

Mit einem HU-Account viele Dienste nutzen

Ansätze für ein universitätseinheitliches Identitätsmanagement

Doris Natusch
natusch@cms.hu-berlin.de

Vorbemerkungen

Der Artikel wendet sich hauptsächlich an Entscheidungsträger, die sich mit der Frage auseinandersetzen müssen, wie viel ihnen der Aufbau eines universitätseinheitlichen Identitätsmanagements wert ist, und versucht herauszufinden, welche Chancen und Möglichkeiten mit einem einheitlichen Identitätsmanagement verbunden sind. Ein Großteil der nachfolgenden Gedanken entstand in einer durch die Steuerungsgruppe »Verwaltungsnetz«¹ initiierten Arbeitsgruppe (IdM-AG), die das Identitätsmanagement zunächst bezogen auf das Personal diskutiert hat. In einem zweiten Schritt sollen die gewonnenen Erfahrungen auch bei der Diskussion des universitätsübergreifenden, also die Studierenden mit einbeziehenden Identitätsmanagements genutzt werden. In der IdM-AG waren der Behördliche Datenschutzbeauftragte, der Personalrat, die Abteilung für Personal und Personalentwicklung und der Computer- und Medienservice vertreten. Die Überlegungen der Arbeitsgruppe mündeten in eine Vorlage, die in der Steuerungsgruppe ausführlich diskutiert und in der im Beschlussentwurf die Einleitung weiterer Verfahrensschritte durch das Präsidium empfohlen wurde.

Einordnung

Unter Identitätsmanagement versteht man die Festlegung und computergestützte Verwaltung und Prüfung von Rollen, in denen Personen – an der Universität sind dies vor allem Lehrende, Forschende, Studierende und Verwal-

tungspersonal – bestimmte Informationen und Dienstleistungen benutzen dürfen. Neben dieser eher technisch geprägten Definition hat Identitätsmanagement auch eine wesentliche Datenschutzkomponente. Ein Benutzer wird mit Hilfe von Identitätsmanagement in die Lage versetzt, persönliche Merkmale nur gezielt und bewusst weiterzugeben. Identitätsmanagement dient also dem Schutz personenbezogener Daten. Im Folgenden soll auf zwei Fragen etwas näher eingegangen werden:

- In welchen Verwaltungsprozessen spielt Identitätsmanagement eine Rolle?
- Was gehört zum Identitätsmanagement?

Die erste Frage könnte man relativ schnell beantworten, indem man feststellt, dass Identitätsmanagement in nahezu allen Verwaltungsprozessen vorkommt. Beispielhaft soll dies anhand der Verwaltungsprozesse, bezogen auf Mitarbeiter, (siehe Abb. 1) dargelegt werden.

Bei der Beantwortung der zweiten Frage sollte man sich vorerst mit einem Auszug aus der Begriffswelt des Identitätsmanagements zufrieden geben, der einen Einblick in die Größenordnung der einzubindenden organisatorischen und

Der Artikel beschreibt erste Überlegungen an der HU zum Aufbau eines universitätseinheitlichen Identitätsmanagements, geht auf den gegenwärtigen Stand ein und legt Argumente dar, die – trotz des hohen organisatorischen und technologischen Aufwandes – dafür sprechen, sich einer derartigen Aufgabe zu stellen.

¹ Die Steuerungsgruppe »Verwaltungsnetz« wurde im Jahre 1994 gegründet und übernimmt seitdem die Aufgaben der Ziel- und Prioritätensetzung in allen IT-Belangen der Verwaltung. Die Steuerungsgruppe wurde durch das Präsidium ausdrücklich autorisiert, ressortübergreifende Entscheidungen in der Frage der IT-Unterstützung in der Verwaltung zu treffen und deren Umsetzung zu veranlassen. Die Steuerungsgruppe wird durch den Vizepräsidenten für Haushalt, Personal und Technik geleitet.

Mitarbeiter und Identitätsmanagement:

- Einstellung
- Beantragung einer Telefonnummer
- Beantragung oder Aktivierung eines Accounts, eines Zuganges zum Mail- und/oder Kalendersystem
- Aufnahme in eine Mailingliste, in ein Informationssystem (z. B. HU-ZIS)
- Namenswechsel
- Teilnahme an einem Kursmanagementsystem (wie z. B. Moodle)
- Übernahme einer neuen Funktion
- Benutzung einer Bibliothek
- Gehaltszahlung
- Durchführung von Veranstaltungen
- Vorlesungen (Aufnahme in das Vorlesungsverzeichnis)
- Durchführung von Forschungsprojekten (Aufnahme in die Forschungsdatenbank)
- Wohnungswechsel
- Wechsel des Büroraumes, der Telefonnummer
- Änderung des Arbeitsvertrages
- Beendigung des Arbeitsverhältnisses

Abb. 1: Beispiele für Verwaltungsprozesse, bei denen Identitätsmanagement eine Rolle spielt

technologischen Prozesse gibt (siehe Abb. 2).

Die Herausforderung beim Aufbau eines universitätseinheitlichen Identitätsmanagements wird nun darin bestehen, ausgehend von einer fundierten Ist-Analyse der bereits vorhandenen Systeme die Architektur des Gesamtsystems zu umreißen und beherrschbare Teilaufgaben, die man etappenweise angehen kann, zu definieren. Nach ersten Schätzungen wird mit einem Zeitrahmen von ca. 5 Jahren gerechnet, bevor das Gesamtsystem zur vollen Wirkung gelangen kann. Das geplante Vorhaben übertrifft an Komplexität und Aufwand nahezu alle bisherigen Aufgaben. Man könnte es fast mit einer Herztransplantation vergleichen. Neben dem Austausch des Kerns bzw. – um beim Vergleich zu bleiben – des Herzens, sind Änderungen und Anpassungen an fast jedem System zu leisten.

Vision

Wie sähe nun das zur vollen Wirkung gelangte universitätseinheitliche Identitätsmanagement an der HU aus? Stellen Sie sich vor, Sie treten Ihre erste Arbeitsstelle in einem wissenschaftlichen Institut an der HU an und erhalten bei der

Begriffswelt Identitätsmanagement:

- Passwortverwaltung und –synchronisierung
- Identitätszertifizierung mit Public-Key-Infrastrukturen
- Externe Identitätsdienste (MS Passport)
- Single Sign On- bzw. Unified-Messaging-Mechanismen
- Rollenkonzepte und Berechtigungen
- Verwaltung des Zugriffs auf Ressourcen (Daten, Drucker, Kopierer ...)
- Authentifizierung und Autorisierung
- Verwendung von Verzeichnisdiensten zur Speicherung von Identitätsinformationen, Passwörtern, Zertifikaten, Rollen, Berechtigungen, Systemrichtlinien
- Einsatz von Metadirectories zur Synchronisierung verschiedener Datenspeicher und Vermeidung von Inkonsistenzen
- Einsatz von Provisioning-Systemen zur Verwaltung von Berechtigungen und Versorgung von Anwendungen mit Identitätsinformationen

Abb. 2: Was gehört zum Identitätsmanagement?

Unterschrift Ihres Arbeitsvertrages in der Personalabteilung einen verschlossenen Briefumschlag mit Ihrem HU-Account und Ihrem Anfangspasswort. Sie gehen dann an Ihren neuen Arbeitsplatz, schalten Ihren Computer ein und klicken die Homepage der HU an. Das Layout der HU-Homepage nur unwesentlich geändert bzw. es ist nur ein kleines Login-Fenster hinzugekommen (siehe Abb. 3). Sie loggen sich also ein und sind

auf Ihrer persönlichen Seite, auf der die IT-Anwendungen und IT-Dienste angezeigt werden, die Sie sofort benutzen können. Sie ändern als Erstes Ihr Passwort und schauen sich dann in Ruhe um. Über einen Web-Mailer öffnen Sie Ihre Mailbox und lesen die ersten Rundmails Ihres Instituts und die News der Pressestelle. Sie stellen fest, dass Sie auch bereits Speicherplatz auf einem Netzlaufwerk benutzen können. Da Sie in Ihrem Institut Vorlesungen halten werden, ist für Sie bereits ein Zugang zum Kursmanagementsystem Moodle und zum elektronischen Vorlesungsverzeichnis eingerichtet worden. Neben Ihrer Lehrtätigkeit sollen Sie sich an einem gerade gestarteten Forschungsprojekt beteiligen, deshalb haben Sie ebenfalls einen Zugang zur Forschungsdatenbank der HU. Danach stellen Sie fest, dass man Ihre Adresse falsch geschrieben hat und Sie nutzen die Gelegenheit, die richtige einzugeben ...

Beim Lesen dieses realistischen Szenarios wird vielleicht etwas klarer, wie viele Dinge im Hintergrund organisiert und technisch gelöst sein müssen, damit alles so wie hier beschrieben funktioniert. Es wird auch deutlich, dass ein universitätsweites Identitätsmanagement eine sehr weitgehende praktische Bedeutung für jeden Einzelnen hat.



Abb. 3: HU-Homepage mit Login-Fenster

Realität

Um die Stellung der HU im Prozess des Identitätsmanagements zu bestimmen: Im Unterschied zu anderen großen Hochschulen, die keine zentrale Accountverwaltung haben und bei denen ca. 100 Mail-Server eine hochschulweite Kommunikation sehr erschweren, gibt es an der HU bereits Ansätze einer zentralen Accountverwaltung. So basieren bereits jetzt u. a. Wireless LAN, Compute- und Fileservices, das HU-weit genutzte Windowsnetzwerk sowie das zentrale Mailsystem auf einer zentralen Accountdatenbank. Die Anzahl der in den letzten Jahren eingeführten IT-Dienste und IT-Anwendungen und auch der Grad ihrer Verflechtung nehmen erheblich zu. Eine Reihe von ihnen wurde im Verlauf der letzten 15 Jahre mehr oder weniger parallel eingeführt. Das hatte zu früherer Zeit seine Berechtigung, weil die Verknüpfung der Daten nicht zu leisten und die Notwendigkeit verknüpfter Systeme im Detail nicht vorhersehbar war. Da heute nahezu sämtliche angebotenen IT-Dienste der Universität über eine IT-gestützte Benutzerverwaltung verfügen, ergeben sich die Möglichkeit und die Notwendigkeit, Verknüpfungen herbeizuführen, um den Service und die Aktualität zu verbessern sowie den Verwaltungsaufwand zu senken. Diese Herausforderung steht vor der Universität. Je früher man sich ihr stellt, desto leichter ist sie realisierbar und umso eher schafft man Möglichkeiten für weitere Entwicklungen.

Die gegenwärtige Situation soll beispielhaft aus Mitarbeitersicht verdeutlicht werden (siehe Abb. 4).

- Es gibt am Computer- und Medienservice (CMS) eine zentrale Accountverwaltung, die für die Benutzeranmeldung an verschiedenen Basisdiensten wie z. B. E-Mail, Wireless LAN, Compute-Service oder den Zugang zum Windowsnetz der HU genutzt wird. Die Accountdatenbank enthält nicht alle Benutzer der HU. So gibt es z. B. eigene Accountverwaltungen in der Informatik, Mathematik, Geschichte und an der Wirtschaftswissenschaftlichen Fakultät.
- Es gibt drei (Master)Identitätssysteme nebeneinander, zwischen denen teilweise Abgleiche bzw. Synchronisationen

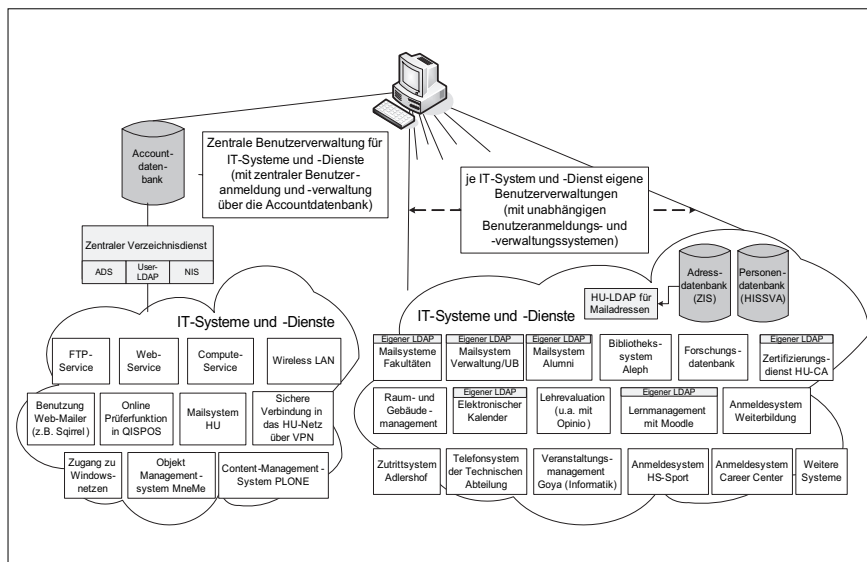


Abb. 4: Identitätsmanagement aus Mitarbeitersicht (heute).

erfolgen. Neben der zentralen Accountdatenbank existieren parallel Mitarbeiter- und Studierendendatenbanken (auf Basis von HIS-Software) sowie die zentrale Adressdatenbank mit den Dienstanschriften der Mitarbeiterinnen und Mitarbeiter.

- Es existiert eine Vielzahl autonomer IT-Systeme mit einem eigenen Benutzerverwaltungssystem, das von den Fakultäten und den Zentraleinrichtungen betreut wird.
- Verwaltungsmitarbeiter, die einen der zentralen Dienste des CMS (z. B. Wireless LAN, HU-Einwahl oder VPN) benutzen, benötigen neben ihrem Verwaltungsnetz-Account einen zweiten Account. Dies trifft übrigens auch für Fakultäten zu, die eine eigene Accountverwaltung haben.

Zielsetzungen und Chancen

Ein Kernziel des Vorhabens ist der Aufbau von universitätseinheitlichen sicheren Identitätsinfrastrukturen (s. Abb. 5). Dies bedeutet:

1. Die Nutzungsmöglichkeiten von IT-Services und Anwendungen an der HU sollen für Mitarbeiter, Gäste und Studierende deutlich verbessert und nahtloser gestaltet werden.
2. Es soll eine einheitliche zentrale Benutzerverwaltung aufgebaut werden, auf deren Grundlage jeder Benutzer ei-

nen zentralen Account erhält. Mit Hilfe dieses einen Accounts ist der Zugang zu den an der HU angebotenen Diensten möglich.

3. Die Identitätsinfrastruktur soll so flexibel gestaltet werden, dass auf organisatorische und auch auf technische Veränderungen schnell und mit geringem Ressourcenaufwand reagiert werden kann.
4. Bereits existierende IT-Dienste und IT-Anwendungen mit einer eigenen Benutzerverwaltung sollen etappenweise auf die zentrale Benutzerverwaltung umgestellt bzw. an diese angepasst werden.
5. Es soll das Grundprinzip gelten, möglichst wenig Rollen und Rechte zentral zu verwalten. Die spätere Möglichkeit eines Single Sign On oder Unified Login sollte dabei offen gehalten werden.
6. Die bereits an der HU aufgebaute Zertifizierungsinstanz (HU-CA) soll weiterentwickelt und in das einheitliche Identitätsmanagement integriert werden.
7. Es sollen die Grundlagen für ein hochschulübergreifendes Identitätsmanagement und damit die Möglichkeit, die IT-Dienste der HU auch externen Hochschulangehörigen anzubieten, geschaffen werden.

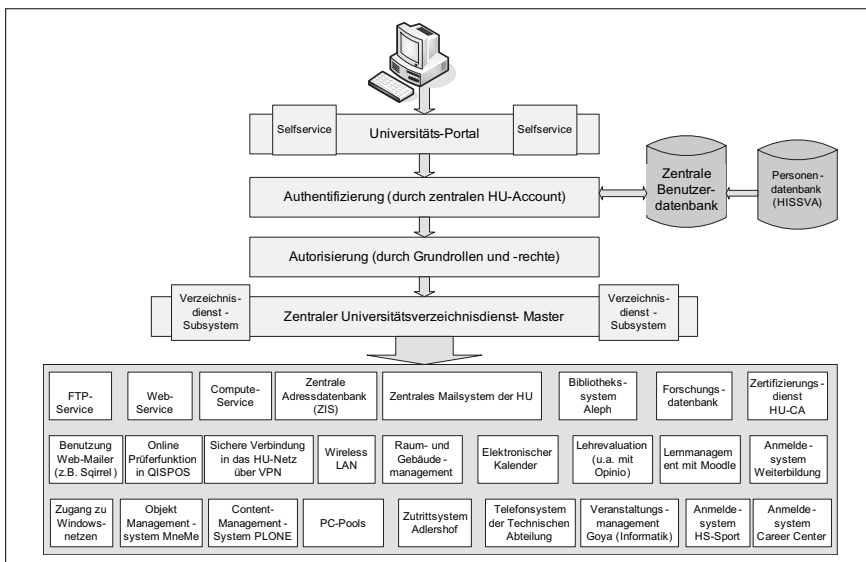


Abb. 5: Identitätsmanagement aus Mitarbeitersicht (zukünftig).

Für die HU eröffnen sich mit dem Aufbau von einheitlichen, sicheren Identitätsinfrastrukturen eine Reihe von Chancen und Möglichkeiten, auf die im Folgenden etwas näher eingegangen werden soll:

- Der Universität stehen aktuelle, konsistente und integre (Identitäts-)Daten für die IT-Anwendungen und IT-Service zur Verfügung.
- Durch Transparenz und Authentizität in den Rechtsregelungen besteht größere Klarheit bei der Aufgabenverteilung.
- Die Sicherheitsrisiken können z. B. durch rechtzeitiges Entziehen der Berechtigungen nach Verlassen der HU reduziert werden.
- Der Aufwand in den IT-betreuenden Bereichen der HU kann reduziert werden.

Um eventuelle Risiken des Aufbaus eines universitätseinheitlichen Identitätsmanagements zu minimieren, wird der gesamte Entwicklungs- und Einführungsprozess durch Dienstvereinbarungen begleitet.

Der Vorteil des Projektes liegt vor allem in der Einführung einer zukunftsweisenden Technologie, die die Anwendung weiterer Systeme mit deutlich geringerem Aufwand ermöglichen wird. Eine Reduzierung von Aufwand wird vor allem in folgenden Maßnahmen gesehen:

- **Rezentralisierung**
Die teilweise existierenden »Doppelangebote« an IT-Diensten werden auf einen Dienst zurückgeführt. Das betrifft u. a. Mailsysteme, Anmelde- und Speichersysteme.
- **Reduzierung der Administrortätigkeiten** in den IT-Diensten und IT-Anwendungen
Es wird eingeschätzt, dass sich der Anteil der Benutzerverwaltung an der Administrortätigkeit derzeit auf 10 bis 30% beläuft. Durch die Anbindung der IT-Systeme an ein zentrales Identitätsmanagement lässt sich dieser Anteil der Benutzerverwaltung auf etwa die Hälfte des Aufwandes senken.
- **Selfservice**
Weiterhin ist es künftig möglich, dass der Benutzer seine persönlichen Daten wie z. B. seine Adresse über eine Selfservice-Schnittstelle ändert. Damit wird zwar die Aufgabe nur »verlagert« und bringt für den Einzelnen einen geringen Mehraufwand, jedoch bei Systemen mit großen Benutzerzahlen eine hohe Einsparung an Verwaltungstätigkeit.

Das sind erste Schätzungen. Eine genauere Analyse der Aufwandsreduzierungen kann erst mit Hilfe einer Aufwands- und Nutzenanalyse erreicht werden.

Perspektive

Das Präsidium der HU hat in seiner Sitzung am 1. Dezember 2005 die Vorlage zum Aufbau eines universitätseinheitlichen Identitätsmanagements diskutiert, ihr rückhaltlos zugestimmt und die Einleitung weiterer Verfahrensschritte beschlossen. Neben der bereits erwähnten Aufwands- und Nutzensanalyse steht eine Fülle von Aufgaben an, die nur unter Einbeziehung aller Kräfte an der HU gemeistert werden kann. Wir werden Sie über den Stand der Dinge auf dem Laufenden halten.

Glossar

Um den Artikel abzurunden, noch einige Begriffe, über deren Inhalt sich die IdM-AG verständigt hat:

Rollen: Jede Person hat eine Identität.

Diese Identität beinhaltet Rollen, die diese Person einnimmt. Rollen können z. B. sein: Mitarbeiter und Student bzw. Differenzierungen wie z. B. Wähler, Bearbeiter von Forschungsdaten, Dienstreisender usw.

Rechte: Den Rollen werden bestimmte Rechte zugeordnet: auf Daten, auf Anwendungen und auf Ressourcen.

Single Sign On (SSO): Es gibt verschiedene Ansätze, die Rechte den Rollen zuzuordnen. Beim Single Sign On loggt sich der Benutzer einmal z. B. auf einem Web-Portal ein und zentral im »Hintergrund« sind seine Rollen und Rechte definiert. Er kann die IT-Systeme nur nutzen, wenn sie auch freigeschaltet wurden.

Unified Login: Im Unterschied zum SSO wird bei jeder Anmeldung (Login) in einem IT-System bei einem zentralen Authentifizierungsdienst angefragt, ob die Person das System benutzen darf.

Zertifizierungsinstanz HU-CA: Innerhalb der Public Key Infrastruktur der HU ist die Zertifizierungsinstanz (Certification Authority=CA) die Stelle, die für die Überprüfung von Identitäten und die Erstellung von Zertifikaten zuständig ist. Ein Zertifikat ist der öffentliche Schlüssel einer Person, der durch die CA signiert und der Person zugeordnet wird.

Aus der Sicht eines Betroffenen

Dr. Reinhold Wulff, Nordeuropa-Institut

Als Vertreter des Personalrats habe ich in der AG »Identitätsmanagement« mitgearbeitet und eine meiner ersten Überlegungen war: Was bedeutet Identitätsmanagement eigentlich für mich als Nutzer? Ich erkannte schnell, dass eine rationellere Organisation der Zugänge zu den verschiedenen von mir genutzten Diensten sehr vorteilhaft wäre. Zunächst einmal sitze ich regelmäßig an vier verschiedenen Computern an meinen unterschiedlichen Arbeitsplätzen: Im Nordeuropa-Institut, im Personalratsbüro, Zuhause. Hinzu kommt das Notebook, das ich insbesondere für die Lehre einsetze. Bei allen vier muss ich mich zunächst bei Windows anmelden – aus Bequemlichkeit nutze ich an allen vier Rechnern dasselbe Passwort – nicht sehr klug, ich weiß. Noch leichtsinniger verfare ich, weil ich fast überall den Passwortmanager von Mozilla, Firefox bzw. Thunderbird benutze, um mir nicht jede Benutzererkennung und jeden Zugangscode merken zu müssen. Denn im Laufe eines Arbeitstages kommen viele solcher Kombinationen auf mich zu: Ich muss mich für mein E-Mail-Konto anmelden und der Institutsserver verlangt meinen autorisierten Zugang, wenn ich auf die dort ausgelagerten Dateien zugreifen will. Jetzt erst kann ich am PC zu arbeiten beginnen. Bald aber wird erneut nach meinen Zugangsdaten

gefragt: Ich will im UB-Katalog suchen – ein neuer Benutzername, ein neues Passwort. Ich möchte meine Online-Materialien für den Unterricht ergänzen: Anmelden, Passwort. Als Erasmus-Beauftragter frage ich unsere Mail ab: Anmelden, Passwort. Dasselbe gilt, wenn ich die Mail für die von mir mitherausgegebenen Zeitschrift lesen möchte. Neuer Account-Name, anderes Passwort. Meine Angaben in der Expertendatenbank ergänzen? Anmelden, auf das generierte Passwort warten. Die Mailingliste für meine Übung ergänzen? Das Notebook im WLAN anmelden? Den Berlin-Brandenburger Gesamtkatalog befragen? Von außerhalb meine E-Mails lesen? Den Alumnis des Nordeuropa-Instituts eine E-Mail senden? Immer wieder: Benutzername (meist unterschiedliche) und Passwort. Und da ich noch viele halb dienstliche, halb oder ganz private Mailinglisten und News-Konten, Internetshops und personalisierte Suchmaschinen nutze, müsste ich über ein Elefantengedächtnis verfügen, um alle Zugangsdaten immer im Kopf zu haben. Deshalb leistet für mich meist der Rechner diese Gedächtnisarbit – bzw. ich beschränke mich auf wenige Kennwörter für die wichtigsten Dienste. Beides aber ist riskant – denn eines meiner Passwörter entschlüsselt, bietet ggf. den Zugang zu vielen Diensten. Und wer sagt

denn, dass der Passwortspeicher von z. B. Firefox nicht zu öffnen ist? Der Rechner aus dem Personalrat wurde gestohlen – da hatte der Dieb eventuell genug Zeit, sich ans Knacken der Verschlüsselung zu machen (lohnt aber nicht, da auf dem Rechner nichts Empfindliches abgelegt war ...). Meine Erkenntnis aus dieser Bestandsaufnahme? Mein durchaus risikobehafteter Umgang mit den Zugängen zu den von mir genutzten Internetdiensten könnte wesentlich bequemer und sicherer werden, wenn die Humboldt-Universität ihre bisher mehr oder weniger zusammenhanglosen Dienste bündeln und Zugänge zentraler gestalten könnte. Dann müsste ich mir nur zwei oder drei Zugangswörter merken, würde diese nicht mehr auf dem Rechner ablegen und hätte auf diesem schnelleren Weg trotzdem Zugang zu den auch bisher schon genutzten Angeboten. Bequemer, schneller und sicherer – vielleicht wird diese Vision in absehbarer Zeit in Erfüllung gehen können. Eine entsprechende Initiative hat die AG »Identitätsmanagement« dem Präsidium zur Umsetzung vorgelegt. Ich hoffe sehr, dass die benötigten Sach- und Personalmittel für Bestandsaufnahme, Perspektivenentwicklung und Umsetzung zur Verfügung stehen werden.