jedoch die *Kontrolle* darüber, welche Abteilung der Hochschule an welche seiner persönlichen Daten gelangt. Zur Wahrung der Informationellen Selbstbestimmung entscheidet im Paderborner IMS der Identitätsinhaber selbst, welche Dienste er nutzen möchte. Dabei handeln der Identitätsinhaber, der IMS-Betreiber und der Dienstanbieter im Rahmen einer für die jeweilige Dienstnutzung vorgeschriebenen Policy. Die einzigen beiden Ausnahmen von diesem Prinzip der *benutzerkontrollierten Provisionierung* sind die Dienste *Authentisierung* und *Mailbox*, welche für den Betrieb des IMS zwingend erforderlich und daher für jede Identität automatisch aktiviert sind.

Nach der initialen Einrichtung eines neuen Dienstes kann eine Beantragung durch beliebige Identitätsinhaber erfolgen. Der Dienstanbieter bearbeitet die vorliegenden Anträge, d. h. er genehmigt sie oder lehnt sie ab. Erst durch Beantragung der Dienstnutzung erhält der Anbieter dabei die Zugriffsrechte auf die in der Policy vereinbarte Teilidentität. Diese einzelnen Schritte werden im Folgenden genauer erläutert.

Einrichtung eines Dienstes

Zur Einrichtung eines neuen Dienstes werden der Name des Dienstes, eine Beschreibung der Details der Dienstnutzung, sowie Erreichbarkeitsdaten der Ansprechpartner des Dienstes erfasst. Ferner wird eine Policy formuliert, welche die zur Nutzung des Dienstes erforderlichen Attribute, Vereinbarungen zum Umgang mit diesen Attributen sowie eine allgemeine Benutzerordnung des Dienstes umfasst.

Beantragung der Dienstnutzung

Über das Self-Care-Interface hat jeder Identitätsinhaber eine Übersicht aller angebotenen Dienste (Abbildung 3). Zu jedem Dienst wird der aktuelle Status angezeigt, z. B. *nicht beantragt, beantragt, persönliches Erscheinen erforderlich, genehmigt, abgelehnt, gekündigt*. Ein Antrag auf Dienstnutzung kann jederzeit gestellt oder zurückgezogen werden, ebenso kann ein bereits genehmigter Dienst wieder gekündigt werden.

Bei der Beantragung eines Dienstes werden die bei der Diensteinrichtung erfassten Dienstdaten einschließlich der Policy angezeigt (Abbildung 4). Die Antragstellung kann nur erfolgen, wenn der Benutzer dieser Policy zustimmt. Es werden ferner die für die Dienstnutzung erforderlichen Attribute und deren aktuelle Werte angezeigt. Dazu gehören üblicherweise mindestens die Identitätskennung und die Mailadresse, um die Identifizierbarkeit und die Erreichbarkeit des Dienstnutzers sicherstellen zu können.

Abbildung 3: Beantragung dezentraler Dienste

Abbildung 4: Beschreibung eines einzelnen Dienstes

Genehmigung der Dienstnutzung

Die Bearbeitung eines Antrags auf Dienstnutzung kann manuell vom Dienstanbieter oder automatisch durchgeführt werden.

Die *manuelle* Bearbeitung erfolgt über das Administratoren-Interface. Der Dienstanbieter kann einen vorliegenden Antrag dort entweder genehmigen und damit seinerseits der Policy zustimmen, oder den Antrag ablehnen und hierfür falls gewünscht eine Begründung angeben. Für die Nutzung einiger Dienste ist ein persönliches Erscheinen des Antragstellers erforderlich, z. B. um eine Magnetkarte auszuhändigen.

Sofern ein persönliches Erscheinen nicht erforderlich ist, können Dienstanträge auch *automatisch* vom IMS bearbeitet werden. Eine Genehmigung oder Ablehnung erfolgt dann abhängig von bestimmten Attributen der Identität. Realisiert wird dieses Verfahren über Filterregeln des Verzeichnisdienstes.

Das manuelle und das automatische Verfahren können kombiniert werden, z. B. erhalten alle Studierenden den Dienst *MS Academic Alliance* automatisch genehmigt, sobald sie ihn beantragen. Alle Anträge von Nicht-Studierenden sollen hingegen vom Dienstanbieter manuell bearbeitet werden.

Die Dienstgenehmigung kann indirekt noch auf eine dritte Weise erfolgen, nämlich durch die *automatische Diensteinrichtung* für bestimmte Benutzergruppen bereits durch Aktivierung der Identitätsquelle. Dieses Verfahren wird im Abschnitt „Dezentrale Registrierung“ behandelt.

Provisionierung der vereinbarten Teilidentität

Die Provisionierung der Teilidentität an den Dienstanbieter erfolgt über ein Zugriffsrecht auf das Identity Repository. Sobald dem Dienstanbieter ein Antrag auf Dienstnutzung vorliegt, erhält er ein Leserecht auf die vereinbarten Attribute. Die Daten dürfen von ihm ausschließlich im Rahmen der in der Policy vereinbarten Dienstnutzung genutzt werden.

Der Dienstanbieter kann – genau wie der Dienstnutzer – einen genehmigten Dienst wieder kündigen. In diesem Falle erlischt augenblicklich das Zugriffsrecht des Anbieters auf die Teilidentität im Identity Repository. Der noch vorhandene Dienstzugang kann jedoch für eine Übergangszeit weiter genutzt werden. Dies dient auch der Datensicherheit im Falle einer versehentlichen Kündigung.

Dezentralisierung der Administration

Ein wichtiges Leistungsmerkmal des Paderborner IMS ist die Möglichkeit der dezentralen Registrierung neuer Identitäten sowie des dezentralen Supports für vorhandene Identitäten z. B. bei vergessenen Passwörtern oder Fragen zum Self-Care-Interface. In solchen Fällen sollen die Benutzer sich statt vom IMS-Betreiber auch von einer beliebigen dezentralen Abteilung (z. B. einem Dienstanbieter) helfen lassen können. Erreicht wird dadurch eine Entlastung des IMS-Betreibers, eine Verbesserung der räumlichen und zeitlichen Erreichbarkeit des Benutzersupports und eine größere Flexibilität der Dienst-

anbieter. Damit bei der daraus resultierenden Vielzahl möglicher Administratoren nicht die Übersicht verloren geht, wurde eine Protokollierung aller wesentlichen Supportvorgänge *(Auditing)* implementiert.

Dezentrale Registrierung

Die Registrierung einer Person kann im Paderborner IMS nicht nur *zentral* über den IMS-Betreiber erfolgen, sondern auch *dezentral* über beliebige Abteilungen (z. B. Dienstanbieter). Diese dezentrale Registrierung bietet einige Vorteile: So kann jede Abteilung ihre eigenen Gäste selbst am besten identifizieren und einrichten; ferner ist sie für diese auch die naheliegendste Anlaufstelle. Ohne die Möglichkeit, benötigte Accounts umgehend selbst anbieten zu können, entstehen oft aus Zeitdruck oder Bequemlichkeit so genannte „Sammelaccounts", welche ein Sicherheitsrisiko darstellen. Dezentrale Registrierungen können auch der Überbrückung dienen, um noch nicht in der HIS-Software erfassten Studierenden oder Mitarbeitern bereits eine Identität zur Verfügung stellen zu können. Dezentral registrierte Identitätsquellen unterscheiden sich nur durch die möglichen Rollen von zentral registrierten: Nur die letzteren besitzen die Rollen *Student* oder *Mitarbeiter*. Daraus resultiert auch, dass Identitäten, die auf dezentral registrierten Identitätsquellen beruhen, trotzdem *sämtliche* Dienste der Hochschule beantragen können – ob die Anträge genehmigt werden, entscheidet sich natürlich im Einzelfall.

Beispiel

Das folgende Beispiel verdeutlicht die Möglichkeiten der dezentralen Registrierung. Eine Person möchte den Dienst „Informatik-Account" nutzen. Es sind zwei Fälle zu unterscheiden:

a) Entweder besitzt die Person bereits (aus irgendeinem Grunde) eine Identität. In diesem Fall stellt sie wie bereits beschrieben via Self-Care-Interface einen Antrag auf Dienstnutzung und wartet auf die Genehmigung durch die Informatik-Rechnerbetreuung.
b) Besitzt sie hingegen noch keine Identität, so braucht die Person deswegen nicht zum IMS-Betreiber geschickt zu werden (der womöglich gerade keine Supportzeit hat oder sich am anderen Ende des Campus befindet, und der allgemein gar nicht wissen kann, ob jemand wirklich Gast der Informatik werden soll). Stattdessen registriert die Informatik-Rechnerbetreuung die Person selbst und legt dabei als Rolle „Gast der Informatik" fest. Durch die Aktivierung erhält die Person dann anschließend eine Identität. Diese Identität wird wie alle anderen Identitäten im *zentralen* Identity Repository angelegt. Dadurch kann die Person anschließend analog zum Fall a) beliebige Dienste aller Dienstanbieter beantragen, ohne dass dazu jeweils eine weitere Registrierung erforderlich würde.

Automatische Diensteinrichtung

Am Ende von Fall b) *könnte* die Person fortfahren wie unter a) geschildert, um an den gewünschten Informatik-Zugang zu gelangen. Allerdings wird zur Zeitersparnis für alle Beteiligten hier stattdessen das Verfahren der *automatischen Diensteinrichtung* ange-

wandt: Für jede Rolle kann festgelegt werden, welche Dienste für eine Identität mit dieser Rolle automatisch bereits bei Aktivierung der Identität *eingerichtet*, d. h. *beantragt* und *genehmigt*, werden sollen. Für die Rolle „Gast der Informatik" wurde festgelegt, dass der Dienst „Informatik-Account" automatisch eingerichtet werden soll. Dadurch besitzt die Person im Fall b) bereits nach Aktivierung ihrer Identität sofort einen Informatik-Zugang. Die automatische Diensteinrichtung ist jedoch nicht verpflichtend, d. h. ein auf diese Weise eingerichteter Dienst kann wie jeder andere Dienst nach Belieben vom Benutzer oder vom Dienstanbieter wieder gekündigt werden.

Dezentraler Support

Der *zentrale,* d. h. vom IMS-Betreiber selbst geleistete Support kann auf *sämtliche* Identitäten zugreifen. Hier können auch diverse Suchfilter verwendet werden. Im Gegensatz dazu kann eine Abteilung, welche *dezentralen* Support leistet, nur auf diejenigen Identitäten zugreifen, welche zuvor via Self-Care-Interface der Betreuung durch ebendiese Abteilung zugestimmt haben. Eine Verwendung von Suchfiltern ist hier aus Datenschutzgründen nicht möglich.

Der Benutzersupport funktioniert über das Administratoren-Interface. Um einem Benutzer zu helfen, z. B. sein Passwort neu zu setzen oder in seinem Namen einen Dienst zu konfigurieren, gelangt der Administrator von dort in eine Maske, die sich stark am Self-Care-Interface orientiert. Hier kann er praktisch alle Aktionen durchführen, die der Benutzer selbst auch durchführen kann. Die einzige Ausnahme ist gerade die Wahl der Abteilungen für den dezentralen Support, da sonst ein für den Benutzer nicht kontrollierbarer Rechtefluss entstehen würde.

Bei der Einrichtung eines Dienstes (s. o.) kann vorgegeben werden, dass die Abonnenten des Dienstes vom Dienstanbieter automatisch dezentralen Support erhalten. Dies erfolgt jedoch rein aus Komfortgründen und kann jederzeit vom Benutzer deaktiviert werden.

Auditing

Gerade durch das Konzept des dezentralen Supports kann es für den Benutzer schnell unübersichtlich werden, welche Person zu welchem Zeitpunkt seine Identitätsdaten lesen konnte oder geändert hat. Daher unterstützt das Paderborner IMS ein umfangreiches Auditing. Prinzipiell kann dabei jede Änderung an jedem Attribut protokolliert und vom Benutzer über das Self-Care-Interface eingesehen werden. Aus Gründen der Übersichtlichkeit werden zurzeit lediglich die folgenden Aktionen (incl. Datum, Zeit, IP-Adresse) protokolliert:

- Support-Vorgänge an sich (d. h. die Tatsache, dass überhaupt ein Administrator auf die Identität lesend oder schreibend zugegriffen hat)
- Passwortänderungen
- Beantragungen und Kündigungen von Diensten
- Aktivierungen und Deaktivierungen von dezentralem Support
- Änderungen der MAC-Adresse für den Dienst „WLAN-Nutzung"

Einsatz und Ausblick

Nach einer Migrationsphase, in der die vorhandenen Benutzerbestände unterschiedlicher Bereiche konsolidiert wurden, ist das auf Basis von Open-Source-Produkten (Apache, OpenLDAP, Perl) realisierte System seit zwei Jahren mit inzwischen über 13.000 Nutzern im Produktionsbetrieb. Jetzt können erstmalig beliebige Personen (Studierende, Personal, Gäste) über *einen* Accountnamen eindeutig identifiziert, adressiert (E-Mail), authentisiert (mittels LDAP oder Kerberos) und autorisiert (Rechtevergabe) werden. Durch dokumentierte Zugriffsrechte, die zentrale Sperrmöglichkeit und Löschung von Identitäten hat sich die Sicherheit der IT-Infrastruktur erhöht.

Für die Nutzer ergeben sich neben der Steuerung der Aktivierung und des Matchings ihrer Identitäten eine höhere Transparenz bzgl. der Datenflüsse und eine zentrale Revisionsfähigkeit, allerdings erfordern das Verständnis über die Möglichkeiten und der Umgang mit dem System von den Nutzern zusätzliche Kompetenzen, die bei den Betreibern in zusätzlichen Beratungs- und Schulungsaufwand münden.

Zur Zeit wird der mögliche Einsatz des Tivoli-Identity-Managers (TIM) von IBM evaluiert. Geplant ist ferner die Anbindung weiterer Dienste, z.B. der Bibliotheksnutzung und eines Online-Adressbuches der Hochschule.

Literaturverzeichnis

[Des02] Dessler, H.: Datenschutzrechtliche Aspekte von Informations- und Verzeichnisdiensten. In: Knop, J. v., Bode, F. (Hrsg.): *Tagungsband über die Informations- und Verzeichnisdienste in Hochschulen*. Düsseldorf: Heinrich-Heine-Universität 2002, S. 11–15

[HKRG03] Hansen, M., Krasemann, H., Rost, M., Genghini, R.: Datenschutzaspekte von Identitätsmanagementsystemen. *DuD – Datenschutz und Datensicherheit* 27(9), 551–555 (2003)

[Ho97] Holl, F.-L.: *Das Konzept der Ordnungsmäßigkeit von Informations- und Kommunikationssystemen – Ein Beitrag zur konstruktiven Erschließung gesellschaftlicher Anforderungen in der Informatik.* HNI-Verlagsschriftenreihe, Bd. 12. Paderborn: Heinz Nixdorf Institut, Universität-GH Paderborn 1997

[KO03] Klapper, F., Oevel, G.: Serviceorientierte Infrastruktur an der Universität Bielefeld und der Universität Paderborn – ausgewählte Ziele und Konzepte. In: Bode, F., Lix, B., Weckmann, H. D. (Hrsg.): *Tagungsband Serviceorientierte Infrastrukturen an Hochschulen*. Universität Duisburg-Essen 2003, S. 40–50

[KP01] Köhntopp, M., Pfitzmann, A.: Informationelle Selbstbestimmung durch Identitätsmanagement. *Informationstechnik und Technische Informatik* 42(5), 227–235 (2001)

[Koe05] König, J.: *Konzept eines LDAP-gestützten integrierten Identitäts-Managements für dienstebasierte Infrastrukturen am Beispiel der Universität Paderborn*. Diplomarbeit, Universität Paderborn 2005

[Mo05] Moog, H.: *IT-Dienste an Universitäten und Fachhochschulen – Reorganisation und Ressourcenplanung der hochschulweiten IT-Versorgung.* Hochschulplanung Band 178. Hannover: HIS Hochschul-Informations-System GmbH 2005