X.500 und Directory-Dienste unter Windows NT

Vortrag für das ZDV NT-Seminar

Karl-Peter Gietz, DFN-Projekt AMBIX,
Zentrum für Datenverarbeitung, Universität Tübingen

Gliederung

Internationale Standardisierungsgremien

- Der X.500-Standard wurde von zwei wichtigen internationalen Normierungsgremien definiert:
  - ISO (International Standards Organization): Die Vereinigung der nationalen Normierungsgremien
  - CCITT (Comitée Consultativ International Telephonique et Telegraphique): Das ehemalige internationale Beratungsgremium der Telekommunikationsgesellschaften
  - ITU (International Telecommunications Union): Die Nachfolgeorganisation der CCITT
- In Europa gibt es das Koordinierungsgremium DANTE (Delivery of Advanced Network Technology to Europe).
- In Deutschland ist der DFN-Verein (Deutsches Forschungs Netzt) für die Einführung und den Betrieb von X.500 zuständig.

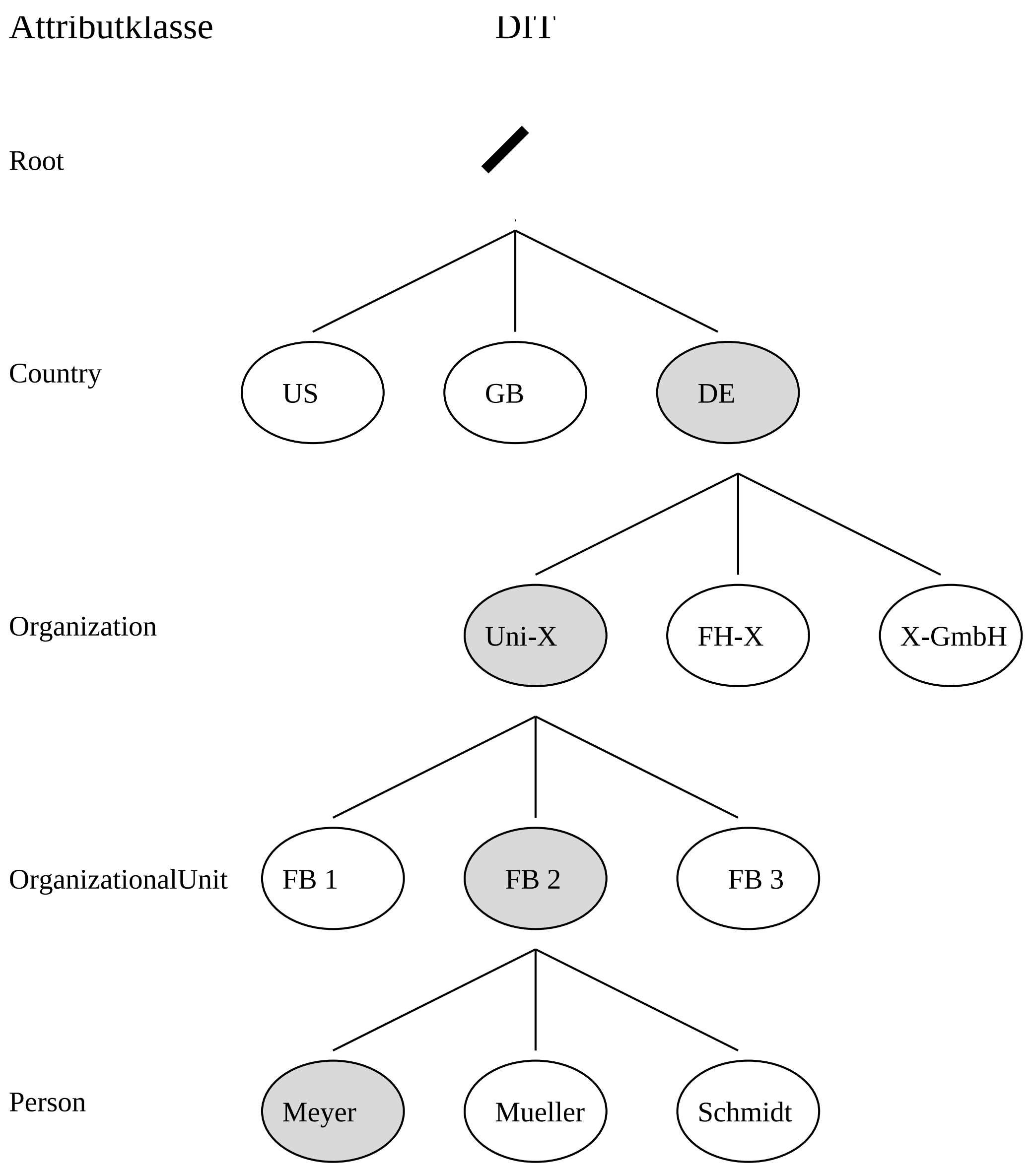
Intergration in die OSI-Welt

- Alle 7 Schichten des OSI-Stacks
- Teil des OID-Baums
- ASN.1 Definition
- Integration mit anderen OSI-Diensten:
  - X.25 (Leitungsprotokoll)
  - X.400 (E-Mail-Protokoll, das auf X.500-Dienste aufbaut)
  - FTAM *File Transfer, Access, and Management* (Sicheres File Transfer Protokoll)

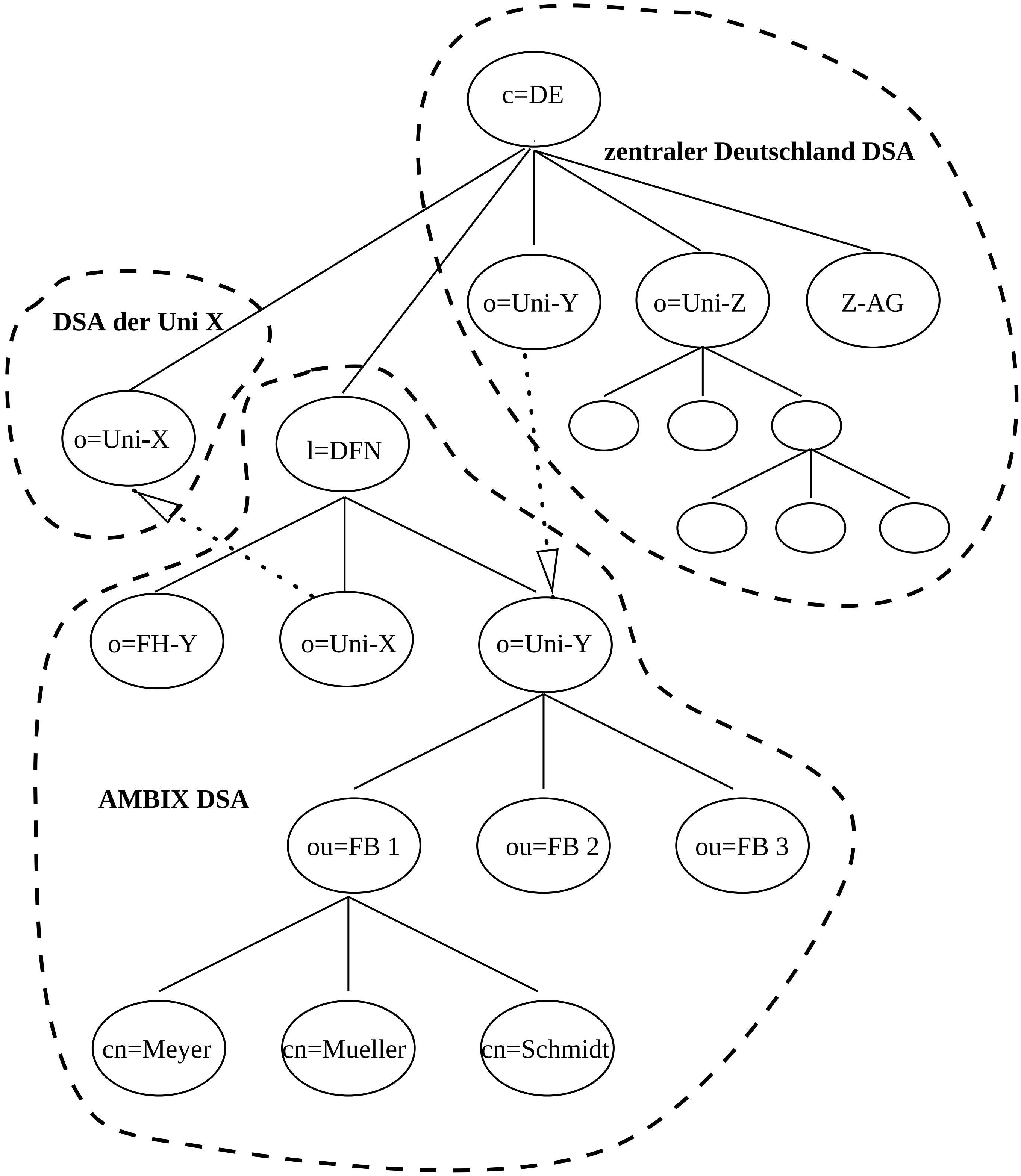
Entwicklung des Standards

Name	Neuerungen	X.509-Version
1988	Gesamtkonzept; Protokolle; Zugriffsrechte ungenau definiert;	X.509v1
1993	Zugriffsrechte umfassend definiert; Aufteilung der Verantwortlichkeiten; neue Protokolle; neue Replikationsmechanismen	X.509v2
1997	noch nicht verabschiedet	X.509v3

Der *Directory Information Tree (DIT)*



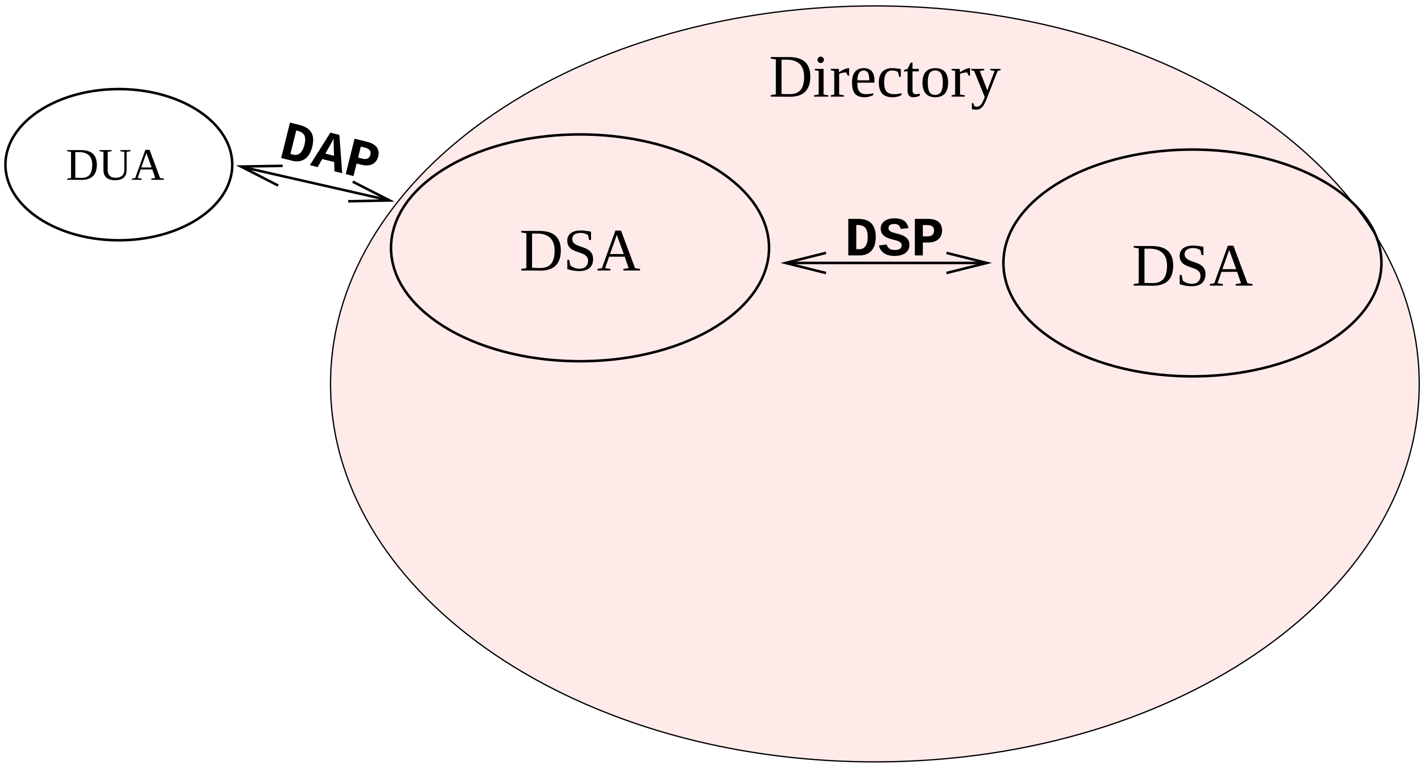
Verteilung des DITs auf die DSAs



Das Client-Server-Modell

- DSA (*Directory System Agent*) mit DSP (*Directory System Protocol*)

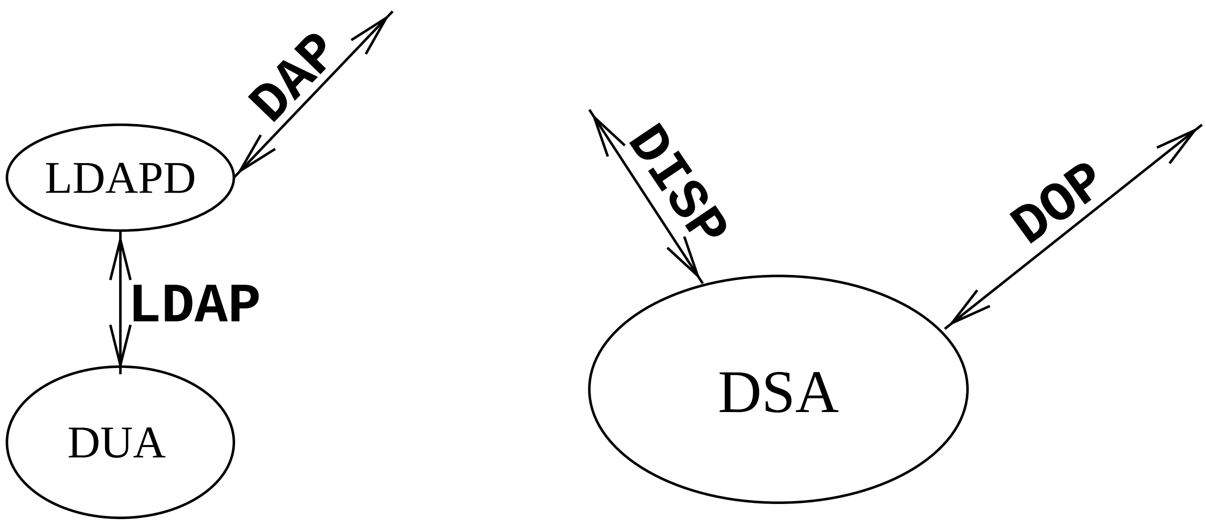
- DUA (*Directory User Agent*) über DAP (*Directory Access Protocol*)



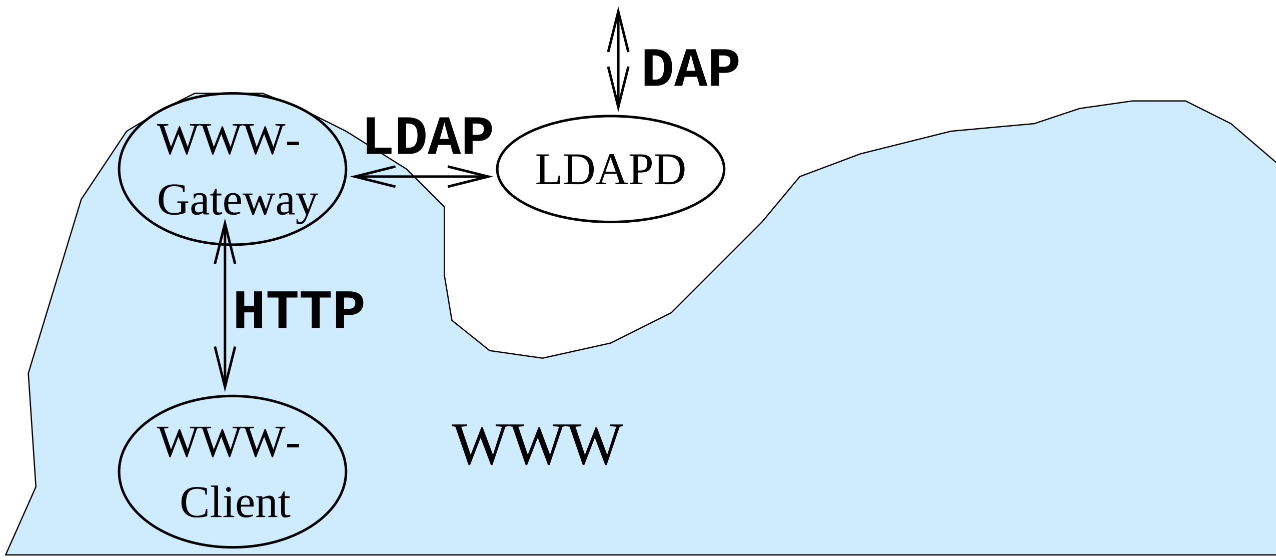
- DSA mit DISP (*Directory Information Shadowing Protocol*) und
- DOP (*Directory Operational Binding Management Protocol*)

- DUA über LDAP (*Lightweight Directory Access Protocol*)

—



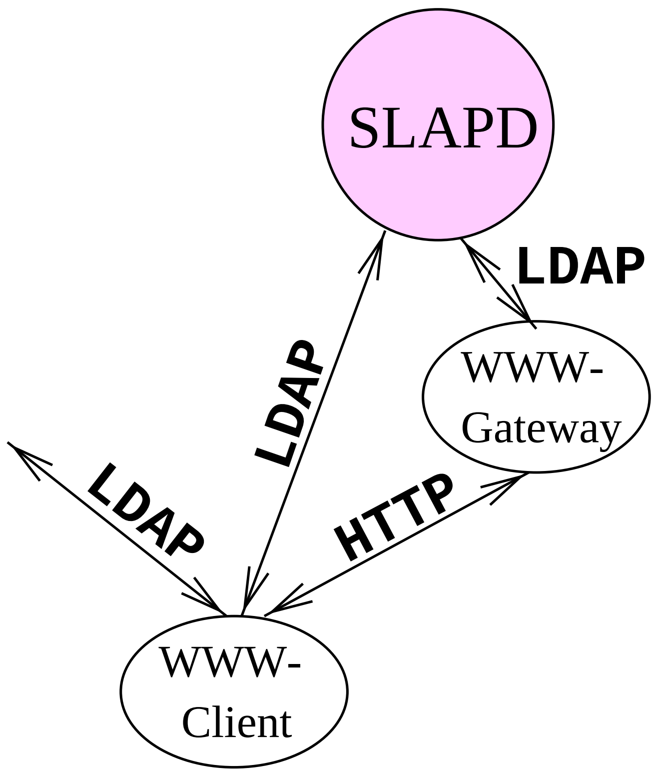
- WWW-X.500-Gateway über LDAP



- SLAPD (*Standalone LDAP Directory Server*)

- WWW-Client über LDAP

—



Das Informationsmodell

Name	Beschreibung	entspricht
Directory	Das über Server auf der ganzen Welt verteilte Informationssystem im baumförmigen DIT.	Datenbank
Eintrag	Ein Knoten im DIT der beliebige Information aufnehmen kann und der durch einen *Distinguished Name* (DN) weltweit gleich ansprechbar ist.	Datensatz
Attribut	Objekt zum Speichern von Information.	keine Entsprechung
Attributtyp	Genau definiertes Attribut. Attributtypen können Eigenschaften (Attributwerte) an Subattributtypen weitervererben.	Datenfeld
Attributsyntax	Beschreibung der Syntax für Werte eines Attributtyps.	Feldtyp
Attributwert	Inhalt eines Attributs, der einer Attributsyntax folgt.	Feldinhalt
RDN	*Relativ Distinguished Name* Schlüssel, der den Eintrag auf der Hierarchieebene im Baum, in welcher sich der Eintrag befindet, eindeutig macht.	keine Entsprechung
DN	*Distinguished Name* Aneinanderreihung von allen RDNs bis zur Wurzel, wodurch ein Eintrag weltweit im Baum eindeutig ansprechbar wird.	Identifizierungsschlüssel
Kollektivattribut	Attribut, dessen Wert für alle hierarchisch tieferliegende Einträge gilt.	keine Entsprechung
Attributset	Gruppierung von Attributen.	keine Entsprechung
Objektklasse	Attribut, das einen Eintrag definiert und obligatorische und optionale Attributtypen bestimmt. Objektklassen können Eigenschaften (Attributwerte, Zugriffsrechte) an Subklassen vererben.	keine Entsprechung

Basic Access Control Scheme I

- Schützbare Elemente („*Protected Items*“) sind:
  - Einträge
  - Attribute
  - Attributwerte
  - DNs
- Diese können einzeln aufgezählt oder in folgenden vordefinierten Gruppen angesprochen werden:
  - Gruppe von Einträgen innerhalb der gleichen AA
  - alle Attribute eines Eintrags
  - alle Werte eines Attributs

Basic Access Control Scheme II

- Es kann genau definiert werden, welcher Vorgang erlaubt bzw. nicht erlaubt sein soll:
  - lesen
  - auflisten
  - vergleichen
  - filtern
  - hinzufügen
  - ändern
  - löschen
  - umbenennen
  - an anderen Ort im DIT exportieren
  - an neuen Ort importieren
  - Rückgabe eines DN
  - Rückgabe einer Fehlermeldung, die die Existenz eines Eintrags verrät
- Solche Rechte können vergeben werden an:
  - einzelne Benutzer(innen)
  - verschieden zusammfaßbare Benutzer-Gruppen
  - unterschiedliche Benutzer-Authentifizierungs-Stufen
  - Alle

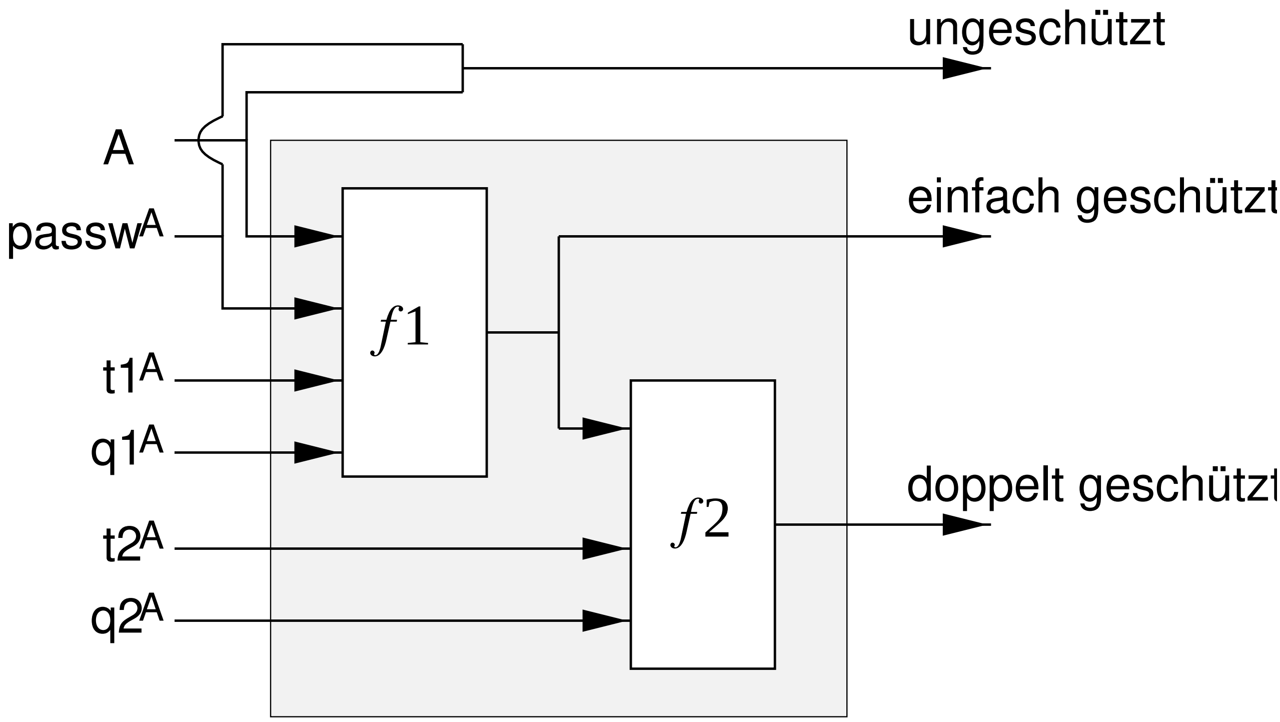
Basic Access Control Scheme III

- Bei der Auswertung der Rechte gelten folgende Grundregeln:
  - Es wird kein Zugriffsrecht durch Voreinstellung vergeben.
  - Ein spezielles Zugriffsrecht (z.B. auf ein Attributtyp) beinhaltet kein allgemeineres (z.B. auf den Eintrag).
  - Ein Zugriffsrecht auf einen Eintrag beinhaltet kein Zugriffsrecht auf die darin enthaltenen Attributtypen und -werte. Die zwei Ausnahmen:
    - Löschung
    - Umbennenung, obwohl hier das Attribut, das für den RDN zuständig ist, geändert wird.
  - Es finden keine Überprüfungen nach unlogischen Kombinationen von Zugriffsrechten statt.

Zugriffskontrollen

Recht	Wirkung bei Eintrag (= E)	bei Attributtyp (= AT)	bei Attributwert (= AW)
Read	erlaubt Lesezugriff für Operationen, die den Namen des E betreffen; ist notwendige aber nicht ausreichende Voraussetzung für Lesezugriffe auf AT bzw. AW	erlaubt Lesezugriff für Operationen die AT einschließen; ist notwendige aber nicht ausreichende Voraussetzung für Lesezugriffe auf AW	erlaubt den Lesezugriff auf einzelne AW
Browse	erlaubt Auflist- und Suchoperationen, die den Namen des E betreffen	n.v.	n.v.
Compare	n.v.	erlaubt nach Vorhandensein eines ATs zu vergleichen; Read-Recht für E ist Voraussetzung	erlaubt Inhalt eines AWs zu vergleichen; Voraussetzungen: Read-Recht für E und Comparerecht für AT
FilterMatch	n.v.	erlaubt einen AT bei der Evaluierung eines Suchfilters zu verwenden; Browse-Recht für E ist Voraussetzung	erlaubt einen AW bei der Evaluierung eines Suchfilters zu verwenden; FilterMatch-Recht auf AT und Browse-Recht für E sind Voraussetzung
Add	erlaubt einen neuen E anzulegen, jedoch ohne AT bzw. AW; Add-Recht für obligatorische AT muß gegeben sein	erlaubt Hinzufügung eines ATs zu einen E; Add-Recht für mindestens einen AW muß gegeben sein, genauso wie Add- bzw. Modify-Recht auf E	erlaubt Hinzufügung eines AWs; falls AT noch nicht existiert, ist Add-Recht für AT Voraussetzung
Modify	erlaubt Veränderungen am E	n.v.	n.v.
Remove	erlaubt Löschung eines E; keinerlei sonstige Rechte sind hierfür vonnöten!	erlaubt Löschung eines AT; Remove-Recht für alle AW und Modify-Recht für E sind Voraussetzungen	erlaubt Löschung eines AW; wenn letzter AW gelöscht wird, ist Remove-Recht für AT Voraussetzung
Rename	erlaubt Umbennenung (= Änderung des RDNs) eines Es; keinerlei Rechte bezüglich AT und AW sind hierfür vonnöten; keinerlei Rechte auf untergeordnete Es, die hierdurch ihren DN ändern, sind vonnöten!	n.v.	n.v.
Export	erlaubt den E an eine andere Stelle im DIT umzusetzen; Voraussetzung ist Import-Recht für den neuen Übergeordneten E; keinerlei Rechte bezüglich AT und AW sind hierfür vonnöten; keinerlei Rechte auf untergeordnete E, die hierdurch ihren DN ändern sind vonnöten!	n.v.	n.v.
Import	erlaubt die Einfügung eines E an dieser Stelle im DIT	n.v.	n.v.
ReturnDN	erlaubt den DN eines E als Ergebnis einer Operation zurückzugeben	n.v.	n.v.
Disclose on Error	erlaubt eine Fehlermeldung als Ergebnis einer Operation zurückzugeben, die das Vorhandensein eines E verrät	n.v.	n.v.

Einfache Authentifizierung



A = DN des Benutzers
$passw^A$ = Passwort von A
t^A = Zeitstempel
q^A = Zufallszahl
f = gerichtete Funktion

Strenge Authentifizierung mit asymmetrischer Verschlüsselungstechnik

- Asymmetrische Verschlüsselung basiert auf zwei Schlüssel:
  - Privater Schlüssel, *Secret Key*, Xs, dient zur Entschlüsselung.
  - Öffentlicher Schlüssel, *Public Key*, Xp, dient zur Verschlüsselung.
- Für Xs und Xp gelten folgende Regeln:
  - Xp wird nach einem bestimmten Algorithmus (z.B. RSA) aus Xs errechnet
  - Aus Xp kann aber nicht Xs errechnet werden
- Eine Entschlüsselung kann folgendermaßen dargestellt werden:
  - D = Xs[Xp[D]]

Anwendungen von assymetrischer Verschlüssellung

- PEM (*Privacy enhancement for Internet Electronic Mail*)
- ODIF (*Office Document Interchange Format*)
- EDI (*Electronic Data Interchange*)

- Mit assymetrischer Verschlüssellung können Signaturen erstellt werden.
- Solche Signaturen bestätigen:
  - Benutzeridentität
  - Unversehrtheit der signierten Daten

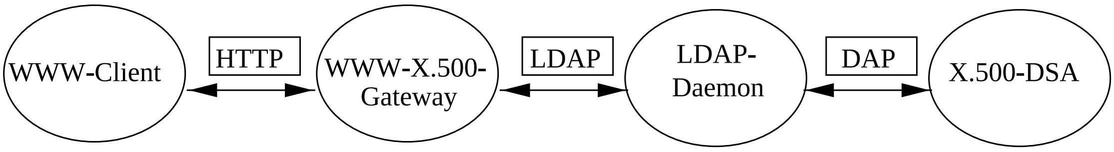
Zertifizierung im X.500

- CA (*Certificate Authority*) ist eine vertrauenswürdige Stelle, die im DIT abgebildet werden kann.
- CA überprüft Zugehörigkeit von *Public Key* und Person: Identität.
- CA überprüft Eindeutigkeit des DNs eines Benutzers: X.500.
- CA signiert *Public Key* des Benutzers: erstellt Zertifikat.
- CA sorgt für Veröffentlichung der zertifizierten *Public Key* im X.500
- CA verwaltet CRLs *Certificate Revocation Lists*) und veröffentlicht sie im X.500, um ungültig gewordene Zertifikate bekanntzugeben.
- CAs können in einer CA-Hierarchie stehen. Eine übergeordnete CA zertifiziert eine untergeordnete.
- An der Spitze eines solchen CA-Baumes steht eine PCA (*Policy Certification Authority*), die für die untergeordneten CAs eine *Security Policy* festlegt.

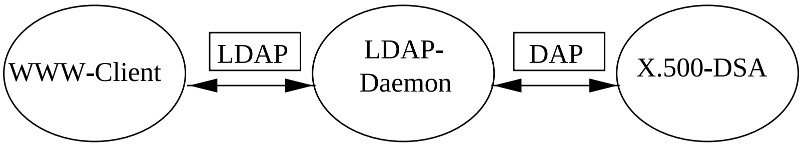
Verantwortlichkeiten bei der Verwaltung

- Die Daten des DIT werden in *Administrativ Areas* (AA) aufgeteilt für die bestimmte Verantwortlichkeiten festgelegt werden können:
  - *Naming Administration*: Hier werden Regeln festgelegt über den Inhalt von namensrelevanten Attributen, also Namenskonventionen, Regeln zur Vermeidung von Doppelnamen etc.
  - *Subschema Administration*: Hier wird festgelegt, welche Information in der AA abgelegt werden kann und welche Attribute zur Bildung der DNs verwendet werden.
  - *Security Administration*: Hier werden alle Zugriffsrechte definiert.
  - *Collective Attribute Administration*: Hier werden die Inhalte der bereits erwähnten *Collective Attributes* festgelegt.
- Für alle diese Funktionen können *Policies* erstellt und Personen als verantwortlich bestimmt werden.

Integration in das WWW



- Web500gw (Web-X.500-Gateway), Frank Richter, TU-Chemnitz
- TWEB (Tübinger Webgateway), Kurt Spanier, Universität Tübingen
- WWW entwickelt sich zu dem alleinigen Benutzer-Zugang zu X.500
- Durch das Gateway eine geordnete Datenbank im WWW-Chaos
- Alle Vorteile von X.500 bleiben erhalten.

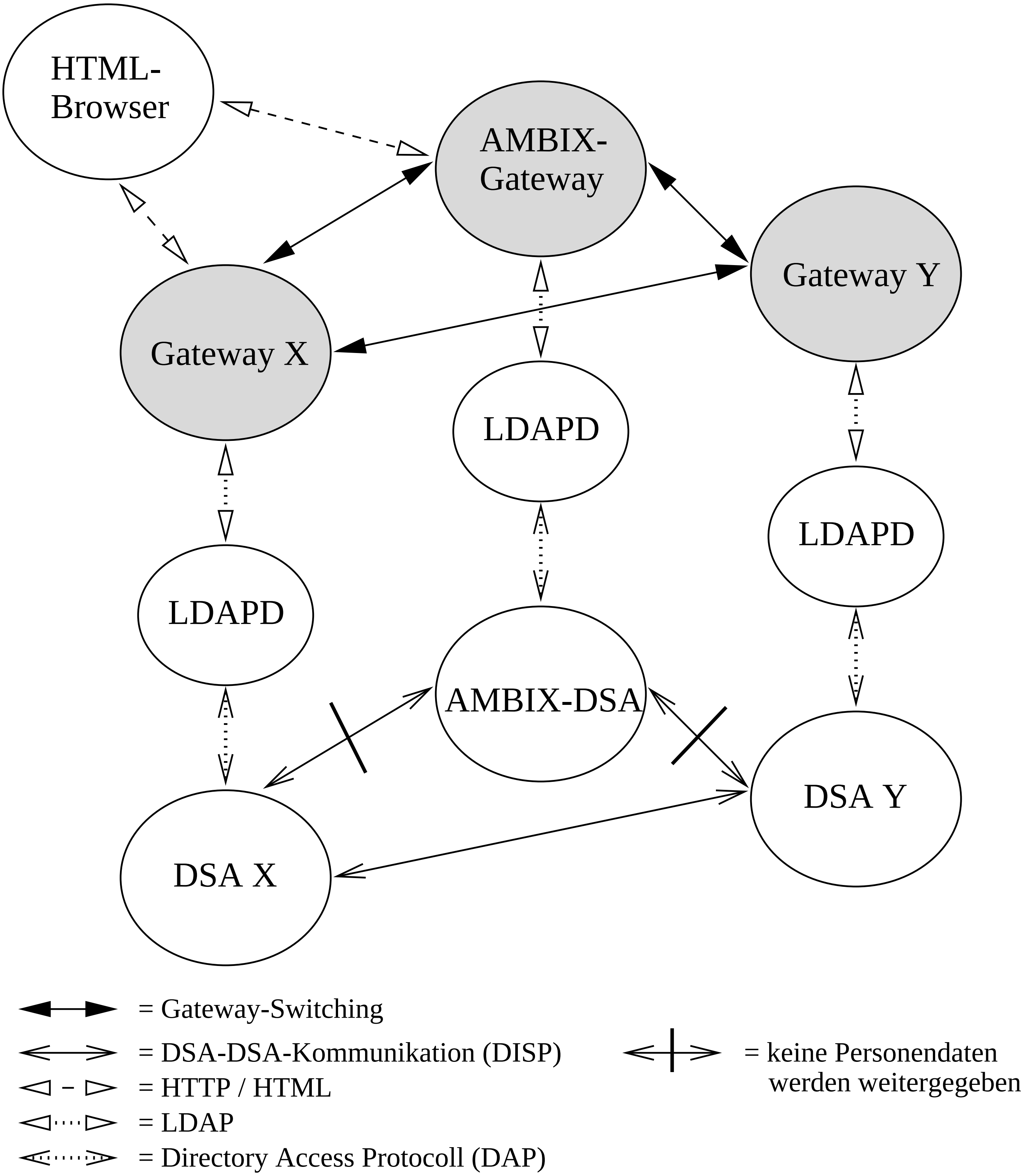


- viele Softwarehersteller kündigen die Unterstützung von LDAP an, u.a. Netscape, Microsoft, AT&T

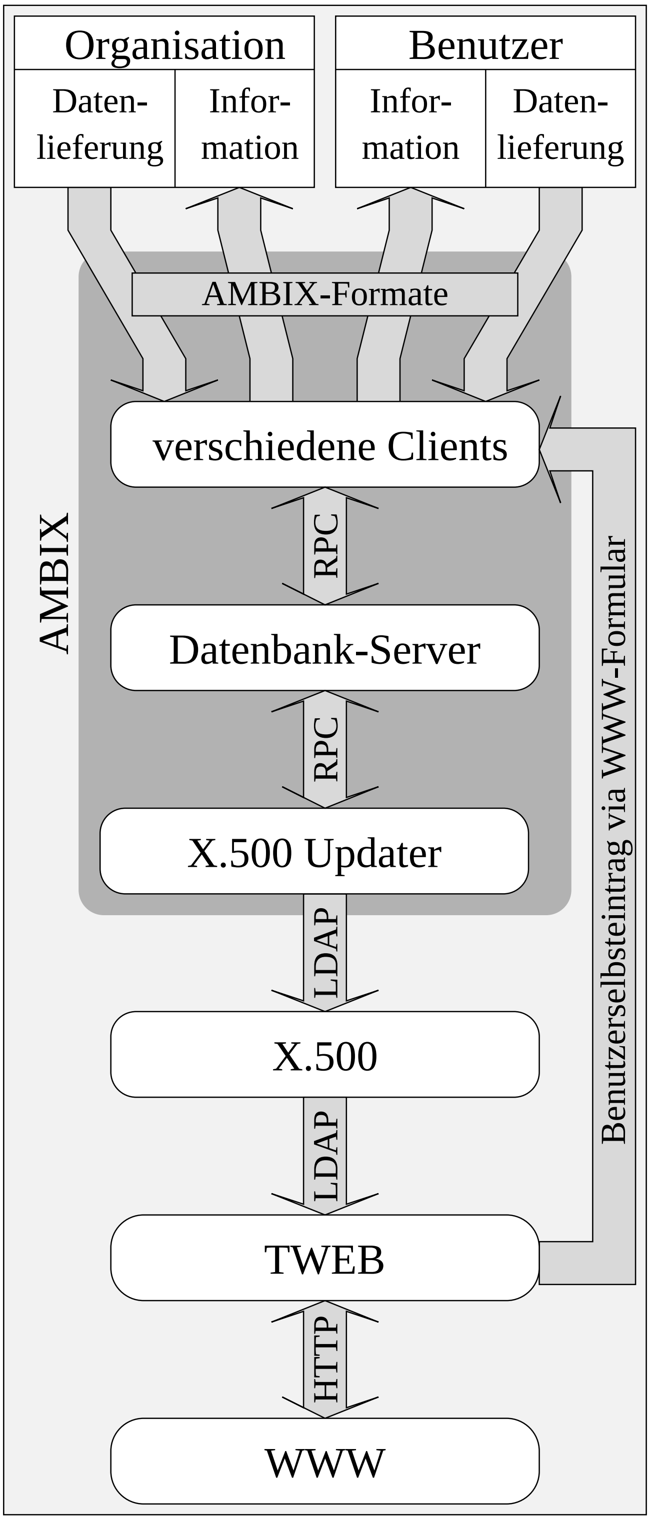
TWEB - Konfigurierung

- Technische Konfigurierung (Zuordnung LDAPDaemon/DSA, Gateway Basisport, etc.)
- Gestalterische Konfigurierung (Darstellung der Attribute, selektive Ausgabe, sprachspezifische Texte, etc.)
- Politische Konfigurierung (Zugriffskontrolle, Modify-Zugriff, Listenbeschränkgungen, Erklärungstexte, etc.)

Gateway-Switching



AMBIX als Brücke zum X.500



Aufgaben von Directory Diensten

- Informationen zu Personen (White Pages) und Organisationen (Yellow Pages)
- Benutzerverwaltung
- Authentifizierung von Benutzern
- Definition von Zugriffsrechten
- Veröffentlichung von Public-Keys und Zertifikaten
- Auffinden von Resourcen im Netz (Drucker, Rechner, Dateien, ...)
- Speicherung und Veröffentlichung beliebiger sonstiger Information

„Directory-enabled computing will be the most significant network technological issue ... over the next three to five years“ (Jamie Lewis, Präsident der Burton Group, eine „research firm focused solely on the analysis of networking computing technology“)

Directory-Produkte für Windows NT

Hersteller	Client	Server	LDAP	API
Netscape	LDAP-Client in Communication Suit; Navigator	Directory Server	ja	Directory SDK für C und Java
Micro $oft	Internetexplorer 3.0	Active Directory	ja	AD Service Interface
IBM		DCE based Directory	ja	
Banyan		StreetTalk (urspr. Teil von VINES)	ja	
Novel		NDS (urspr. Teil von Netware)	ja	Java Class Library
NetVision		Synchronicity (NT-Verwaltung via NDS	?	
Zoomit	Compass	VIA („Metadirectory“)	ja	
SUN			ja	
HP			ja	
SGI			ja	
AT&T			ja	
Oracle			ja	

Directory-Politik der Hersteller

- Alle Hersteller sehen die Bedeutung von Directory-Diensten im Intra- und Internetbereich.
- Alle erkennen an, daß X.500 alle Anforderungen erfuellt.
- Alle halten LDAP für den besten Weg zu X.500.
- Wie bei HTML sind sowohl Micro $oft als auch Netscape „heavily committed“
  - Beide bekennen sich zu den LDAP-RFCs
  - Beide suchen Kontakt zur entsprechenden IETF (asid)
  - Beide machen eigene Vorschläge für LDAP v3 (z.B. SSL gesicherte Kommunikation)
  - Der Unterschied:
    * Netscape macht LDAP zur Basis seines Directory Servers
    * (Netscape hat den LDAP-Autoren Tim Howes eingekauft)
    * Micro $oft stellt ein Gegenmodell zu der „komplexen low-level-c-Schnittstelle“ LDAP auf: Das „wesentlich einfacher verwendbare“ Active Directory Service Interface (ASDI)
    * Von den zwei *White Papers* zu ASDI beschäftigt sich eins nur mit der Integration von LDAP.

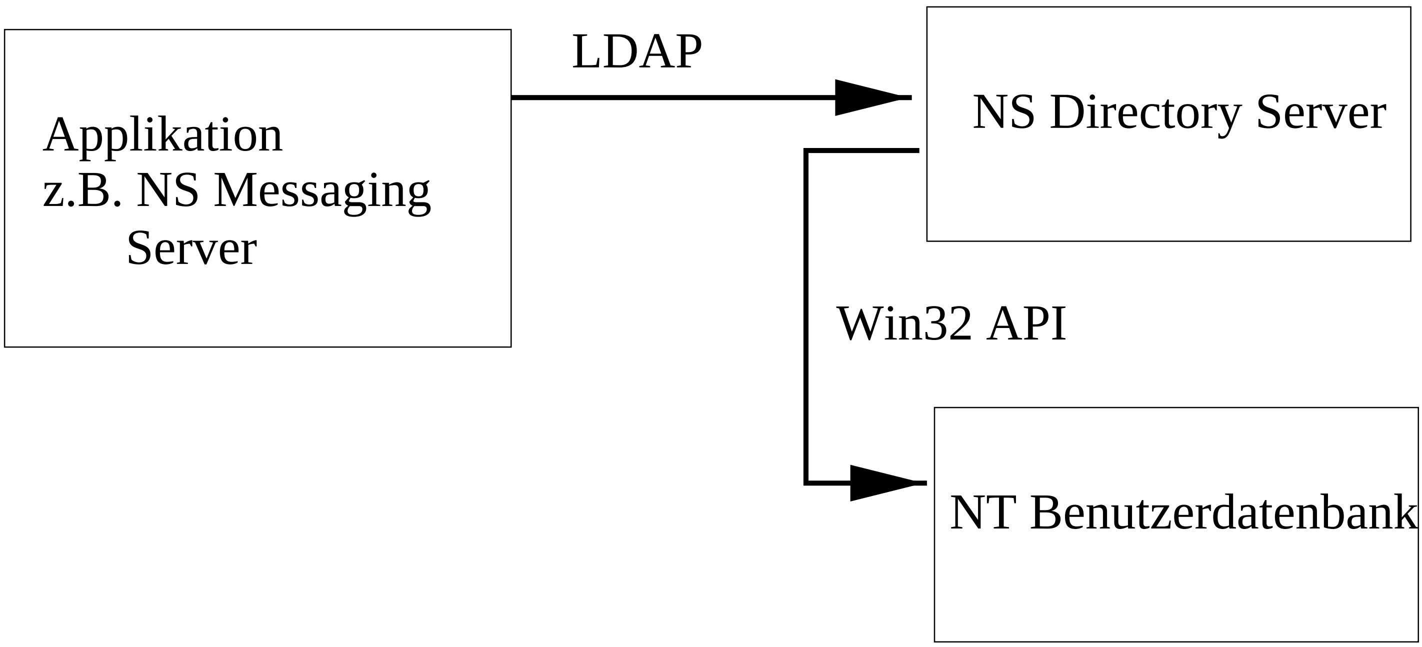
LDAP die Zukunft von X.500?

LDAP wird zunehmend von Softwarefirmen unterstützt. Es setzt sich defacto als der Directory Standard durch. Dies liegt an fogenden Eigenschaften von LDAP:

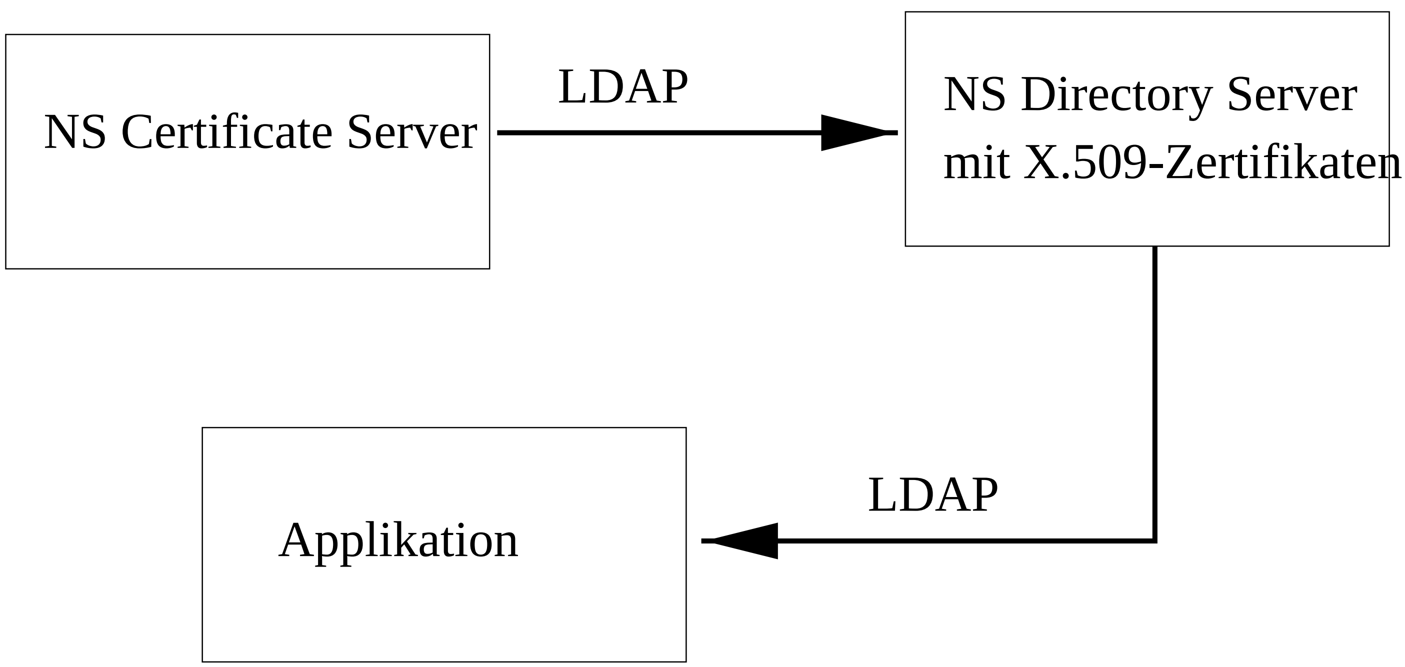
- Das X.500 Datenmodell wird abgebildet.
- Einfachere Schnittstelle fuer DUAs.
- Einfache String-Codierung der Protokoll-Daten-Elemente
- Alle wichtigen Operationen können durchgeführt werden.
- LDAP läuft direkt unter TCP (kein resourcenschluckender OSI-Stack).
- LDAP ist durch eine Reihe von RFCs als Internetstandard anerkannt.
- Durch SLAPD vollständiges Client / Server-Modell
- Einbindung der DSA-DSA-Protokolle DSP und DISP ist in Arbeit
- Netzsicherheitsfeatures (SSL) in Arbeit

Serverkonzept von Netscape: z.B. Authentifizierung

Einfache Authentifizierung

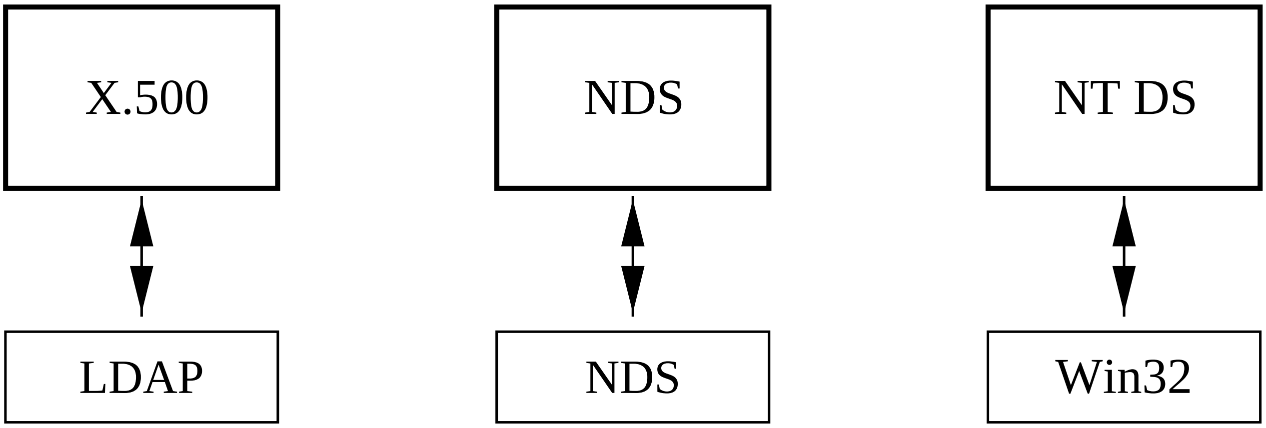


Strenge Authentifizierung über Zertifikate



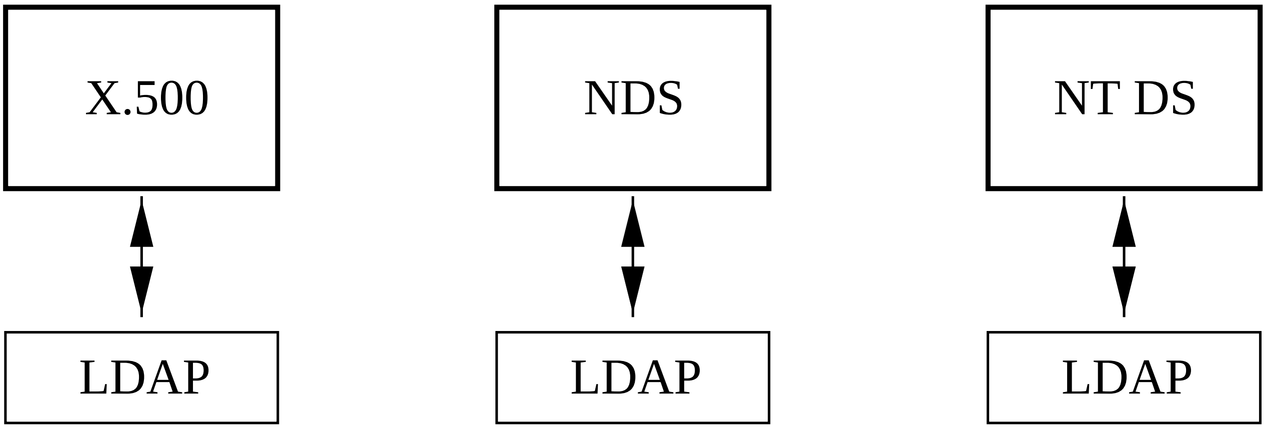
Drei Directory Szenarien, I

Heute: verschiedene APIs für verschiedene Directories:



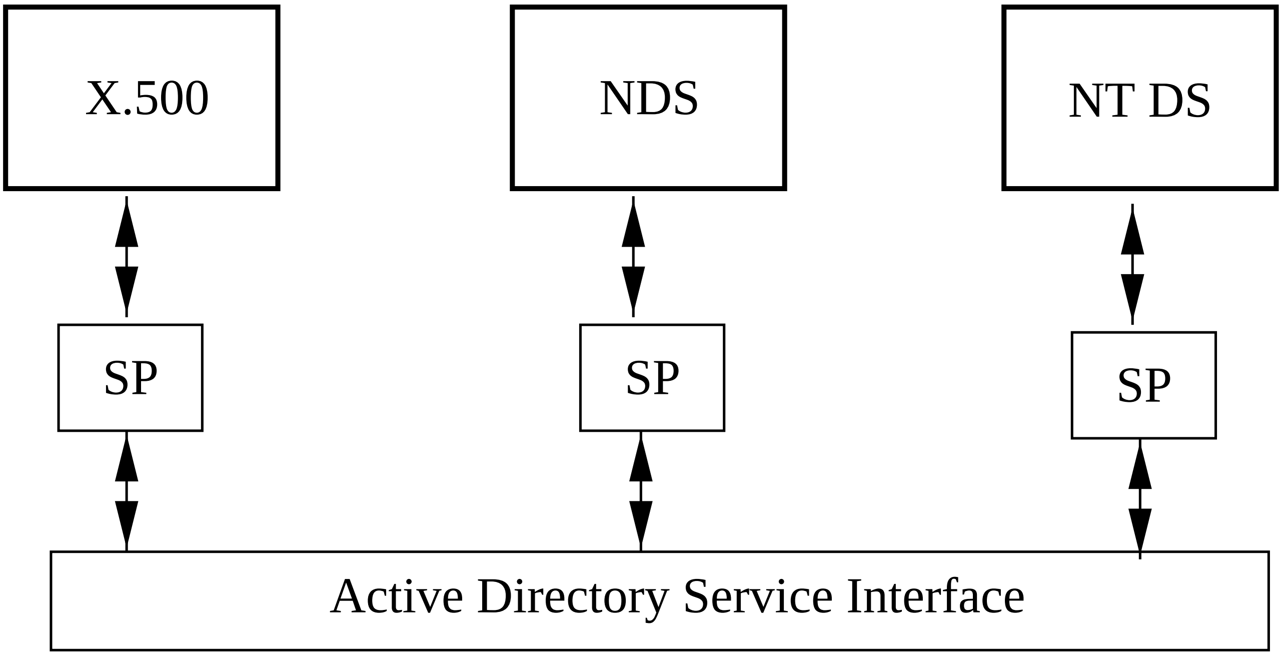
Drei Directory Szenarien, II

Augenblickliche Entwicklung: LDAP als Standard-API:



Drei Directory Szenarien, III

Micro $ofts Traum:



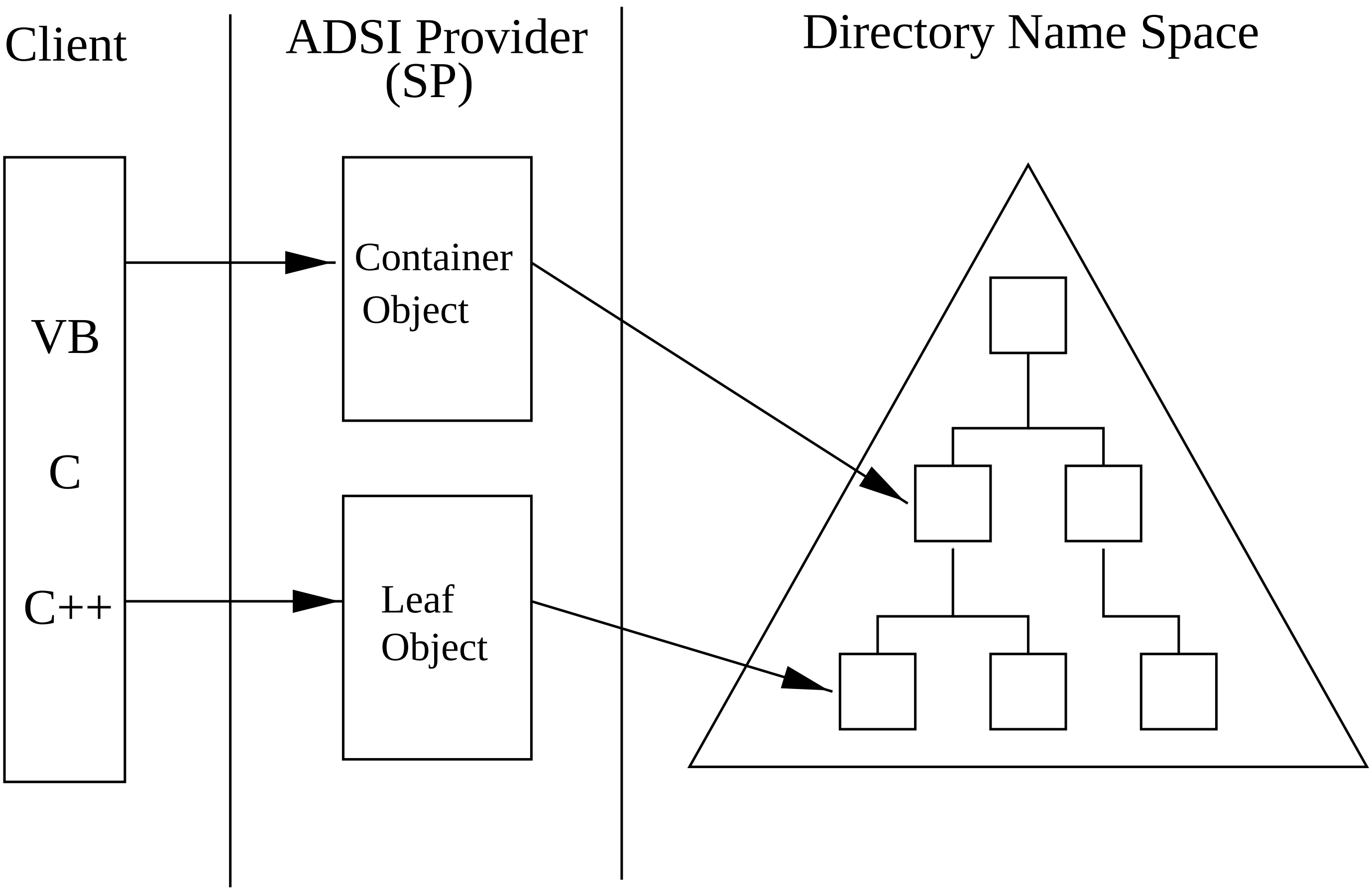
SP = Server Provider

ADSI: *Active Directory Service Interface*

- „Metadirectory“, das verschiedene Proprietäre Directory-Dienste integriert.
- Soll intergrierte Bestandteil von Win NT 5.0 sein und die Registry ersetzen.
- Verwaltet NT Objekte wie Domains, User, Global Groups, Registry etc.
- Unterstützt LDAP als eine der Server Provider
- Ebenfalls von M$ vordefiniert: Server Provider für Win NT, NDS und Lotus Notes.
- In Aussicht gestellt Server Provider für die DSA-Protokolle DSP und DISP
- Sprachunabhängig (OLE: VB, C++, Java, Perl)
- QueriSoft bietet eine auf ADSI basierende Scriptsprache
- Teil von ODSI (*Open Directory Service Interface*)
- Konzept ähnelt sehr dem X.500

ADSI Objekte

- ADSI Objekte sind *Common Object Modell* (COM) konform.
- COM wurde als Brücke zwischen Windows und Unix entwickelt.
- COM-Objekte werden mittels Standard OLE-Prozeduren programmiert.
- ADSI-Objekte sind Baumartig gegliedert.
- Es werden Container Objects und Leaf Objects unterschieden:



ADSI und X.500

Die verschiedenen Objektarten haben Entsprechungen
in der X.500 Welt:

ADSI	X.500
Schema Management Objects	Administrative Areas
Class Container Object	Object Class
Property	Attribute Type
Syntax	Attribute Syntax
ADSPathString	Distinguished Name (DN)

ADSI - vordefinierte Standardobjekte

Auch die vordefinierten Standardobjekte haben zum Teil wörtliche Entsprechungen(*):

- Namespace
- Country *
- Locality *
- Organization *
- OrganizaionalUnit *
- Domain
- Computer
- User
- Group
- Alias
- Service
- Printqueue
- Print Device
- Print Job
- File Service
- Session
- Resource

ADSI - Perspektiven

- Viele Hersteller haben Unterstützung von ASDI signalisiert.
- M$ wirbt mit der Plattform- und Herstellerunabhängigkeit.
- Entwickler werden aber an das proprietäre ADSI gebunden.
- Weitere Server Provider können von jedermann definiert werden.

Literaturverzeichnis

- Directory Services Tomorrow. - PC Magazine 21. Januar 1997
- Gietz, et.al.: X.500 für alle - Das DFN–Projekt AMBIX / Gietz. K.-P.; Schneider, R.; Spanier, K. - In: DFN Mitteilungen, Heft 42, November 1996
- Gietz, K.-P.: Sicherheitsaspekte im X.500 und im Projekt AMBIX / In: DFN-Bericht: Workshop „Sicherheit in vernetzten Systemen“, 4.-5. März 1997, Hamburg, DFN-CERT (Hrsg.), in Vorbereitung.
- Micro Soft White Paper: Microsoft Active Directory Service Interface: ADSI - Open Interfaces for Managing and Using Directory Services. - 1996
- Micro Soft White Paper: Active Directory Service Interfaces: The Easy Way to Access and Manage LDAP-Based Directories. - 1997
- Netscape White Paper: An Internet Approach to Directories. - 1997
- RFC 1684 Introduction to White Pages Services based on X.500 / Jurg, P. - August 1994
- RFC 1777: Lightweight Directory Access Protocoll / Yeong, W.; Howes, T.; Kille, S. - März 1995
- RFC 1778: The String Representation of Standard Attribute Syntaxes / Howes, T.; Kille, S.; Yeong, W. - März 1995
- RFC 1779: A String Representation of Distinguished Names / Kille, S. - März 1995
- RFC 1804: Schema Publishing in X.500 Directory / Mansfield, G.; Rajeev, P.; Raghavan, S.; Howes, T. - Juni 1995
- RFC 1823: The LDAP Application Program Interface / Howes, T.; Smith, M. - August 1995
- Steedman, D.: X.500 - The Directory Standard and its Application / Steedman, Douglas. - Twickenham: Technology Appraisals LTd, 1993
- Waugh, A.: X.500 and the 1993 Standard - Technical Report TR-SA-94-03 / Waugh, Andrew. - CSIRO Division of Information Technology, 1994
- [X.500 (1993)] The Directory: Overview of Concepts, Models, and Services - Recommendation X.500 ISO/IEC 9594-1 / Information Technology; Open Systems Interconnection. - 1993
- [X.501 (1993)] The Directory: Modells - Recommendation X.501 ISO/IEC 9594-2 / Information Technology; Open Systems Interconnection. - 1993
- [X.509 (1993)] The Directory: Authentication Framework - Recommendation X.509 ISO/IEC 9594-8 / Information Technology; Open Systems Interconnection. - 1993
- [X.511 (1993)] The Directory: Abstract Service Definition - Recommendation X.511 ISO/IEC 9594-3 / Information Technology; Open Systems Interconnection. - 1993