



Virtuelle Universität durch Sicherheit und Personalisierung auf der Basis von Novell NDS eDirectory

Werner Degenhardt, Cristian Perez de Laborda

Universität München

Websites, auch universitäre Websites, unterscheiden sich in vielerlei Hinsicht. Der Grad der Personalisierung ist dabei eines der wichtigsten Unterscheidungsmerkmale und gleichzeitig eines, das mit den meisten Mühen verbunden ist.

Personalisierung ist nicht nur angenehm und vom Nutzer gewollt¹, sondern hat eine handfeste kommerzielle Basis: Personalisierte Websites haben eine durchweg bessere 'conversion rate' vom Besucher zum Kunden als nicht-personalisierte Websites.

Der wichtigste kommerzielle Grund für den Einsatz von Personalisierungsmechanismen in Websites ist die Hoffnung, damit langfristige Beziehungen zum Kunden aufbauen zu können.² In gewissen Sinne ist das die Hoffnung, mit den Mitteln des Internet wieder zu einer vor-industriellen Form der Beziehung zwischen Produzenten und Konsumenten zurückzufinden, ohne die Vorteile der Massenmedien aufgeben zu müssen. Virtuelle Universität ist in diesem Sinne nichts anderes als die Übertragung von Ideen und Mechanismen des E-Business auf akademische Lehr- und Forschungseinrichtungen.

Die Universität ist ja auch in einer ganz ähnlichen Situation wie Unternehmen im privaten Wirtschaftssektor. Den Kunden - den Studierenden und Mitarbeitern der Universität - werden vor-industriell (manchmal liebevoll, immer in Handarbeit) gefertigte Produkte im typischen anonymen Massenbetrieb des Industriezeitalters verkauft.

Wenn man so will, vereinigt das universitäre Ausbildungssystem heute die Nachteile zweier Epochen: vor-industriell unvollkommene Produkte werden in Massenabfertigung an eine weitgehend anonyme Kundschaft gebracht.³ Für die Beziehung Kunde-Dienstleister ist das ganze natürlich nicht förderlich. In Zeiten schwindender Mittel und wachsender Konkurrenz das Ruder herumzureissen ist ohne neue Ideen allerdings nicht trivial.

1 Internetportal der Universität München

Die Universität München verfolgt - wie viele andere Universitäten auch - die Idee, das Web als Plattform für die Verbesserung der oben geschilderten Situation zu nutzen. Eigene

¹ Bei Mobiltelefonen ist Personalisierung eines der wichtigsten Verkaufsargumente

² Siebel, Thomas M., House, Pat, „Cyber Rules. Strategies for Excelling at E-Business“, Doubleday 1999

³ Tsichritzis, Dennis, „Reengineering the University“, Communications of the ACM, 42 (6) pp 93-100, June, 1999





Untersuchungen legen wesentliche Faktoren nahe, die den Erfolg einer Initiative dieser Art wahrscheinlich werden lassen⁴

- Dezentralisierung der Arbeit
- Koordination der Prozesse
- Rezentralisierung der Technik

Dezentralisierung der Arbeit bedeutet, daß die organisatorischen Prozesse dort bleiben, wo sie am besten aufgehoben sind: Bei den Prozeßbeignern, die sich mit ihren Angelegenheiten auskennen.

Koordination der Prozesse bedeutet, daß die eingesetzte Internet-Technologie dazu benutzt wird, die dezentralen Prozesse zu koordinieren. Andernfalls bleibt alles so wie es ist und wird durch den Einsatz von Technologie nur noch komplizierter.⁵

Erfolgreicher Einsatz von Internet-Technologie dezentralisiert nur die Anwendungen und deren inhaltliche Pflege. Die Technik, auf der die Anwendungen basieren, wird rezentralisiert. Die Gründe dafür sind einfach: Die Prozeßkoordination ist unternehmenswichtig und darf nicht wegen mangelnder Uptime von technischen Komponenten fehlschlagen. Diese Entscheidung klingt zwar banal, ist in einer Universität von der Größe der LMU nicht leicht durchzusetzen.

Internet-Technologie wird damit als zentrale Plattform benutzt, auf der sich die Koordination von Menschen und Daten in der Universität abspielt.



Der Benutzer erlebt das ihm bereitgestellte Internet-Angebot einer Universität als geschützten persönlichen Kommunikationsraum, der ihm gleichzeitig einen vorher noch nicht dagewesenen personalisierten Mehrwert bietet, ohne den Aspekt der Sicherheit zu vernachlässigen.



Die Universität München will seinen Mitgliedern diesen Kommunikationsraum in der Form eines Internetportals zur Verfügung stellen, das den Wesenskern der Personalisierung erfüllt: Die richtige Person bekommt zur richtigen Zeit, ohne viel Aufwand das, was sie braucht: Seien es Informationen, Anwendungen (wie ein Programm zur Stundenplanoptimierung) oder Transaktionen (wie die Zulassung zum Studium).

2 LMU Corporate Directory

Die Voraussetzung für Personalisierung eines Internetportals ist ein Mechanismus, der Profile von Personen speichern kann, die Identität einer Person zur Laufzeit feststellt und auch weiß, welche Rechte auf Objekte des Internetportals mit einer bestimmten Person verbunden sind. Das ganze soll für den Benutzer transparent sein. Ein Anwender, der beispielsweise kein Recht hat, einen administrativen Bereich zu bedienen, soll die entsprechenden

⁴ Degenhardt, Werner, Meuser, Peter, „Intranet-Lösungen im Unternehmen. Benchmarking-Studie zum Einsatz von Intranet-Technologie und Intranet-Anwendungen im Unternehmen“, Siemens Unternehmenskommunikation, 1998

⁵ Malone, Thomas W. et al., „Tools for inventing organizations: Toward a handbook of organizational processes“, *Management Science* 45(3) pp 425-443, March, 1999



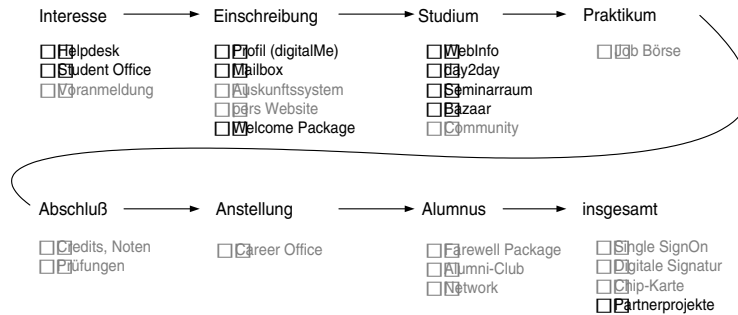


Abbildung 1. Das Internetportal der LMU begleitet die Studierenden solange sie etwas mit der Universität zu tun haben wollen

Links erst gar nicht sehen. Jeder bekommt also die auf seine Bedürfnisse und Rechte abgestimmte Website auf den Bildschirm.

Das Internetportal der LMU verwendet für diesen Zweck Novell's NDS eDirectory in der Version 8.5. Diese Version hat nur noch wenig mit dem Directory zu tun, das der Netzwerkadministrator aus der Administration des Netzwerkbetriebssystems Netware kennt.⁶

Das Directory, das den beschriebenen Zweck erfüllt, muß beliebigen Objekte, beliebige Attribute hinzufügen können und in der Lage sein, Rechte auf diese und sogar auf die Ebene von Attributswerten zu vergeben. Bei dem eigenen Personenobjekt, muß die dazugehörige Person bestimmen können, wer welche Werte von Attributen sehen, ändern oder löschen darf.

Im Corporate Directory der Universität München gibt es für die Speicherung der Personenprofile eine eigene spezielle Objektklasse, die nach und nach alle Attribute aufnimmt, die für die digitale Identität einer *lmuPerson* von Nöten sind.

Prinzipiell kann man in diesem Corporate Directory alles speichern, was an Informationen zu einer Person anfällt. Zum Beispiel kennt das Directory nicht nur alle Namensräume in denen eine Person bekannt ist, sondern auch seinen Verwendungszweck.

Allein was die Eigennamen von Personen anbelangt, gibt es viele Wahrheiten, die auch repräsentiert werden müssen. So kennt zum Beispiel das Standesamt (und die Bezirksfinanzdirektion) einen Franz Maria Hueber, der aber im Web als Freddy Huber gefunden werden will, in seinem Institut ist er der Franz. Als Komplikation kommt hinzu, daß der Nachname Hueber wie die amerikanische Schreibweise des Nachnamens aussieht, aber nicht ist. Bei der Rückübertragung des Nachnamens aus dem amerikanischen Sprachgebrauch, wird der Herr Hueber in der Regel zum Herrn Hüber.

Im Endeffekt hat jede Person eine Reihe von Schreibweisen für Vornamen und Nachnamen, die in unterschiedlichen Verwendungszusammenhängen gültig sind. Ebendies trifft

⁶ eDirectory wird im Internetportal als Metadirectory eingesetzt und konkurriert hier mit Produkten wie Siemens DirX oder iPlanet Directory Server

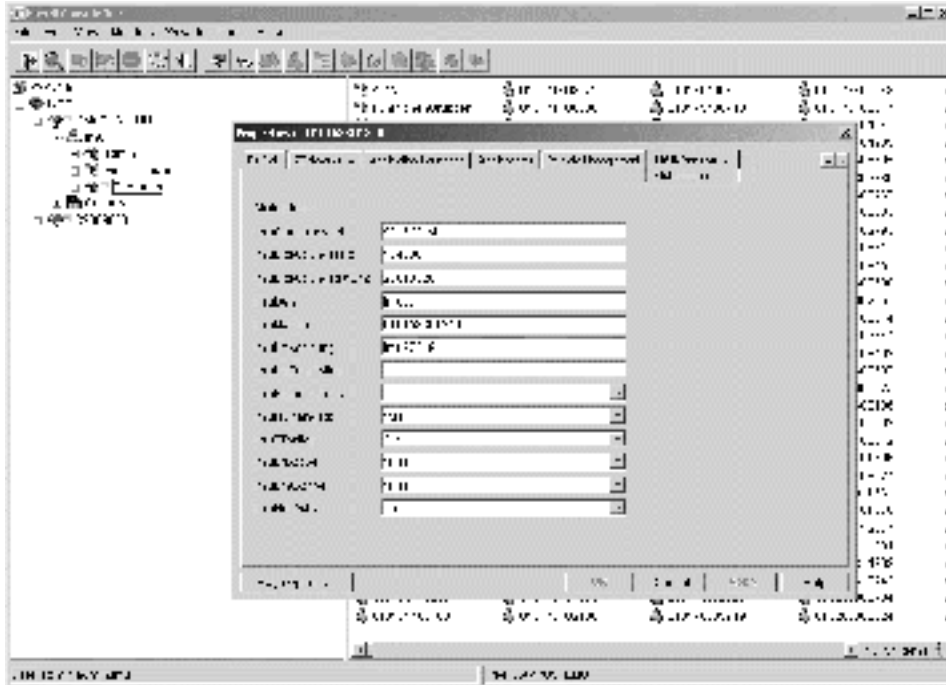


Abbildung 2. Für die Speicherung von Personenprofilen wird eDirectory um neue Objektklassen und Attribute erweitert

auf viele andere Attribute in gleicher Weise zu und macht das im Directory gespeicherte „Metaverse“ zu einer umfangreichen Unternehmung.⁷

Prinzipiell ist das ganze realisierbar, man muß sich aber im Klaren sein, daß man sich vornherein Gedanken über die Umsetzung des Directory-Schemas machen muß. Dieses Problem würde natürlich auch bei der Verwendung von relationalen Datenbanken, in ähnlicher Weise auftreten. Bei einem Directory wird die Sache allerdings noch dadurch kompliziert, daß man die möglichen Rechtesituationen immer mit berücksichtigen muß.

3 Personalisierung

Personalisierung von Internetportalen ist ein sehr neues Gebiet, so daß es wenig Übereinstimmung über den Gebrauch des Begriffs gibt. Manchmal wird Personalisierung auch als Synonym für *customization* gebraucht, für die Anpassung von Websites an die Bedürfnisse der Benutzer.

Gebräuchliche Beispiele für personalisierte Websites sind

⁷ ZOOMIT VIA Metadirectory, Concepts and Architecture, July 1997. Zoomit wurde inzwischen von Microsoft übernommen und soll mit seinem Produkt VIA in Microsoft® Directory Synchronization Services (MSDSS) aufgehen.

- <http://my.netscape.com>, für die Konfiguration eines persönlichen Informationsportals
- <http://www.amazon.com>, für sogenannte Purchase Circles⁸ oder Recommender Systems
- <http://store.apple.com>, für die Konfiguration von Produkten vor der Produktion

Im Falle von Netscape bedeutet Personalisierung die Auswahl aus einem Überangebot von Informationen. Bei Amazon bedeutet Personalisierung die Anpassung von Angeboten an das persönliche Interesse beziehungsweise der Interessengruppe, dem sogenannten *Purchase Circle*, zu dem man gehört. Bei Apple handelt es sich ganz einfach um eine Datenbankanwendung, die die Konfiguration eines Halbfertigprodukts erlaubt.

Auswahl, Anpassung, persönliche Datenverarbeitung sind wichtige Dinge. Für die Virtuelle Universität braucht man aber noch ein wenig mehr. Das Internetportal der Universität München geht davon aus, daß die Virtuelle Universität den *Campus* auch in seinen sozialen Funktionen repräsentieren muß, wenn sie ihrem Namen gerecht werden will.

Im Virtuellen Campus bedeutet das zum Beispiel

- Benutzer können Profile oder Ausschnitte von Profilen anderer Benutzer sehen
- Benutzer können sehen, wo sich ein anderer Benutzer im Portal gerade aufhält
- Benutzer können mit anderen Benutzern auf der Basis von bestimmten Merkmalen des Profils Kontakt aufnehmen

Wenn solche Funktionen realisiert werden, werden rechtliche Bestimmungen von Datenschutz und Schutz der Persönlichkeit relevant. Tatsächlich muß für die Personen, deren Profile im Directory hinterlegt sind, die informationelle Selbstbestimmung⁹ technisch realisiert werden. Informationelle Selbstbestimmung im Internetportal bedeutet, daß jede Person bestimmen kann, wer welche Attribute oder sogar Werte von Attributen sehen, ändern oder löschen darf.

Die Benutzerschnittstelle muß ein striktes „opt-in“ ermöglichen. Das heißt, daß jeder Zugriff auf das persönliche Profil durch andere vom Benutzer explizit erlaubt werden muß. Opt-in ist weniger ein technisches Problem als ein Problem der Benutzerführung. Die Möglichkeiten die ein Benutzer hat, bei einigen hunderttausend Objekten, die dynamisch und fast beliebig zu überlappenden Gruppen zusammengefaßt werden, sind unüberschaubar groß.

Das Internetportal der Universität München bietet deshalb *flavors* mit voreingestellten nützlichen Freigaben an, die der Benutzer dann durch „opt-out“ auf seine persönlichen Bedürfnisse reduzieren kann (meine Telefonnummer dürfen alle sehen, die mit mir gemeinsam eine Veranstaltung besuchen, aber nicht Rudi Müller).

4 Sicherheit

Personalisierung und informationelle Selbstbestimmung setzt voraus, daß die gespeicherten Daten sicher sind. Daten sind dann sicher, wenn nur authentifizierte Personen auf Daten

⁸ Beck, Rachel, „Tracking the Hot Items“, The Associated Press, 1999

⁹ Gola, Peter, „Personaldaten im Internet“, *Computer Fachwissen*, 11/2000

zugreifen können, für die sie autorisiert sind und die Daten sicher zur authentisierten und autorisierten Person übertragen werden.

Sicherheit im Internetportal beginnt mit der Zertifizierung der Benutzer. Bei Studierenden und Mitarbeitern ist das relativ einfach, da diese Personen ihre Identität bei internen Zertifizierungsstellen nachweisen (Studentenkanzlei, Personalabteilung). Schwieriger ist es bei Externen, wie zum Beispiel Lehrbeauftragten, Gästen von Forschungseinrichtungen. Es ist auch an der Universität München noch unklar, wie die Zertifizierung dieser Personen geregelt werden soll. Die benötigte Hierarchie der *certification agencies* ist an einer Universität von der Größe und Komplexität der LMU nicht leicht zu installieren.

Authentisierung wird im Internetportal der LMU über das Standard LDAP Bind hergestellt. Benutzername und Paßwort berechtigen zum Zugriff auf die geschützten Bereiche. Es sind stärkere Authentisierungsverfahren, wie Public Key oder Chipkarten möglich, aber bisher noch nicht nötig. ACLs (access control lists) eines Directory dienen zur Rechteverwaltung und bestimmen, was der Benutzer im Directory und den Anwendungen tun darf, die auf dem Directory aufsetzen (Authorisierung).

Mittelfristig ist geplant, die Rechteverwaltung von Web-Anwendungen, weitgehend in das Directory zu übernehmen. Die Web-Anwendung kann die ACL entweder über LDAP aus dem Directory auslesen oder eine Art API benutzen, die der Anwendung auf eine Authorisierungsanfrage einfach ein JA oder NEIN zurückgibt.

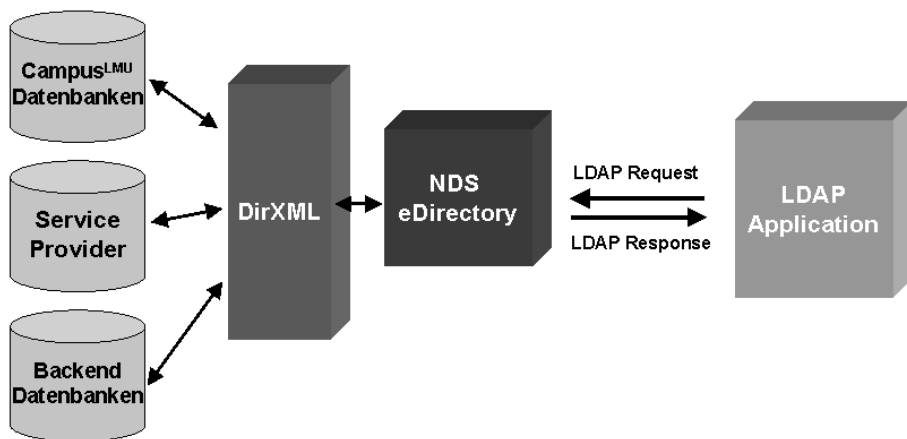


Abbildung 3. Das Directory synchronisiert Datenquellen über DirXML und stellt Anwendungen Directory-Funktionen über LDAP zur Verfügung

Mindestens genauso wichtig wie eine LDAP-Schnittstelle ist DirXML, ein Mechanismus zur Synchronisierung von Backend-Datenbanken mit dem Directory. DirXML eignet sich auch dazu, Backend-Datenbanken über das Directory miteinander zu synchronisieren.

Novell NDS eDirectory stellt eine Reihe von Sicherheitsfunktionen als *layered services* von NDS eDirectory zur Verfügung. Was man gerne benutzen wird ist iChain, eine Sicherheitsinfrastruktur, die die folgenden Dienste zur Verfügung stellt:

- Kontextloser Login, Web-Authentisierung
- SSLizer zur verschlüsselten Verbindungen zu den Browsern
- Server-Caching (durch die ICS Komponente)
- Rollenbasierte Authorisierung
- Web Single Sign-On

iChain kam leider erst auf den Markt als die Entwickler des Internetportals der Universität München die grundlegenden Probleme wie Kontextloser Login, Web-Authentisierung und Web Single Sign-On schon auf andere Art und Weise selbst gelöst hatten.

Das Problem des Kontextlosen Login wird im Internetportal der LMU durch die Benutzung eines flachen Namensraums für die ganze Universität gelöst. Das hat seinen Wert, weil die Accounts in allen Login-Situationen der Universität ohne weitere Komplikationen benutzt werden können. Doppelte Benutzernamen werden bei der Account-Vergabe durch einen Vergabe-Algorithmus aufgelöst.

Das Single-Sign-On wird im Internetportal der LMU durch einen gemeinsamen Authentisierungs-Header der einzelnen Module gelöst. Die Module holen sich die nötige Information von einem zentralen Rechner, der als Datenlieferant dient. iChain löst das Problem auf umgekehrte Art und Weise. Durch das Einfügen der Authentisierungsinformation aus NDS eDirectory in den http Authorisierungs-Header, wird der Benutzer durch die iChain an dem Modul authentisiert.

In heterogenen Serverfarmen ist die Sicherheit der Datenübermittlung ein echtes Problem, da so gut wie jede Entwicklungsumgebung SSL auf andere Art und Weise herstellt.

Die SSLizer Komponente von iChain übernimmt die http-Datenströme der an den iChain/ICS Server angeschlossenen Webserver und wandelt sie in https-Datenströme zum Browser.

Webserver und Anwendungen auf den Webservern bemerken davon nichts und müssen sich nicht weiter mit diesem Problem befassen. Angenehme Nebeneffekte sind zusätzlich, daß nur ein einziges Zertifikat (für den iChain/ICS Server) benötigt wird und daß es keinen Performance-Verlust durch den https-Overhead auf den Webservern gibt.

5 Single Sign-On

Nichts ist abträglicher für die Integrität der Benutzererfahrung in einem Internetportal als der Zwang, sich zu den einzelnen Modulen jeweils getrennt anmelden zu müssen. Das iChain-Verfahren ist eine gute Lösung für das Problem, der Authentisierungs-Header ebenso.

Das iChain-Verfahren setzt allerdings voraus, daß bei einer unverschlüsselten Übertragung zwischen denen am Single Sign-On beteiligten Webservern und der iChain/ICS, ein abhörsicheres Netz zur Verfügung steht. Ist dieses nicht vorhanden, kann zwar zwischen

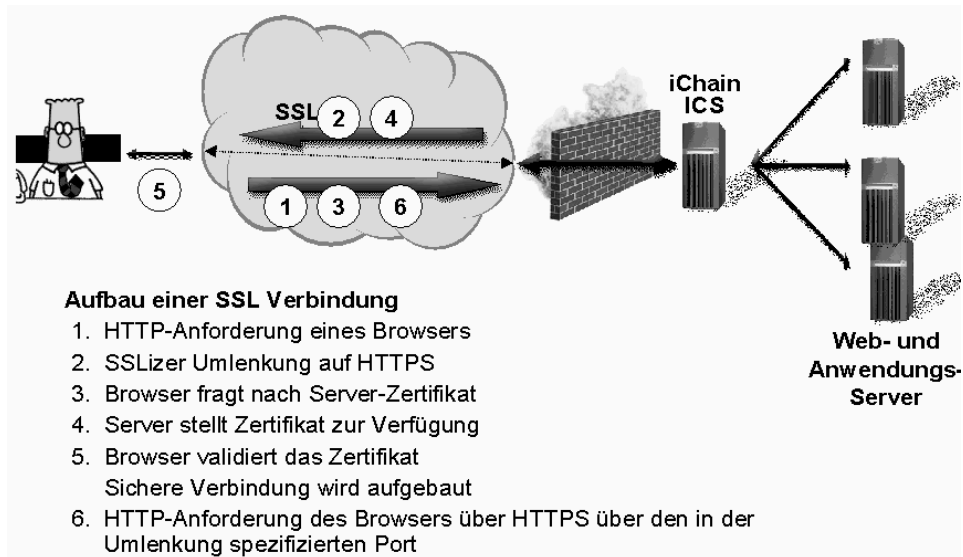


Abbildung 4. Novell's iChain ist die bequemste Art, eine SSL Verbindung zu einer heterogenen Webserver-Farm aufzubauen

iChain und Webserver auf eine verschlüsselte Verbindung zurückgegriffen werden, der Performance-Vorteil auf der Seite des Webservers geht aber dann verloren. Das Verfahren des Authentisierungsheaders setzt voraus, daß jede Anwendung den Code für den Authentisierungsheader inkludiert.

Bei Anwendungen, die logistisch weit voneinander entfernt sind, aber dennoch in einem Single Sign-On Verbund zusammenarbeiten wollen, müssen andere Lösungen gefunden werden.

Eine Lösung ist die Freigabe des LDAP-Zugangs zum Directory für Partneranwendungen. Die Partneranwendung muß dann zumindest über einige Interna des Directory-Schemas informiert sein, ebenso müssen die Betreuer des Directory das Verhalten der Anwendung überwachen.

Eine andere Lösung ist die Hintergrund-Synchronisierung von Account-Informationen über DirXML oder eine ähnliche Lösung. Die Partneranwendung hat lediglich eine Datenaustausch-Vereinbarung mit dem Directory für bestimmte Objekte und Attribute, macht damit aber ansonsten, was sie will.

Die Hintergrund synchronisierung mit dem Directory ist vor allem auch für LANs interessant, die sich die Arbeit mit dem Erfassen und Verwalten von Benutzeraccounts sparen wollen. Da Benutzeraccounts und Benutzerprofile ohnehin zentral im Corporate Directory gehalten werden, gibt es für die Mehrfacherfassung von Daten keinen guten Grund mehr. Novell hat in seinem Produkt Novell Account Management die Werkzeuge zusammengestellt, die für die Synchronisierung von Account-Information im Corporate Directory mit Windows, Netware, Linux und Solaris benötigt werden.



6 Virtuelle Universität

Virtuelle Universität bedeutet, daß Mitgliedern und Partner der Universität im Internet ein geschützter persönlicher Kommunikationsraum zur Verfügung gestellt wird, der wünschenswerte Eigenschaften der *brick-and-mortar* Universität auf der Internet-Plattform realisiert.

Zentrale Software für die Virtuelle Universität ist ein Directory, das Benutzerprofile und Objektrechte verwaltet und Anwendungen sichere Authentisierungs- und Authorisierungsfunktionen zur Verfügung stellt.

NDS eDirectory mit seinen *layered services* ist der zur Zeit am besten ausgestattete Directory Service und stellt mit Diensten wie OnDemand auch Abrechnungsfunktionen zur Verfügung, die in Zukunft auch für Virtuelle Universitäten von Bedeutung sein werden.

