Sicherheitsaspekte im X.500 und im Projekt AMBIX

Vortrag für den Workshop
„Sicherheit in vernetzten Systemen“
am 4. und 5. März 1997 in Hamburg

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

Gliederung

1 Security im X.500

- 1.1 Einführung in X.500
  - 1.1.1 Aufbau und Struktur
  - 1.1.2 Verantwortlichkeiten der Verwaltung
  - 1.1.3 Zugriffsmöglichkeiten auf das X.500
- 1.2 Zugriffskontrollen im X.500
- 1.3 X.509 - Authentifizierungsmechanismen
  - 1.3.1 Einfache Authentifizierung
  - 1.3.2 Strenge Authentifizierung mittels *Public Keys*

2 Security im Projekt AMBIX

- 2.1 Das DFN-Projekt AMBIX
- 2.2 Datenschutzrechtliche Grundlage
- 2.3 Implementierung der Zugriffsbeschränkungen
  - 2.3.1 Zugriff von anderen DSAs bzw. DUAs
  - 2.3.2 Zugriff über das AMBIX WWW-X.500-Gateway
  - 2.3.3 Angriffe auf die AMBIX-Rechner
- 2.4 Authentifizierung von Datenlieferungen
  - 2.4.1 Organisationslieferungen
  - 2.4.2 Benutzerinteraktion
- 2.5 *Public-Key* -Verwaltung

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.

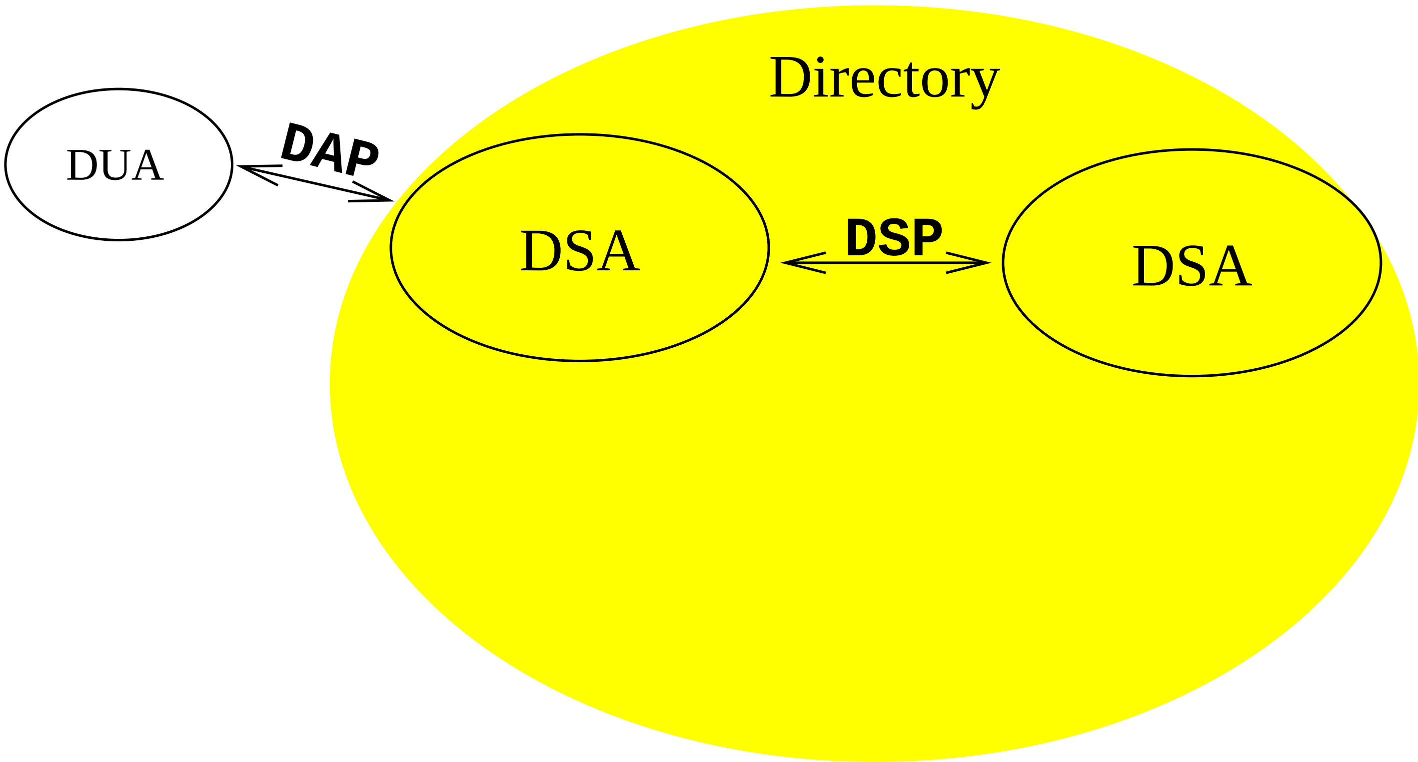
X.500 - Standards

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 in Planungsphase	X.509v3

Das Client-Server-Modell

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

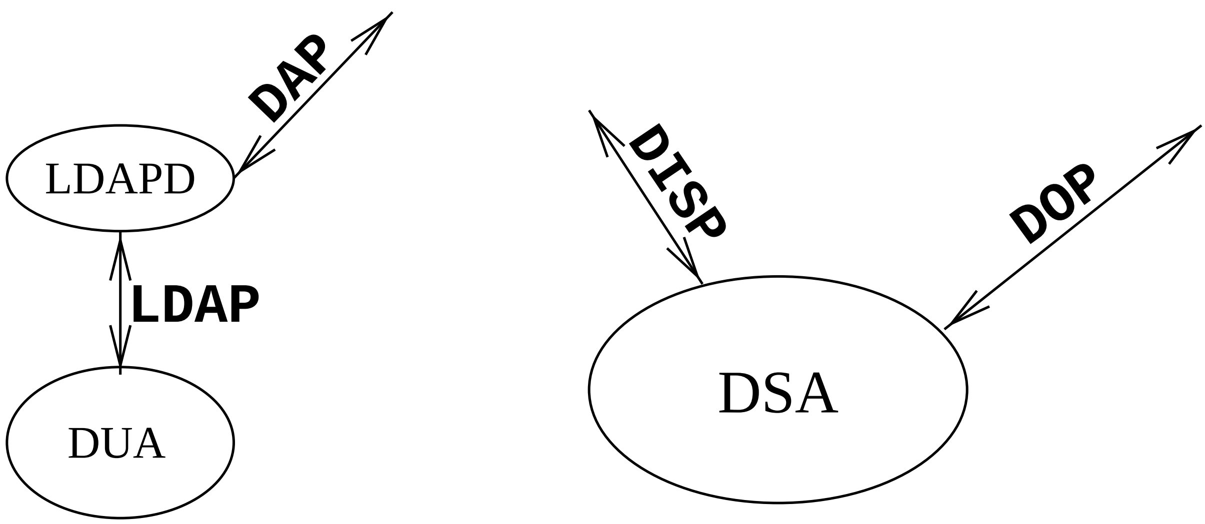
- DUA (*Directory User Agent*) über DAP (*Directory Access Protocol*)



Das Client-Server-Modell

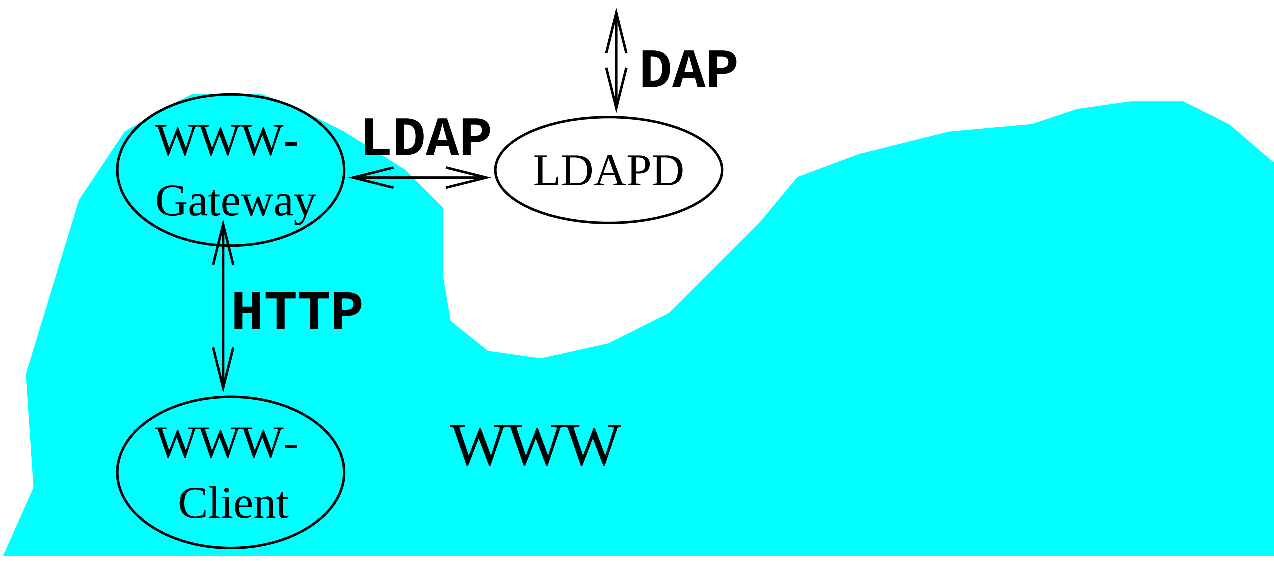
- DSA mit DISP (*Directory Information Shadowing Protocol*) und
- DOP (*Directory Operational Binding Management Protocol*)

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



Das Client-Server-Modell

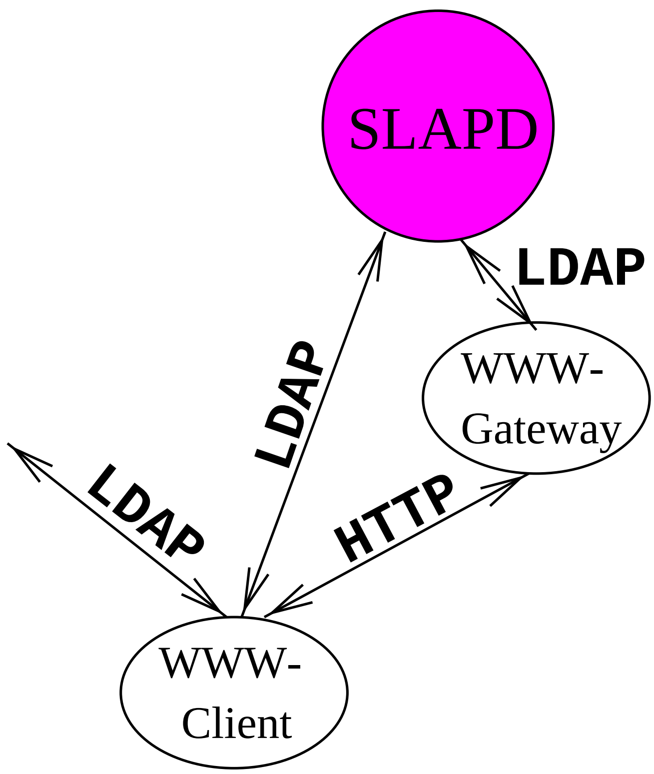
- WWW-X.500-Gateway über LDAP



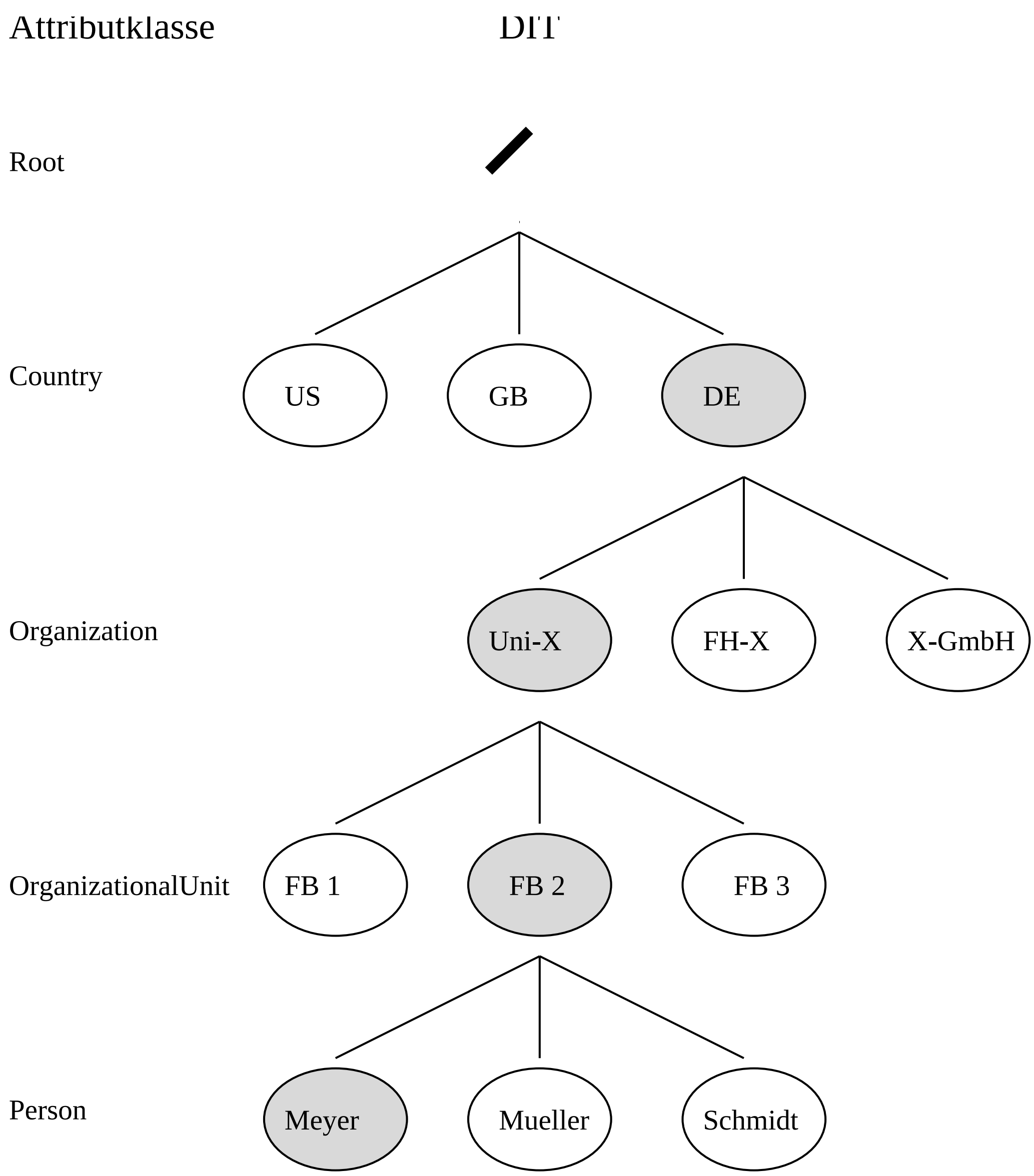
Das Client-Server-Modell

- SLAPD (*Standalone LDAP Directory Server*)

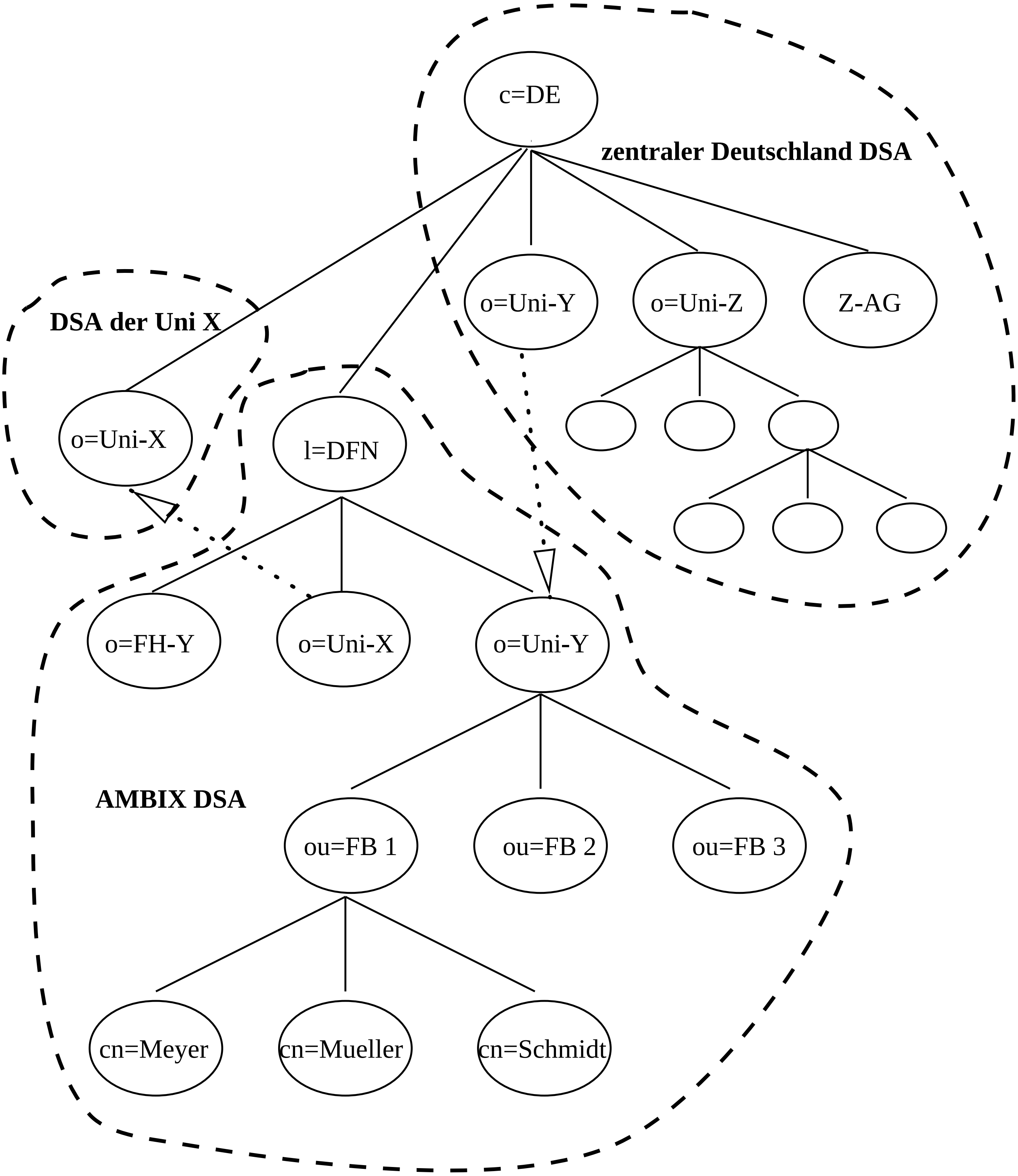
- WWW-Client über LDAP



Der *Directory Information Tree (DIT)*



Verteilung des DITs auf die DSAs



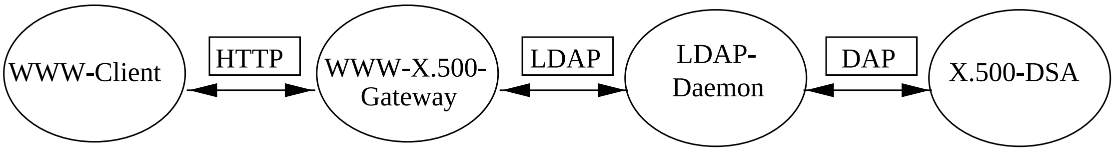
Bestandteile des X.500

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.	Identifizierungs-schlüssel
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

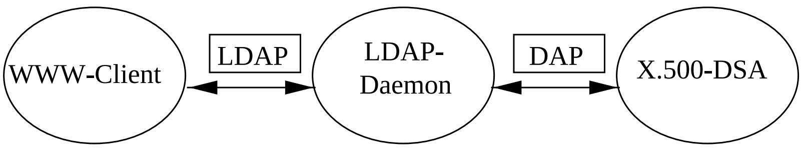
Verantwortlichkeiten der Verwaltung

- 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.)

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

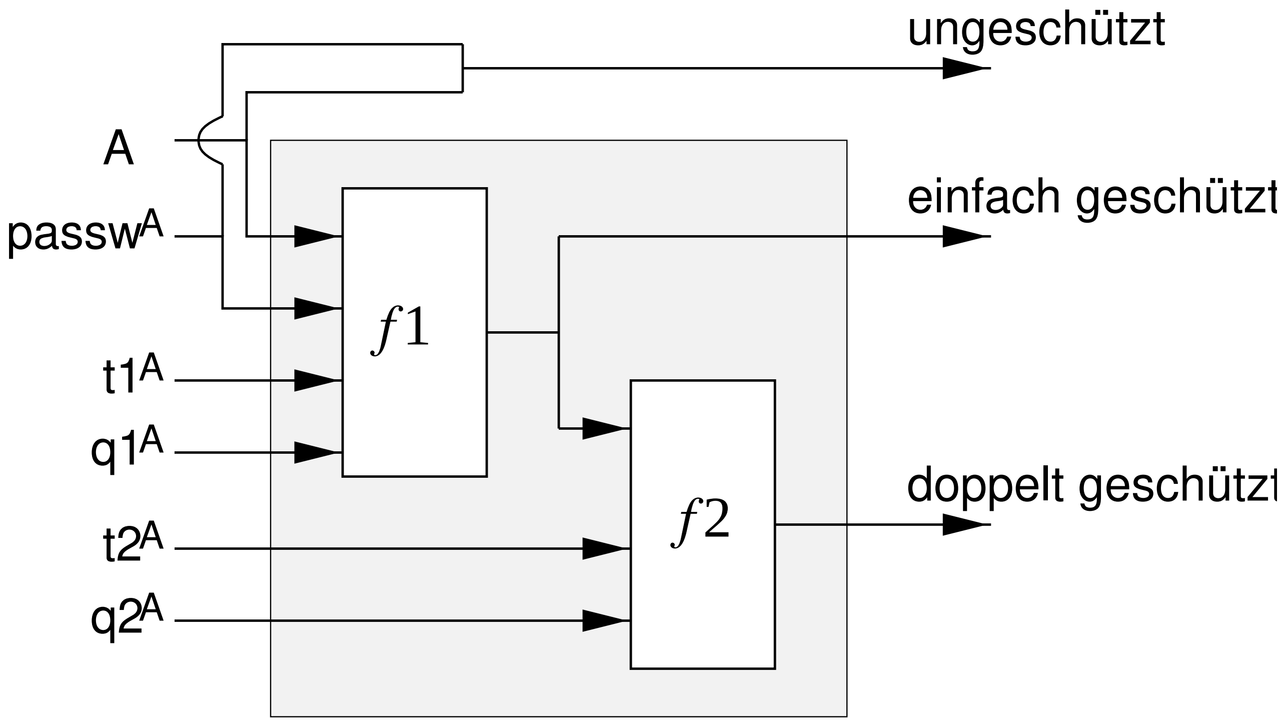
Basic Access Control Scheme III

- 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 List*s) 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.

SecuDE

- Mit SecuDE hat die Gesellschaft für Mathematik und Datenverarbeitung (GMD) Sicherheitsfunktionalität auf der Basis von X.509 zur Verfügung:
  - Programmierschnittstelle (API)
  - Libraryroutinen
  - Hilfswerkzeugen

DFN-Projekt AMBIX

AMBIX

(**A**)ufnahme von (**M**)ail-(**B**)enutzern (**i**)n das (**X**).500-Directory

Datenschutzproblematik

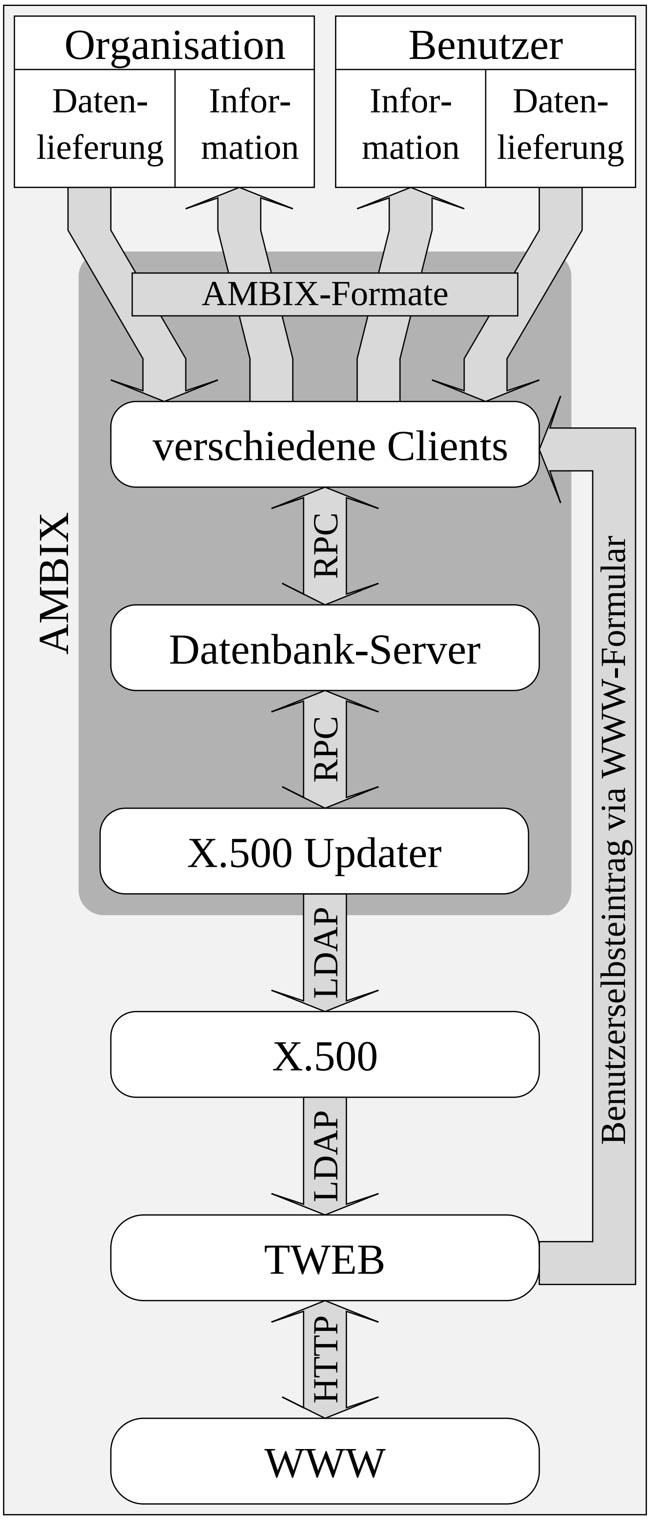
- Interessenkonflikt:
  - Mitarbeiterverzeichnis
  - Datenschutzinteresse der Betroffenen
- Hauptproblem: Werbung durch E-Mail
- Ursprünglicher Minimalset von Daten:
  - Organisationszugehörigkeit
  - Name und akademischer Titel
  - Telefon- und Faxnummer
  - E-Mail-Adresse
- Geplante Erweiterung des Minimalset (ausschlißlich freiwillige Angaben):
  - Arbeitsgebiet
  - URL der *Home Page*
  - *Public keys* für asymmetrische Verschlüsselung, bzw. deren Zertifikate

Die AMBIX-Maschine

Netzwerkfähige Client-Server-Architektur

- Eingabe
  - Struktur- und Personendatenmeldungen von Organisationen
  - Datenänderungen von Organisationen
  - Datenlieferungen von WinShuttle
  - Selbsteinträge per WWW-Formular
  - Widerspruch, Zustimmung und Datenänderungen von Betroffenen durch E-Mail-Formular
- Verarbeitung
  - alle Daten werden formal überprüft
  - E-Mail-Adressen werden zusätzlich regelmäßig gecheckt
  - Telefon- und Faxnummern werden in einheitliches Format konvertiert
  - alle Vorgänge werden protokolliert
- Ausgabe
  - Fehlerprotokolle der Datenlieferungen
  - von Organisationen gemeldete Personen werden angeschrieben und informiert
  - fehlerhafte Datenänderungsversuche durch Betroffene werden beantwortet
  - die Selbsteinträgerdaten werden den Organisationen gemeldet
  - die Daten werden ins X.500 einspeist bzw. aktualisiert

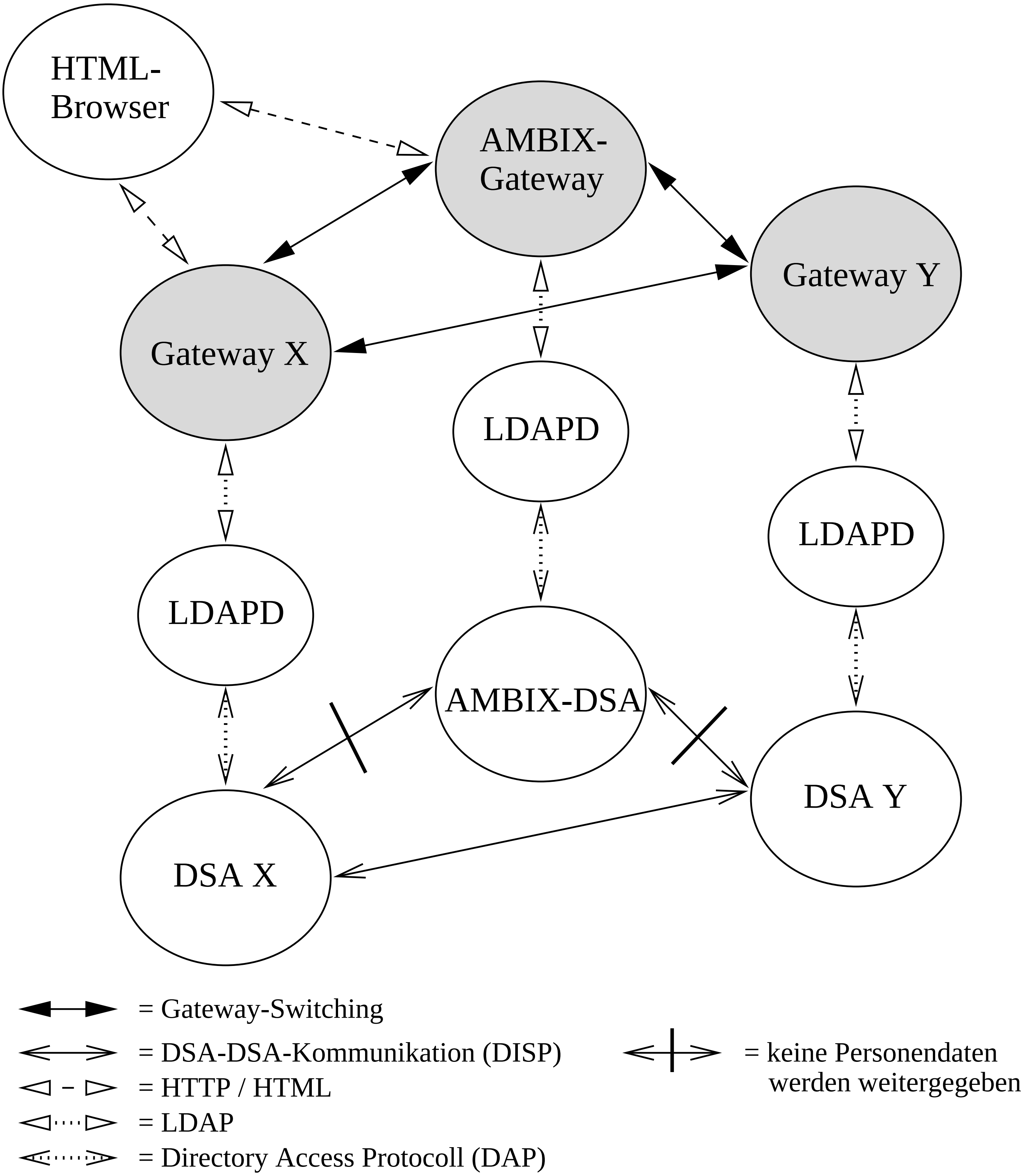
AMBIX als Brücke zum X.500



Zugriffsbeschränkungen bei den AMBIX-Daten

- Organisationsstrukturdaten werden ohne Beschränkung weitergegeben
- Personendaten müssen vor unberechtigtem Zugriff geschützt werden:
  - Zugriffe von anderen DSAs werden abgewiesen
  - Zugriffe von anderen DUAs werden abgewiesen
  - Zugriffe von fremden WWW-Gateways werden abgewiesen
  - Ausschließlich das AMBIX-TWEB erhält Zugriff auf Personendaten
- Das AMBIX-TWEB hat folgende Zugriffsbeschränkungen für Personendaten:
  - Nicht an Rechner, die nicht im DNS (*Domain Name Service* eingetragen sind.
  - Nicht an Rechner, deren Toplevel-Domain keinem Land entspricht (z.B.: „.com“ und „.net“).
  - Nicht an Rechner, deren Toplevel-Domain einem Land entspricht, in dem kein adäquater Datenschutz betrieben wird.
  - Nicht an Roboter, die das *Robot Exclusion Protocoll* (REP) befolgen.
  - Nicht an Roboter, die nicht das REP befolgen, erkennbar durch:
    - regelmäßiger Zugriff
    - häufiger Zugriff
    - Eintrag der entsprechenden Domain im TWEB-Konfigurationsfile

Gateway-Switching



Sicherung gegen Angriffe auf die AMBIX-Rechner

- Sicherung der RPC-Schnittstelle der projektinternen Client/Server Kommunikation
- TCP-Wrapper zur Zugriffskontrolle und Überwachung auf TCP-Ebene: telnet, rlogin, remsh, rexecd, etc.
- Secure Shell, um ein sicheres *remote login* mit Authentifizierung über RSA-Verschlüsselungstechnik und eine ebenso sichere Tunnelung der X.11-Verbidung zu erreichen.
- Portmapper zur Zugriffskontrolle und Überwachung auf Port-Ebene: alle RPC-Dienste.
- Logsurfer, mit dem alle sicherheitsrelevanten Logfiles automatisch ausgewertet werden können.

Authentifizierung von Datenlieferungen

- Datenlieferungen durch die Organisationen
  - Für jede Organisation wurde mindestens ein(e) Administrator(in) bei AMBIX registriert.
  - Administrator(in) identifiziert sich durch E-Mail-Adresse und Passwort.
  - Verifizierung und Verschlüsselung der Daten durch *Public-Key*-Verfahren ist in Planung.
- Benutzerinteraktion
  - Jede(r) gemeldete Benutzer(in) erhält an die registierte E-Mail-Adresse ein Daten-Änderungs-Formular zugeschickt.
  - Im Formular ist eine mit einer komplexeren Prüfsumme versehene Personenidentifikationsnummer eingetragen.
  - Diese Nummer wird zur Authentifizierung verwendet.
  - Daten werden auf formale Kriterien hin überprüft.
  - Verifizierung und Verschlüsselung der Daten durch *Public-Key*-Verfahren ist in Planung.

Sicherheitsprobleme

- Problem: Ein Benutzer überschreibt mit dem Formular eines Anderen dessen Daten mit seinen eigenen.
- Lösungsansatz: Keine gleichzeitige Änderung von Vor- und Nachnamen möglich.

- Problem: Ein Benutzer trägt via Selbsteintrag unsinnige Daten ein.
- Lösungsansatz: Alle Daten werden formal überprüft und zusätzlich zur Kontrolle an zuständige(n) Administrator(in) geschickt.

- Problem: Ein Benutzer trägt via Selbsteintrag einen Anderen ein, jedoch mit eigener E-Mail-Adresse, um E-Mails an den Anderen abzufangen.
- Lösungsansatz: Überprüfung durch Administrator(in). Verhinderung durch korrekten Eintrag via Organisationsdatenlieferung.

- Generell werden alle gemeldete E-Mail-Adressen angeschrieben, wobei:
  - Jede Datenänderung angezeigt wird;
  - mit Fehlermeldung zurückkommende Mails automatisch zur Löschung der E-Mail-Adresse führen.

Verwaltung von *Public-Keys* und deren Zertifikate

- In Zusammenarbeit mit der DFN-PCA an der Universität Hamburg sollen über AMBIX *Public-Keys* und deren Zertifikate verwaltet werden.
- Folgende Regeln wurden vereinbart:
  - Durch CAs zertifizierte Schlüssel werden grundsätzlich nur von registrierten CAs bzw. der DFN-PCA an AMBIX geliefert.
  - Zertifikate werden generell nur von solchen CAs angenommen, die sich in der Zertifizierungshierarchie unterhalb der DFN-PCA befinden.
  - Benutzer(innen) und Organisationsadministrator(inn)en (OAs) dürfen eigene, unzertifizierte (bzw. selbst-zertifizierte) Schlüssel ins X.500 eintragen.
  - CAs und OAs dürfen nur Einträge löschen, die kein gültiges Benutzer- oder CA-Zertifikat mehr enthalten. Einmal veröffentlichte CA-Zertifikate dürfen frühestens nach Ablauf der Gültigkeitsdauer aus dem X.500 entfernt werden, auch wenn ein Zertifikat zwischenzeitlich widerrufen wurde.
  - Benutzer(innen) dürfen nach wie vor jederzeit ihren eigenen Eintrag löschen lassen, auch wenn dieser ein noch gültiges Zertifikat enthält.
  - Ändert sich der DN eines eingetragenen Benutzers, ist der zuständige OA zu benachrichtigen.

Literaturverzeichnis

- 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

- Kossakowski, K.-P.: Sicherheit im Deutschen Forschungsnetz / Kossakowski, K.-P. - In: Workshop „Sicherheit in vernetzten Systemen“ DFN-Bericht Nr. 75, 1994

- Directory Security - Mechanisms and Practicality / North American Directory Forum (NADF), DF-479/SD-11, 1993

- Schneider, W.: SecuDE - Overview, Version 4.0 / Schneider, Wofgang. - Darmstadt: Gesellschaft für Mathematik und datenverarbeitung (GMD), 1992

- Schneider, W.: PASSWORD - Ein EG-Projekt zur pilotmäßigen Erprobung von Authentisierungsdiensten / Schneider, Wolfgang.- Gesellschaft für Mathematik und Datenverarbeitung (GMD), o.j.

- Waugh, A.: X.500 and the 1993 Standard - Technical Report TR-SA-94-03 / Waugh, Andrew. - CSIRO Division of Information Technology, 1994

- Steedman, D.: X.500 - The Directory Standard and its Application / Steedman, Douglas. - Twickenham: Technology Appraisals LTd, 1993

- [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

Kontakt

- E-Mail: ambix-d@mail500.uni-tuebingen.de
- URL: http://ambix.uni-tuebingen.de