

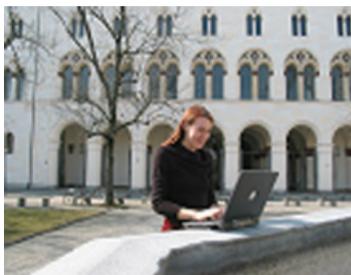
INFORMATIONEN- UND KOMMUNIKATIONSINFRASTRUKTUR

# Das Ende der Warteschlange – Identity Management an den Universitäten

DIE MÜNCHNER HOCHSCHULEN UND DAS LRZ STELLEN DEN STUDENTEN UND MITARBEITERN EINE VIELZAHL ELEKTRONISCHER DIENSTE ZUR VERFÜGUNG. FÜR DIE EFFEKTIVE VERWALTUNG DER DIENSTNUTZER UND IHRER BERECHTIGUNGEN ARBEITET DAS LRZ ENG MIT LMU UND TUM ZUSAMMEN, UM EIN HOCHSCHULÜBERGREIFENDES IDENTITY MANAGEMENT SYSTEM AUFZUBAUEN.

VON WOLFGANG  
HOMMEL

Traditionell wird neuen Studenten in den ersten Tagen ihres akademischen Lebens vor allem eines abverlangt: Geduld. Bis die Computerräume genutzt werden können, die E-Mail-Adresse eingerichtet ist, Online-Zugriff auf die Bibliothek von zu Hause aus möglich ist und die ersten Vorlesungsunterlagen aus dem E-Learning-System bezogen werden können, vergehen Tage oder gar Wochen. Für fast jeden Dienst muss man sich getrennt anmelden, also Schlange stehen, um Formblätter auszufüllen, die Nutzungsrichtlinien zu unterschreiben und Passworte abzuholen. Wer nach einigen Wochen umzieht, weil er mittlerweile doch noch eine bezahlbare Wohnung in Hochschulnähe gefunden hat, muss diese Adressänderung wiederum an vielen Stellen durchführen lassen.



Das Identity Management erleichtert den Studierenden den Zugang zu den Angeboten ihrer Hochschule.

## Qualität und Quantität

Das LRZ hat Benutzerkennungen an mehr als 60.000 Studenten vergeben; hinzu kommen die Kennungen für einen Großteil der Mitarbeiter der Münchner Hochschulen und solche für die Hochleistungsrechner des LRZ, die mittlerweile im Rahmen von Grid-Projekten europaweit genutzt werden. Eine manuelle Verwaltung aller Benutzer und ihrer Berechtigungen für die einzelnen Dienste und Systeme, wie sie derzeit noch an vielen Stellen praktiziert wird, droht die personellen Kapazitäten zu sprengen. Dadurch, dass dieselben Daten mehrfach erfasst werden, entstehen Inkonsistenzen, beispielsweise veraltete Anschriften oder Mobiltelefonnummern, so dass viele Benutzer in Problemfällen nur schwierig zu erreichen sind. Einigen Diensten wird sogar das Ausscheiden eines Mitarbeiters oder Studenten nicht zeitnah mitgeteilt, so dass diese Dienste zum Teil noch monatelang unberechtigt genutzt werden könnten.

Bei der Verwaltung der ständig zunehmenden Anzahl von IT-Diensten hat sich deshalb herauskristalliert, dass eine zentrale, in die vorhandenen Geschäftsprozesse nahtlos integrierte Benutzerverwaltung für

den effizienten Betrieb unabdingbar ist. Dadurch können auch die Dienstverantwortlichen von zeitfressenden Routinearbeiten wie dem Anlegen, Aktualisieren und Löschen von Kennungen entlastet werden.

## Identity Management

Die technische Umsetzung einer modernen, zentralen Benutzerverwaltung erfolgt über so genannte *Identity Management Systeme*. Der Begriff *Identity* bringt zum Ausdruck, dass ein Benutzer als Ganzes gesehen wird und nicht mehr wie bisher auf seine einzelnen Kennungen reduziert wird. Ein *Identity Management System* besteht aus einer zentralen Datenbank, in der die Kontaktdaten der Benutzer, ihre Kennung und ihre Berechtigungen hinterlegt werden. Diese zentrale Datenbank wird von den führenden Systemen, beispielsweise der Studenten- und Mitarbeiterverwaltung, direkt mit den relevanten Informationen gespeist und reflektiert damit jederzeit den offiziellen Datenbestand. Das *Identity Management System* übernimmt dann die Verteilung der jeweils benötigten Daten an die angeschlossenen Zielsysteme, beispielsweise die E-Mail-Server und das E-Learning-System. Scheidet ein Hochschulangehöriger

ger aus, werden die so angelegten Kennungen in den Zielsystemen auch wieder automatisch gelöscht.

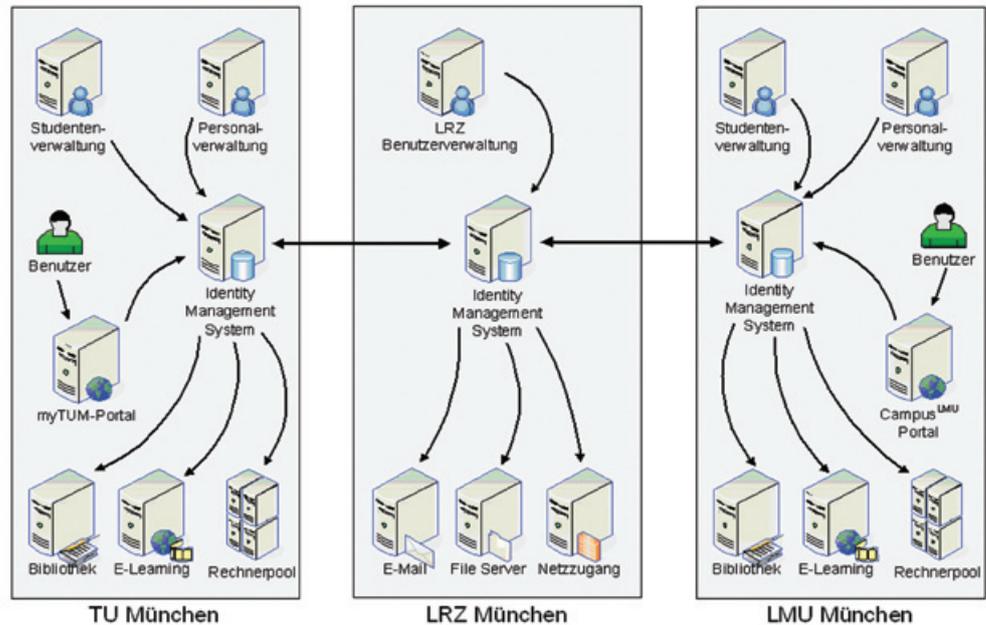
Als willkommener Nebeneffekt ergibt sich, dass jeder Benutzer nur noch eine Kennung für alle Dienste hat und sich damit nicht mehr viele verschiedene Kennungen und Passworte merken muss.

**Datenschutz**

Dadurch, dass die Vielzahl verschiedener Wege, auf denen Benutzerdaten bisher zwischen den einzelnen Stellen hochschulintern ausgetauscht wurden, beispielsweise bei der Anmeldung zu Praktika, über das Identity Management System vereinheitlicht werden, ergibt sich auch eine stärkere Betonung des Datenschutzes: An einer zentralen Stelle kann explizit definiert werden, wer auf welche personenbezogenen Daten Zugriff erhält. Die Datenflüsse können somit effizient überwacht, dokumentiert und im Rahmen der informationellen Selbstbestimmung zur Einsicht bereitgestellt werden. Statt des gläsernen Menschen wird somit vielmehr ein transparentes Verwaltungssystem geschaffen, von dessen Vorzügen sich die Hochschulangehörigen selbst überzeugen können.

**DFG-Förderung**

Die Ludwig-Maximilians-Universität (LMU), das LRZ und die Technische Universität München (TUM) haben in den letzten Jahren damit begonnen, *Identity Management Systeme* für ihre Dienste zu realisieren. An der LMU ist *Identity Management* ein zentraler Bestandteil von Campus<sup>LMU</sup> und bereits erfolgreich in Betrieb. Die TUM realisiert ihr *Identity Management* im Rahmen des DFG-geförderten Projekts IntegraTUM in enger Zusammenarbeit mit dem LRZ, das seine seit jeher zentrale Benutzer-



verwaltung derzeit ebenfalls auf zeitgemäße *Identity Management-Software* umstellt.

Dadurch, dass Dienste wie E-Mail, File Server, Backup und das Betreiben von Web-Servern zentral vom LRZ angeboten werden, ist eine Kopplung der drei *Identity Management Systeme* notwendig, wie aus Abbildung 1 ersichtlich.

Mittelfristig ist hier ferner eine direkte Anbindung an die Virtuelle Hochschule Bayern (VHB) geplant, die ihre An- und Rückmeldeverfahren derzeit ebenfalls auf solche Systeme umstellt.

**Nutzwert**

Durch diese Modernisierung wird sich der Ablauf der Immatrikulation neuer Studenten deutlich ändern: Nach der Bewerbung, die an der TUM auch online möglich sein wird, erhalten die zukünftigen Studenten bereits ihre Kennung, um damit an elektronischen Eignungsprüfungen und Vorkursen teilnehmen zu können. Mit der Immatrikulation werden die Kennungen termingerecht zum Semesteranfang

freigeschaltet und können vom ersten Tag an benutzt werden. Viele Verwaltungsangelegenheiten können über ein sicheres Web-Interface online durchgeführt werden. Änderungen, zum Beispiel von Anschrift oder Telefonnummer, müssen nur noch an dieser einen Stelle durchgeführt werden und werden automatisch an alle betroffenen Systeme propagiert. Diese moderne Informations- und Kommunikationsinfrastruktur erleichtert damit nicht nur den Betrieb der Dienste, sondern gestaltet die gesamte IT-Dienstlandschaft an den Münchner Universitäten benutzerfreundlicher und nahtloser.

Die vom LRZ im Rahmen von IntegraTUM gewonnenen Erfahrungen werden dazu genutzt werden, entsprechende Projekte mit den anderen Münchner Hochschulen durchzuführen.

*Der Autor ist Mitarbeiter des Leibniz-Rechenzentrums und für die Konzeption und Realisierung von Identity-Management-Lösungen an der TU München und am Leibniz-Rechenzentrum verantwortlich.*



**Abb. 1:** Datenflüsse mit Benutzerinformationen