

Andreas Karst

Erweiterung der Virtuellen Universität um einen LDAP Directory Service

Diplomarbeit

BEI GRIN MACHT SICH IHR WISSEN BEZAHLT



- Wir veröffentlichen Ihre Hausarbeit, Bachelor- und Masterarbeit
- Ihr eigenes eBook und Buch - weltweit in allen wichtigen Shops
- Verdienen Sie an jedem Verkauf

Jetzt bei www.GRIN.com hochladen
und kostenlos publizieren



Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Copyright © 2000 Examicus Verlag
ISBN: 9783656980865

Andreas Karst

Erweiterung der Virtuellen Universität um einen LDAP Directory Service

Examicus - Verlag für akademische Texte

Der Examicus Verlag mit Sitz in München hat sich auf die Veröffentlichung akademischer Texte spezialisiert.

Die Verlagswebseite www.examicus.de ist für Studenten, Hochschullehrer und andere Akademiker die ideale Plattform, ihre Fachtexte, Studienarbeiten, Abschlussarbeiten oder Dissertationen einem breiten Publikum zu präsentieren.



Fachbereich Informatik
Lehrgebiet Praktische Informatik I

Diplomarbeit

**Erweiterung der Virtuellen Universität um einen
LDAP Directory Service**

Autor: Andreas Karst

Erklärung

Hiermit versichere ich, die vorliegende Diplomarbeit selbständig verfasst zu haben. Dabei wurden keine anderen, als die angegebenen Quellen und Hilfsmittel benutzt und Zitate kenntlich gemacht.

Ettringen, den 14.02.2000

Andreas Karst

Inhaltsverzeichnis

Erklärung.....	III
Inhaltsverzeichnis.....	V
Abbildungsverzeichnis.....	IX
1 Einleitung	1
1.1 Die Inhalte im Überblick.....	1
1.2 Die Virtuelle Universität.....	2
1.3 Directory Services	3
1.4 Standards für Directories: X.500 und LDAP	5
1.5 Weitere Begriffe und Grundlagen.....	6
2 Die Funktionsweise von LDAP	11
2.1 Kommunikation zwischen Client und Server	11
2.2 Die LDAP-Modelle.....	13
2.2.1 Das Informationsmodell	14
2.2.2 Das Namensmodell.....	15
2.2.3 Das Funktionsmodell.....	19
2.2.4 Das Sicherheitsmodell	23
3 Directory vs. Datenbank.....	25
3.1 Verhältnis von Lese- bzw. Such- zu Schreibzugriffen.....	25
3.2 Komplexität.....	26
3.2.1 Operationen	26
3.2.2 Anwendungslogik auf dem Server.....	27
3.2.3 Unterstützung von Transaktionen	28
3.2.4 Beziehungen	29
3.2.5 Zusammenfassung	30
3.3 Kapselung.....	30
3.4 Standardisierung.....	31
3.4.1 Standardisierung von Datenmodell und Schema	32
3.4.2 Standardisierung der Kommunikationsschnittstellen.....	33
3.4.3 Ergebnis.....	35
3.5 Verteilung von Datenbeständen auf mehrere Server	35
3.6 Redundante Allokation.....	38
3.7 Zugang für Internet-Anwendungen.....	41
3.7.1 Datenbank-Zugang über das Common Gateway Interface (CGI).....	42
3.7.2 Datenbank-Zugang mit Application Programming Interfaces (APIs)	43
3.7.3 Andere Datenbank-Zugänge	46
3.7.4 Zugang zu Directory Services	48
3.7.5 Ergebnis.....	49
3.8 Modellierung.....	49
3.9 Flexibilität des Schemas.....	50
3.10 Zusammenfassung.....	51

4 Anwendungen	53
4.1 Klassische Authentifizierung	54
4.1.1 Klassische Authentifizierung ohne Directory Service	54
4.1.2 Klassische Authentifizierung mit Directory Service	56
4.1.3 Voraussetzungen	59
4.1.4 Benötigte Daten und LDAP-Operationen	61
4.1.5 Nebenbedingungen	62
4.1.6 Beurteilung	64
4.2 Sichere Authentifizierung und ihre Verwaltung	65
4.2.1 PKI ohne Directory Service	66
4.2.2 PKI mit Directory Service	68
4.2.3 Voraussetzungen	69
4.2.4 Benötigte Daten und LDAP-Operationen	70
4.2.5 Nebenbedingungen	70
4.2.6 Beurteilung	71
4.3 Zugriffskontrolle für Anwendungsserver	72
4.3.1 Zugriffskontrolle ohne Directory Service	72
4.3.2 Zugriffskontrolle mit Directory Service	72
4.3.3 Voraussetzungen	80
4.3.4 Benötigte Daten und LDAP-Operationen	81
4.3.5 Nebenbedingungen	81
4.3.6 Beurteilung	82
4.4 Adressierung und Verschlüsselung von Mails	82
4.4.1 Auskunft über Mail-Adressen	83
4.4.2 Bereitstellung von Zertifikaten	84
4.4.3 Mail Routing	86
4.4.4 Voraussetzungen	88
4.4.5 Benötigte Daten und LDAP-Operationen	89
4.4.6 Nebenbedingungen	89
4.4.7 Beurteilung	90
4.5 Organisationssystem für Personen und Objekte	92
4.5.1 Einsatzbereiche eines Organisationssystems	92
4.5.2 Potential eines Directory basierenden Organisationssystems	93
4.5.3 Voraussetzungen	94
4.5.4 Benötigte Daten und LDAP-Operationen	94
4.5.5 Nebenbedingungen	95
4.5.6 Beurteilung	96
4.6 Weitere Anwendungen	98
4.6.1 Verwaltung der Konfiguration von verteilten Diensten	98
4.6.2 Ortsunabhängigkeit des Arbeitsplatzes	99
4.6.3 Zugangsüberwachung mittels Kartenleser	100
4.6.4 Workflow-Anwendungen	101
4.7 Zusammenfassung	101
4.7.1 Zusammenstellung benötigter Daten und LDAP-Operationen	101
4.7.2 Zusammenfassende Beurteilung	104
5 Realisierung	106
5.1 Entwurf des Schemas	106
5.1.1 Vorgehensweise	107
5.1.2 Das Schema	108
5.2 Der Namensraum	113
5.2.1 Auswirkungen der Struktur des DIT	113
5.2.2 Strukturierung des DIT der FernUniversität	114
5.2.3 Benennung der Einträge	116
5.3 Partitionierung des DIT	116

5.4 Redundante Allokation.....	118
5.4.1 Einsatz redundanter Allokation	118
5.4.2 Replikationsverfahren.....	120
5.4.3 Übermittlung der Updates.....	123
5.4.4 Lastteilung und Ausfallsicherheit	125
5.4.5 Sonstige Anforderungen	126
5.4.6 Zusammenfassung	128
5.5 Änderung persönlicher Daten durch Benutzer.....	128
5.5.1 Änderung gemeinsamer Daten von Directory und Datenbank	128
5.5.2 Schnittstelle zur Änderung	129
5.6 Datenschutz und Datensicherheit.....	134
5.6.1 Zugriffskontrolle.....	134
5.6.2 Iterationen.....	135
5.6.3 Direkter Zugriff der Clients für Auskünfte	136
5.6.4 Gefahren ungesicherter Kommunikation	141
5.6.5 Zusammenfassung	144
5.7 Koexistenz des Directories mit anderen Datenquellen	144
5.7.1 Berücksichtigte Daten und Datenquellen.....	145
5.7.2 Grundsätzliche Alternativen der Koexistenz	145
5.7.3 Realisierung der Synchronisation	149
5.7.4 Zusammenfassung	153
5.8 Zusammenfassung des Modells	153
6 Zusammenfassung und Ausblick.....	156
6.1 Zusammenfassung der Ergebnisse	156
6.2 Angrenzende Themen und weitere Entwicklung	157
Anhang	A 1
Literatur.....	A 1

Abbildungsverzeichnis

Abbildung 1.2-1: Oberfläche der Virtuellen Universität im Browser	2
Abbildung 1.3-1: Directory-Zugriff mit einem Browser	4
Abbildung 2.1-1: Typischer Verlauf einer LDAP-Kommunikation.....	12
Abbildung 2.1-2: Nachrichtenaustausch zwischen Client und Server.....	12
Abbildung 2.1-3: Parallele Suchanfragen.....	12
Abbildung 2.1-4: Zugriff auf einen LDAP-Server über ein LDAP-API	13
Abbildung 2.2-1: Vereinfachtes theoretisches Beispiel für einen DIT.....	16
Abbildung 2.2-2: Partitionierung eines DIT	18
Abbildung 2.2-3: Gleichzeitige Umbenennung und Verschiebung eines Eintrags	21
Abbildung 3.4-1: Zugriff auf verschiedene DBMS mittels RDA.....	34
Abbildung 3.5-1: Arten der Partitionierung von Relationen	36
Abbildung 3.6-1: Lastteilung und lokale Kopie im Normalfall.....	38
Abbildung 3.6-2: Situation im Fehlerfall.....	39
Abbildung 3.7-1: Zugriff auf Datenbanken via CGI	42
Abbildung 3.7-2: Varianten JDBC-Treiber	44
Abbildung 3.7-3: Zugriff auf Datenbanken via web.sql	47
Abbildung 4.1-1: Redundante Benutzerdaten.....	55
Abbildung 4.1-2: Nicht-Redundante Benutzerdaten	56
Abbildung 4.1-3: LDAP-Authentifizierung durch die Anwendung	57
Abbildung 4.1-4: PAM-Architektur	58
Abbildung 4.2-1: SSL-PKI im PASS-Projekt.....	67
Abbildung 4.2-2: PKI mit Directory Service.....	68
Abbildung 4.3-1: Zugriffskontrolle mit lokalen ACLs.....	73
Abbildung 4.3-2: Zugriffskontrolle mit ACLs in einem zentralen Directory.....	74
Abbildung 4.3-3: Zugriffskontrolle mit ACLs in lokalem Directory	76
Abbildung 4.3-4: Verwendung der Zugriffskontrolle des Directory Service	77
Abbildung 4.4-1: Mailverzeichnis der FernUniversität.....	83
Abbildung 4.4-2: Suche einer Mail-Adresse bei einem LDAP-Directory Service.....	84
Abbildung 4.4-3: Suche nach Zertifikaten über die Web-Schnittstelle der CA	85
Abbildung 4.4-4: Suche nach Zertifikaten bei einem LDAP Directory Service	86
Abbildung 4.4-5: Kommunikation Adressierung und Verschlüsselung von Mails.....	86
Abbildung 4.4-6: Mail Routing mit LDAP Directory Service	87
Abbildung 4.5-1: Beispiel: Integration von Telefonsystem und Directory Service	94
Abbildung 4.6-1: Ablage von Server-Konfigurationen in einem Directory	99
Abbildung 4.6-2: Steuerung von Kartenlesern mittels Directory Service	100
Abbildung 5.2-1: Entwurf eines DIT für die FernUniversität Hagen.....	115
Abbildung 5.4-1: Umleitung von Updates an den Master Server mittels Referral.....	121
Abbildung 5.4-2: Umleitung von Updates an den Master Server mittels Chaining	121
Abbildung 5.4-3: Funktionsweise eines Loadbalancing-Routers	126
Abbildung 5.5-1: Formular zur Datenänderung für die Virtuelle Universität.....	132
Abbildung 5.6-1: Verwendung eines gefilterten öffentlichen Directory Servers.....	138
Abbildung 5.7-1: Funktionsweise eines virtuellen Directories	146
Abbildung 5.7-2: Redundante Speicherung gemeinsamer Attribute	148
Abbildung 5.8-1: Logische Netzwerkarchitektur des Modells.....	155

1 Einleitung

Durch die permanent wachsende Bedeutung des Internets für alle Bereiche des täglichen Lebens, rücken auch die im Internet verwendeten Technologien immer weiter in den Mittelpunkt des informationstechnischen Interesses. Besonders hervorgeraten hat sich diesbezüglich in letzter Zeit die Technologie der *LDAP Directory Services*, die – schenkt man der einschlägigen Fachliteratur Glauben – im Begriff sind eine zentrale Position in modernen informationstechnischen Infrastrukturen einzunehmen. Dort werden sie als universelle zentrale Auskunftssysteme eingesetzt, um die Verwaltung von Benutzerdaten, Mail-Adressen, Sicherheitsinformationen u.a. zu vereinfachen.

Im Rahmen dieser Diplomarbeit wird untersucht, inwiefern der Einsatz eines LDAP Directory Service für die *Virtuelle Universität* der FernUniversität Hagen, als einer auf dem Internet basierenden Infrastruktur zur Unterstützung von Fernstudien, sinnvoll und realisierbar ist. Dazu muss zunächst geklärt werden, wie ein LDAP Directory Service funktioniert, worin er sich von ähnlichen Systemen unterscheidet und was die wesentlichen Vorteile seiner Verwendung sind. Darauf aufbauend können dann Einsatzmöglichkeiten bei der Virtuellen Universität identifiziert, untersucht und beurteilt werden. Die dabei gewonnenen Erkenntnisse dienen schließlich als Grundlage für den Entwurf eines entsprechenden Directory Service.

1.1 Die Inhalte im Überblick

Dementsprechend beschäftigt sich Kapitel 2 „Die Funktionsweise von LDAP“ mit dem Protokoll, das zur Kommunikation mit dem Directory Service eingesetzt wird und dadurch seine Charakteristik maßgeblich prägt.

Um die typischen Eigenschaften eines LDAP Directory Service genauer zu spezifizieren und mögliche Einsatzbereiche abgrenzen zu können, werden in Kapitel 3 „Directory vs. Datenbank“ Directories mit den Systemen verglichen, denen sie am ähnlichsten sind, nämlich mit Datenbanken.

In Kapitel 4 „Anwendungen“ folgt dann eine detaillierte Untersuchung und Beurteilung möglicher Verwendungen eines LDAP Directory Service im Umfeld der Virtuellen Universität, einschließlich der Voraussetzungen und Nebenbedingungen, die ihre Umsetzung für den Directory Service bedeuten.

Mit den bis dahin gesammelten Erkenntnissen, wird es in Kapitel 5 „Realisierung“ anschließend möglich sein, die wesentlichen Kriterien für die Implementierung eines LDAP Directory Service zu spezifizieren.

Kapitel 6 „Zusammenfassung und Ausblick“ dient schließlich der Zusammenfassung der Ergebnisse sowie dem Ausblick auf angrenzende Themen und die weitere Entwicklung.

Zunächst aber, wird in den folgenden Abschnitten dieses einleitenden Kapitels die Virtuelle Universität der FernUniversität Hagen kurz vorgestellt und der Begriff des Directory Service sowie seine Entwicklung und Benutzung beleuchtet. Ferner werden grundlegende Begriffe und Zusammenhänge aus dem informationstechnischen Umfeld, die für das Verständnis der weiteren Ausführungen erforderlich oder zumindest hilfreich sind, erläutert.

1.2 Die Virtuelle Universität

Die Virtuelle Universität ist ein integriertes Online-System, das an der FernUniversität Hagen entwickelt wurde, um den Studenten weitestgehende räumliche und zeitliche Unabhängigkeit für ihr Studium zu bieten. Diese Zielsetzung ist insbesondere vor dem Hintergrund der Situation der Fernstudenten zu sehen, die in der Regel neben einer beruflichen Tätigkeit ihrem Studium nachgehen und deshalb die Dienstleistungen der FernUniversität von Zuhause aus und zu individuell unterschiedlichen Zeiten in Anspruch nehmen möchten. Das ideale Medium zur Realisierung dieser beiden Ziele bietet das Internet, das heutzutage flächendeckend und rund um die Uhr verschiedenste Dienste zur Verfügung stellt.

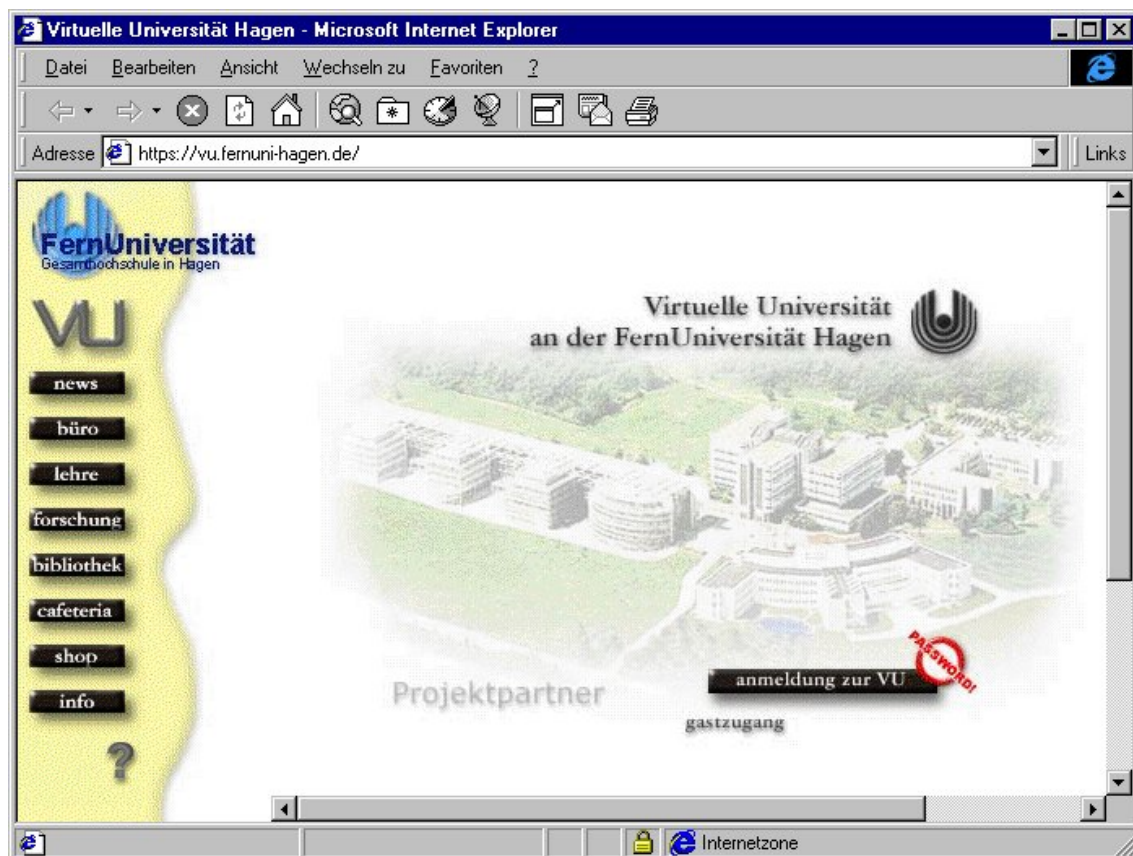


Abbildung 1.2-1: Oberfläche der Virtuellen Universität im Browser

Inhalte und Funktionen

Die Studenten erhalten über die Virtuelle Universität Zugang zu allen Informationen und Funktionen, die mit ihrem Studium zusammenhängen [BMS96a], [BMS96b]: neben dem Zugang zu Lehrmaterialien wie z.B. Textkursen, Computer Based Trainings, Videos, Animationen und Simulationen, können sie an interaktiven Lehrveranstaltungen, Übungsgruppen und Praktika teilnehmen. Sie sind in der Lage administrative Funktionen wie das Belegen von Kursen, die Rückmeldung zum nächsten Semester oder die Änderung der persönlichen Daten zu erledigen. Alle wichtigen Informationen rund um das Fernstudium stehen in strukturierter Form zur Verfügung. In der Bibliothek der FernUniversität können die Studenten online Bücher suchen und zur Fernausleihe bestellen bzw. online verfügbare Veröffentlichungen auf ihren PC laden. Forschende haben Zugriff auf Papers und Berichte zu Forschungsprojekten an der FernUniversität.

Schließlich gibt es durch alle Bereiche hindurch die Möglichkeit sich über Schwarze Bretter, Chat, Videokonferenz oder Mail mit Kommilitonen, Tutoren und Professoren auszutauschen, um so die soziale Isolation des Fernstudiums zu überwinden.

Technische Voraussetzungen

Um die Virtuelle Universität nutzen zu können, benötigt man neben einem PC einen Zugang zum Internet. Dieser kann z.B. über das Projekt „Uni@home“ eingerichtet werden, das den Studenten einen bundesweiten Netzzugang zum Ortstarif ermöglicht [FUH99]. Darüber hinaus ist eine Browser-Software erforderlich, die mit Hilfe von integrierten sogenannten „Helper Applications“ die Funktionen realisiert [BMS96a]. Um den Missbrauch durch Unberechtigte zu verhindern, erfolgt die Kommunikation mittels einer „sicheren Verbindung“ über Secure Socket Layer (SSL, siehe 1.5 „Weitere Begriffe und Grundlagen“) und ist durch eine Benutzererkennung und ein Kennwort geschützt.

1.3 Directory Services

Der Begriff *Directory Service* bedeutet auf deutsch Verzeichnisdienst. Daraus wird deutlich, dass es sich um einen (Computer-)Dienst handelt, der ein Verzeichnis zur Verfügung stellt. Verzeichnissen begegnet man überall im täglichen Leben. Die letzte Begegnung mit einem Verzeichnis hatte der Leser vor wenigen Seiten: das Inhaltsverzeichnis dieser Diplomarbeit. Andere Beispiele sind Telefonbücher, Mitarbeiterverzeichnisse, Vorlesungsverzeichnisse usw. Dabei bestehen Verzeichnisse immer aus einer Anzahl von Einträgen, die jeweils verschiedene Informationen zu einem Objekt enthalten und nach bestimmten Kriterien gruppiert sein können. So enthält das Inhaltsverzeichnis dieser Diplomarbeit Einträge, in denen die Kapitel- und Abschnittüberschriften sowie deren Seitenzahlen zu finden sind. Die Einträge sind nach Kapitel gruppiert und nach Seitenzahlen sortiert. Ein Telefonbuch hingegen enthält Einträge, die neben dem Namen und der Telefonnummer von Personen ggf. noch weitere Informationen wie Adresse oder Beruf enthalten können. Die Einträge sind dort nach Orten gruppiert und innerhalb der Orte alphabetisch nach Namen sortiert.

Arten von Directories

Analog zu den gedruckten „Papierverzeichnissen“, gibt es elektronische Verzeichnisse (Directories), die von Computern zur Verfügung gestellt werden. Es handelt sich dabei um spezielle Datenbanken, die getypte Informationen zu Objekten wie z.B. Personen, Gruppen, Computern, Druckern usw. speichern. Die ersten Directories tauchten bereits in den frühen 70‘er Jahren auf und dienten auf Großrechnersystemen der Benutzerverwaltung. Seitdem gab es eine Vielzahl von Entwicklungen, die die Einsatzmöglichkeiten von Directories erheblich erweiterten:

- Directories werden als integrierter Bestandteil von Mail- und Groupware-Produkten wie z.B. Lotus Notes, Novell GroupWise oder Microsoft Exchange zur Verwaltung von Benutzern und Gruppen eingesetzt.
- Internet Directories wie z.B. Yahoo’s Four11 Directory (<http://www.four11.com>) dienen als zentrale Auskunftssysteme für Benutzer des Internets, die Mail-Adressen, Telefonnummern etc. suchen.
- Directories werden in Netzwerkbetriebssystemen eingesetzt, um Netzwerkressourcen zu verwalten. Beispiele sind die Novell Directory Services (NDS) in Novell’s Netware und das Active Directory in Microsoft’s Windows 2000.

Während diese Directories nur bestimmte Objekte für bestimmte Aufgaben verwalten und/oder nur in einer homogenen Umgebung, d.h. mit Hilfe der speziellen Software eines bestimmten Herstellers zugänglich sind, gibt es auch Directories, die diese Einschränkungen überwinden. Sie sind in der Lage verschiedenste Objekte und ihre Eigenschaften zu speichern, um damit beliebige Anwendungen zu bedienen. Der Aufbau solcher Directories und der Zugriff auf sie ist durch Standards geregelt, die von einer Vielzahl von Herstellern unterstützt werden und dadurch auch in heterogenen Umfeldern nutzbar sind. Beispiele für solche Standards sind X.500 und LDAP, die im weiteren Verlauf dieses Kapitels noch betrachtet werden.

Verwendung

Ein Benutzer kann die Einträge von standardisierten Mehrzweck-Directories nach beliebigen Kriterien durchsuchen und auf die Informationen der passenden Objekte zugreifen. Dabei spielt es keine Rolle, welche Software er dazu verwendet, solange diese den Standard unterstützt. Wenn er z.B. den Namen einer Person weiß, kann er ein Mitarbeiterverzeichnis nach dieser Person durchsuchen, um die Mail-Adresse zu ermitteln. Hat er den Namen vergessen, reicht auch eine beliebige andere Information, wie die Zimmernummer des Gesuchten. In einem Verzeichnis der Netzwerkressourcen eines Unternehmens kann er sehr effizient den räumlich nächsten Netzwerkdrucker mit einer Duplexeinheit ermitteln, um einen Druckjob dorthin zu schicken. Die Einsatzmöglichkeiten sind dabei kaum begrenzt und werden ein zentrales Thema dieser Diplomarbeit sein.

Abschließend sollte sich der Leser ein erstes Bild von der einfachen und intuitiven Verwendung eines Directory Service machen. Hierzu ist – abgesehen von einem PC mit Internet-Zugang – nichts weiter nötig, als ein Browser wie z.B. der Netscape Communicator oder der Microsoft Internet Explorer in einer aktuellen Version. In diesen Browsern sind bereits einige Directory Services vorkonfiguriert. Beim Internet Explorer ruft man lediglich „Bearbeiten – Verzeichnis durchsuchen“ auf und wählt im folgenden Dialog den Directory Service und die Suchkriterien aus, vgl. Abbildung 1.3-1. Nach erfolgreicher Suche werden die Ergebnisse dann im unteren Listenfenster angezeigt.

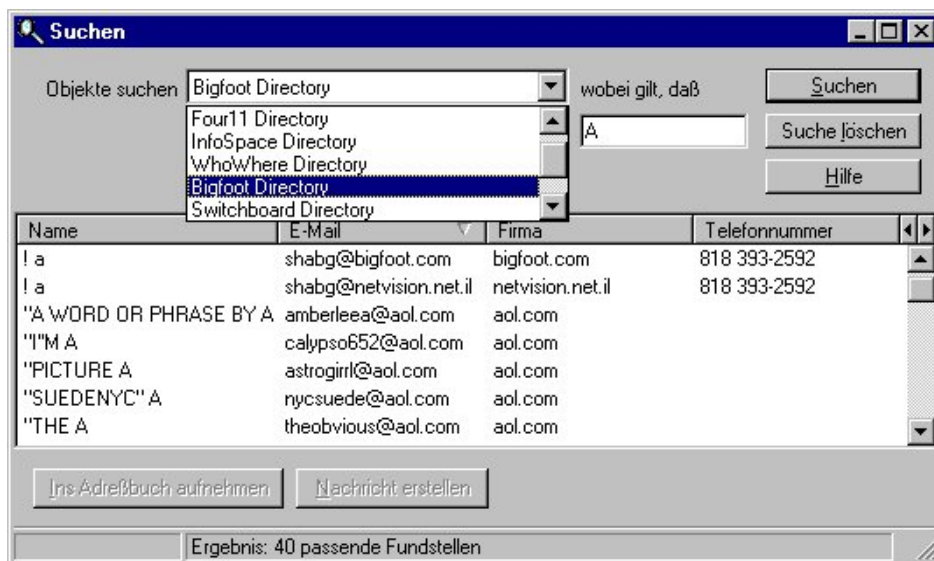


Abbildung 1.3-1: Directory-Zugriff mit einem Browser