Identity Management – Prozessintegration als Schlüssel zum Erfolg

Bernd Hohgräfe

Siemens AG
Kruppstraße 16, 45128 Essen
bernd.hohgraefe@siemens.com

1 Motivation

Identity Management ist eine notwendige Voraussetzung für jede Art von E-Business – auch im universitären Umfeld. Diese These mag auf den ersten Blick überraschen, ist aber im aktuellen Kontext zunehmender Privatisierung der Hochschulen zu sehen. Studierende sind immer mehr als Kunden zu betrachten, der Einschreibe- bzw. Rückmeldevorgang dementsprechend als die Bestellung einer von der Hochschule zu erbringenden kostenpflichtigen Leistung. Als zahlender Kunde erwartet der Studierende dann einen entsprechenden Gegenwert, nicht nur im Hinblick auf die Qualität der Lehre, sondern auch auf die schnelle Bereitstellung der für sein Studium notwendigen Infrastruktur wie Studierendenausweis, Benutzerkonten, Zugangsberechtigungen, Bibliotheks- und Mediennutzung sowie entsprechende Support- und Servicelevel. Eine solche Erwartungshaltung der Studierenden ist in den USA, nicht zuletzt aufgrund der hohen Kosten eines Studiums, bereits üblich und wird sich auch in Deutschland mit der Einführung von Studiengebühren verbreiten. Identity Management kann hier einen deutlichen Beitrag zur Optimierung der entsprechenden hochschulinternen Prozesse im Hinblick auf Zeit und Kosten leisten.

2 Entwicklung vom Meta Directory zum Identity Management

„A set of processes and a supporting infrastructure for the creation, maintenance, and use of digital identity“ – so definiert die Burton Group Identity Management. Es handelt sich dabei um die konsequente Weiterentwicklung der Lösungen, die vor vielen Jahren zuerst als Verzeichnisdienst (Directory Service) eingeführt, dann zu sogenannten Meta Directory Lösungen erweitert wurden und heute Benutzerverwaltung (User Management), Rollen- und Berechtigungsverwaltung sowie Provisionierung (Provisioning) umfassen.

Während ein Verzeichnisdienst anfänglich als reines Auskunftssystem für Identitäten der angeschlossenen Systeme diente und damit eine eher passive Funktion hatte, entstand schon bald die Notwendigkeit, die in jeder Organisation existierenden verschiedenen Verzeichnisse und Datenbanken miteinander abzugleichen.

Reine Meta Directory Lösungen stellen die Konsistenz und Aktualität der personenbezogenen Daten in allen angeschlossenen Systemen sicher, gleichen jedoch nur einzelne Attribute ab, ohne Einträge aktiv anzulegen. Bei den angeschlossenen Systemen handelt es sich typischerweise um Datenhaltung und Benutzerverwaltung von Betriebssystemen,

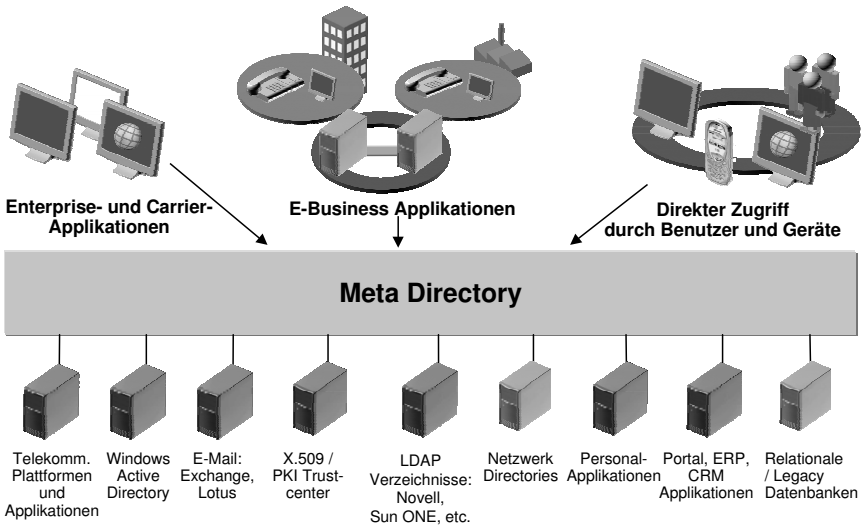

Abbildung 1: Ein Meta Directory dient als Informationsdrehscheibe

Mailservern, Telekommunikationsanlagen, Portallösungen und verschiedenen Applikationen. Bei einer solchen Meta Directory Lösung wird die Benutzerverwaltung weiterhin von den einzelnen Systemen bzw. Applikationen übernommen.

Dem gegenüber erfolgt bei einer Identity Management Lösung die Benutzerverwaltung zentral für alle angeschlossenen Systeme, wobei eines der angeschlossenen Systeme – wie das Hochschul-Informationssystem HIS – durchaus die Quelle für einen neuen Benutzer sein kann. Im Rahmen der Benutzerverwaltung werden für einzelne Benutzer und Gruppen dann die notwendigen Berechtigungen vergeben. Jeder Berechtigung sind entsprechende Benutzerkonten und Gruppenzugehörigkeiten in den angeschlossenen Systemen sowie evtl. notwendige Geräte (Assets) zugeordnet. Das automatisierte Anlegen und Löschen dieser Benutzerkonten, die Zuordnung zu den korrekten Gruppen in den jeweiligen Zielsystemen sowie die Auslösung von Bestellvorgängen wird als Provisionierung bezeichnet.

3 Mehrwert durch den Einsatz von Rollen

Berechtigungen werden zunehmend nicht mehr direkt, sondern indirekt über Rollen vergeben. Dieses sogenannte Role Based Access Management (RBAM) ist inzwischen standardisiert und hat zwei wesentliche Vorteile: Zum einen kann einer Rolle eine Menge einzelner Berechtigungen zugeordnet sein, so dass Benutzern beim Anlegen nur noch eine Rolle statt vieler einzelner Berechtigungen zugewiesen werden muss. Zum anderen können die einer Rolle zugeordneten Berechtigungen bei Bedarf einfach angepasst werden und gelten damit automatisch für alle Inhaber dieser Rolle.

Rollen können darüber hinaus auch automatisiert aufgrund von sogenannten Policies vergeben werden. Dabei können Personen, die eine bestimmte Rolle innehaben, in Abhän-

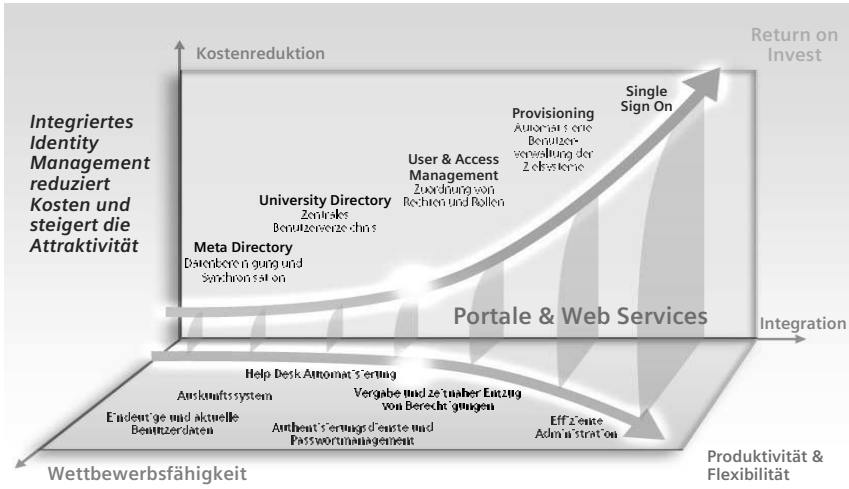

Abbildung 2: Eine Identity Management Lösung hat viele Nutzendimensionen

gigkeit von bestimmten Rollenparametern, wie beispielsweise Funktion, Fachbereich und Standort, unterschiedliche Berechtigungen zugeordnet werden. So ergeben sich für einen Dekan je nach Fachbereich unterschiedliche spezifische Berechtigungen. Damit wird die Benutzerverwaltung deutlich vereinfacht und beschleunigt.

Innerhalb einer Hochschule können einem Studierenden durchaus mehrere Rollen gleichzeitig zugeordnet sein, z. B. als Studierender, studentische Hilfskraft und in der studentischen Selbstverwaltung. Im Zeitverlauf können einzelne Rollen hinzukommen oder entfallen. Dabei ist insbesondere die Bedeutung des automatisierten Entzugs von Rollen und/oder Berechtigungen unter Sicherheitsaspekten nicht hoch genug einzuschätzen. So kann einem Studierenden bei der Exmatrikulation automatisch die Rolle Studierender entzogen und die Rolle Alumnus zugewiesen werden. Es ist denkbar, dass er als Alumnus seine E-Mail-Adresse behält, aber seine Berechtigungen entsprechend angepasst werden. Damit können Sicherheitsrisiken durch unberechtigten Zugriff ehemaliger Studierender vermieden werden.

4 Access Management als sinnvolle Ergänzung

Wenn Benutzer, Rollen und Berechtigungen an der Hochschule erst einmal zentral verwaltet und vergeben werden, macht es Sinn, auch den Zugang zu bzw. Zugriff auf Ressourcen zentral zu überwachen. Ressourcen können dabei Arbeitsplatzrechner, Betriebssysteme, Portale, Applikationen, Datenbestände und Datenbanken sein. Dabei sind die folgenden Aspekte von Bedeutung:

- **Authentifizierung** Benutzer müssen eindeutig identifiziert werden. Elektronische Identitäten müssen sicher und zweifelsfrei validiert werden. Dies ist die Voraussetzung für die korrekte Autorisierung. Hier können neben Login und Passwort auch

Chipkarten oder biometrische Verfahren zum Einsatz kommen, um eine möglichst starke Authentifizierung zu erreichen.

- **Autorisierung** Der Zugriff auf geschützte Ressourcen muss gemäß der Sicherheits-Richtlinie (Rollen- und Berechtigungskonzept) überprüft werden. Dabei dürfen nur berechtigte Zugriffe zugelassen werden. Die Rechtmäßigkeit eines Zugriffs kann dabei von weiteren Parametern wie Zugriffsort und -zeit abhängen.
- **Auditing** Alle Aktivitäten im Zusammenhang mit Benutzerzugriffen müssen gespeichert, überwacht und für regulative Anforderungen zugreifbar sein. Dies ist insbesondere für alle finanziellen und prüfungsbezogenen Transaktionen unabdingbar, um auch später noch entsprechende Nachweise erbringen zu können.
- **Accounting** Abrechnungsrelevante Daten müssen benutzerbezogen gespeichert und für Abrechnungszwecke verfügbar sein. Die Granularität der Erfassung hängt davon ab, ob und wie IT-Leistungen an der Hochschule verrechnet werden. Identity und Access Management schaffen hier die Voraussetzung für zukünftige nutzungsbezogene Verrechnungsmodelle.

5 Verwaltungsprozesse für Studierende und Verwaltung

Die heutigen Prozesse im Hochschulbereich sind historisch gewachsen und orientieren sich vielfach noch an papierbasierten Abläufen. So ist es nach wie vor üblich, dass ein neuer Studierender sich zuerst im Studierendensekretariat immatrikuliert, dann in der Bibliothek einen Benutzerausweis beantragt (und später abholen muss), danach im Hochschulrechenzentrum ein Benutzerkonto erhält und im weiteren Verlauf seines Studiums immer wieder persönlich zur Belegung von Veranstaltungen und Anmeldung zu Prüfungen in der Verwaltung erscheinen muss. Neben der mehrfachen manuellen und redundanten Datenerfassung, dem hohen, wenngleich verteilten Administrationsaufwand und mangelnder Transparenz bei den vergebenen Berechtigungen hat dies auch für den Studierenden spürbare Nachteile, da er verschiedene Verwaltungsstellen aufsuchen und mehrfach Wartezeiten in Kauf nehmen muss.

Dass es anders gehen kann, zeigen Beispiele aus der Wirtschaft, die zunehmend auch in modernen Verwaltungen eingeführt werden. Das o. g. Beispiel der Immatrikulation eines neuen Studierenden könnte damit auch folgendermaßen ablaufen:

1. Der neue Studierende immatrikuliert sich (nach wie vor persönlich, aber auch dies mag mit der Einführung digitaler Signaturen in einigen Jahren obsolet sein) im Studierendensekretariat. Dort wird er als neuer Studierender mit seinen Stammdaten im Hochschul-Informationssystem HIS angelegt und dann über die Verbindung zu HIS im Identity Management System automatisch ein Verzeichniseintrag generiert.
2. Im nächsten Schritt werden ihm in der rollenbasierten Benutzerverwaltung aufgrund seiner Stammdaten (Standort, Fachbereich etc.) entsprechende Rollen zugewiesen. Dies kann ganz oder teilweise automatisiert, einschließlich entsprechender Freigabe- und Genehmigungsverfahren, und auch dezentral in den einzelnen Fachbereichen geschehen.

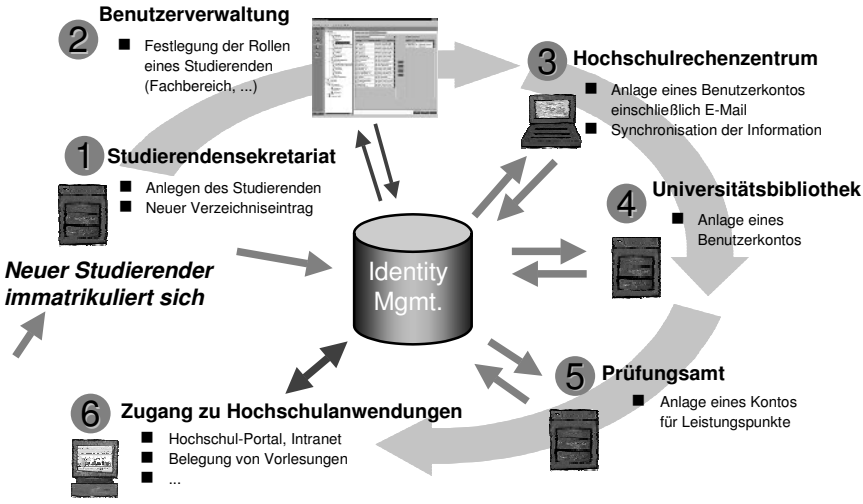

Abbildung 3: Optimierte Administrationsprozesse vereinfachen Verwaltung und Provisionierung

3. Danach wird vom Identity Management System für den Studierenden im Hochschulrechenzentrum automatisch ein Benutzerkonto angelegt und eine E-Mail-Adresse vergeben. Die Berechtigungen seines Benutzerkontos hängen dabei von den ihm zugewiesenen Rollen ab. Diese Informationen werden zurück in die Benutzerverwaltung synchronisiert und stehen damit allen angeschlossenen Systemen zur Verfügung.
4. Im Ausleihsystem der Universitätsbibliothek wird für den Studierenden automatisch ein Benutzerkonto mit entsprechenden Konditionen angelegt (abhängig von seiner Rolle, z. B. kostenpflichtig für Gasthörer). Die Bestätigung wird an seine aus Schritt 3 bekannte E-Mail-Adresse verschickt.
5. Dann wird im Prüfungsamt für den Studierenden automatisch ein Konto für seine Leistungspunkte angelegt. Der erste Kontoauszug wird an seine aus Schritt 3 bekannte E-Mail-Adresse verschickt.
6. Abhängig von den zugewiesenen Rollen kann der Studierende sofort das Hochschul-Portal nutzen, online Veranstaltungen belegen, sich zu Prüfungen anmelden, Ergebnisse einsehen und weitere Services der Hochschule nutzen.

Über die Immatrikulation hinaus gibt es weitere Beispiele für automatisierbare Prozesse im universitären Alltag, von denen hier nur eine Auswahl aufgeführt ist:

- Bezahlung von Studiengebühren, Kopieraufträgen und Mensaessen
- Rückmeldung für ein Semester und die entsprechenden Wahlfächer
- Online-Reservierung von Büchern
- Elektronische Signatur und Abgabe von Semesterarbeiten
- Online-Anmeldung zu Prüfungen und Abfrage von Ergebnissen
- Fernzugriff auf zentral gespeicherte Vorlesungsunterlagen
- Verschlüsselter Datenaustausch bei externen Studienarbeiten
- Nutzung von Tele-Learning

6 Identity und Access Management als Infrastrukturkomponenten

Allen gemeinsam ist, dass die erforderliche Technik und benötigten Produkte zur Umsetzung bereits zur Verfügung stehen. So sind elektronische Geldbörsen – in Form der Geldkarte oder als Fahrausweis mit integriertem Chip für den ÖPNV – bereits im Einsatz. In großen Unternehmen wie der Siemens AG erfolgt die Ausleihe von Medien bereits elektronisch, Verpflichtungserklärungen werden digital signiert, Belegschaftsaktien online bestellt und Gehaltsabrechnungen elektronisch verschlüsselt verteilt, und vom Arbeitsplatz beim Kunden oder zuhause greifen Mitarbeiter über ein Virtual Private Network auf das Siemens Intranet zu. Die Herausforderung besteht nun im universitären Umfeld – genau wie in der Wirtschaft – darin, diese Prozesse im Gesamtzusammenhang zu sehen und Synergien bzgl. der bereitzustellenden Infrastruktur zu erkennen. Identity und Access Management sind dabei – genau wie Public Key Infrastrukturen (PKI) und Chipkarten – Infrastrukturkomponenten, die sich um so eher amortisieren, je mehr Anwendungen und Prozesse sie nutzen. Ihr Einsatz ist heute weniger eine technische als vielmehr eine organisatorische Frage.

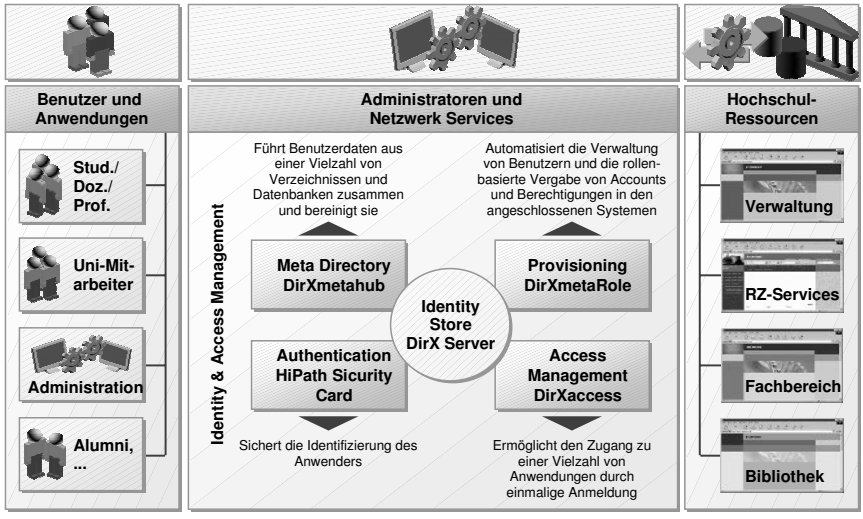

Abbildung 4: Module des Siemens Identity und Access Management bilden eine integrierte Lösung

Als Beispiel für eine solche Infrastruktur sei hier stellvertretend die Architektur der Siemens Identity und Access Management Lösung beschrieben. Als gemeinsame Datenablage für Identitäts- und Konfigurationsdaten wird der bewährte, X.500 und LDAP konforme Directory Server DirX verwendet. Er dient als zentrale Informationsdrehscheibe für die anderen Komponenten der Produktfamilie DirX Solutions:

- DirXmetahub führt Benutzerdaten aus einer Vielzahl von Verzeichnissen und Datenbanken zusammen und bereinigt sie.

- DirXmetaRole automatisiert die Verwaltung von Benutzern und die rollenbasierte Vergabe von Benutzerkonten und Berechtigungen in den angeschlossenen Systemen.
- DirX Access ermöglicht den Zugang zu einer Vielzahl von Anwendungen durch einmalige Anmeldung (Single Sign On).

Ergänzend können Siemens Chipkartenlösungen zur sicheren Identifizierung von Anwendern eingesetzt werden.

Identity und Access Management Lösungen müssen über die Verwaltung von Benutzerkonten für lokale menschliche Nutzer hinaus noch zwei weitere Gruppen von Benutzern abbilden:

- „Maschinelle Nutzer“, sogenannte Funktions-Accounts, die in der Praxis von Anwendungsprogrammen zu vielfältigen Zwecken genutzt werden. Der Zugriff erfolgt heute i. d. R. über Web Services.
- Entfernte Benutzer, z. B. Studierende anderer Hochschulen. Statt diese Benutzer zusätzlich (und redundant) lokal zu pflegen, kommt hier das Konzept der „Federated Identity“ zum Einsatz, bei dem einem nicht lokalen Benutzer – aufgrund einer vorab vereinbarten Vertrauensbeziehung mit seiner Organisation – entsprechende lokale Berechtigungen eingeräumt werden, ohne dass dieser Benutzer lokal verwaltet werden muss.

Beide Konzepte – Web Services und Federated Identity – sind noch relativ neu und daher noch nicht so weit verbreitet. Allerdings gilt auch hier bereits, dass die erforderliche Technik und benötigten Produkte zur Umsetzung bereits zur Verfügung stehen.

Nun kann es sich keine Hochschule leisten, Identity und/oder Access Management um ihrer Selbst willen einzuführen, sondern dies geschieht immer im Hinblick auf die damit verbundenen qualitativen und quantitativen Vorteile und den Nutzen für die Beteiligten. Für die Studierenden sind dies z. B.

- Einführung von Self Service Diensten,
- freier Zugriff auf Veranstaltungsunterlagen,
- Online-Belegung von Veranstaltungen und
- Einsicht in Prüfungsergebnisse.

Administratoren und Verwaltung profitieren u. a. von der

- Vermeidung redundanter Datenerfassung,
- Transparenz vergebener Berechtigungen,
- systemgestützten Administration und
- leichteren Integration neuer Dienste.

Die Hochschule insgesamt kann damit ihre Prozesse optimieren, standardisieren und dementsprechend günstiger realisieren. Dies gilt umso mehr, als nicht nur Personen, sondern auch Objekte wie Ressourcen (z. B. Hörsäle) und Assets (Fahrzeuge, Arbeitsplatzrechner, . . .) zunehmend mit einer Identität versehen und in Identity Management Systemen verwaltet werden können.

7 Projekte und Erfahrungen

An einer Reihe von Hochschulen und Universitäten in Deutschland sind inzwischen Projekte im Umfeld Identity und Access Management begonnen, an wenigen allerdings bisher abgeschlossen worden. Dabei kommen Produkte verschiedener Hersteller bzw. Open Source Software (openLDAP) zum Einsatz. Der Schwerpunkt der Projekte liegt bisher im Bereich Meta Directory und Identity Management, was sich auch aus den Anforderungen bzw. Zielen der Projekte ableitet. Unter den Anforderungen, die zur Etablierung eines Identity Management Projektes führten, finden sich z. B.:

- Optimierung der Administration und Kosteneinsparungen
- Automatisierte Benutzerverwaltung über bestehende Systemgrenzen hinaus
- Berechtigungsvergabe durch die Fachbereiche ohne detaillierte IT-Kenntnisse
- Einheitliche Benutzerverwaltung für verschiedene Benutzergruppen (Studierende, Lehrende, Wissenschaftliche Mitarbeiter, Verwaltungsmitarbeiter und externe Mitarbeiter)
- Prozessoptimierung im Hinblick auf eine zukünftig stärkere Integration der Telekommunikation in die IT-Umgebung durch Voice over IP

Abbildung 5: Erfahrungen der Universität Rostock

Mit der Einführung eines Identity Management Systems verfolgen die beteiligten Hochschulen und Universitäten u. a. die nachstehenden Ziele:

- Novellierung von Verwaltungsprozessen
- Reduzierung der Anzahl der verwendeten Anmeldeformulare
- Zentrale Benutzerverwaltung für Mitarbeiter und Studierende
- Vereinheitlichung der Namensgebung (Benutzerkonto, Mail-Adresse, etc.)

- Verbesserung der Konsistenz, Aktualität und Qualität der Benutzerdaten
- Abgleich der personenbezogenen Daten zwischen Mail- und Telefonsystemen, Personaldatenbanken, Directory Servern, SAP-Kostenstellen und Auskunftssystem
- Automatische Erstellung von Benutzerzertifikaten

Selbstverständlich variieren Anforderungen, Treiber und Ziele von Hochschule zu Hochschule, abhängig von der Zahl der Studierenden, der Anzahl und Heterogenität der eingesetzten Systeme, den bisherigen bzw. geplanten Prozessen, der finanziellen Ausstattung und nicht zuletzt auch der Innovationsfreudigkeit der beteiligten Organe. Wie der Erfahrungsbericht der Universität Rostock bestätigt, ist eine Identity Management Lösung damit immer auch eine hochschulindividuelle Lösung, die sorgfältige Planung und intensive Zusammenarbeit aller internen und externen Partner erfordert, dann aber auch positive Aspekte für alle Beteiligten mit sich bringt. Aus den bisherigen Rückmeldungen aus laufenden Hochschul-Projekten lässt sich jedenfalls entnehmen, dass sich die meisten erfreulich positiv entwickeln und damit ihren Beitrag zur Optimierung und Kundenorientierung der hochschulinternen Prozesse leisten.