AMBIX

Unterstützung elektronischer Kommunikation im DFN

Dr. Ralf Schneider
DFN–Projekt AMBIX
Zentrum für Datenverarbeitung
Universität Tübingen

GUUG–FJWS97

X.500 ?

X.500 – Ein OSI–Standard

- Mechanismus zur weltweiten Verteilung von Daten
- Directory–Service
- standardisiert von internationalen Normierungsgremien
  - – praxisfern
  - – geringe Akzeptanz (anfänglich)
  - – Komplexität
  - + konform mit OSI *(Open Systems Interconnection)*
  - + einheitliches und objektorientiertes Konzept
  - + modernes Design

Internationale Gremien

Normierungsgremien:

ISO: *International Standard Organisation*, Vereinigung der nationalen Normierungsgremien

CCITT: *Comité Consultatif International Téléphonique et Télégraphique*, ehemaliges internationales Beratungsgremium der Telekommunikationsgesellschaften

ITU: *International Telecommunications Union*, Nachfolgeorganisation der CCITT

weitere Gremien:

DANTE: *Delivery of Advanced Network Techology to Europe*, europäisches Gremium zur Koordinierung des X.500

DFN: *Deutsches Forschungs Netz*, Einführung und Betrieb von X.500 in Deutschland

X.500 Projekte

1986 VERDI *(VERteiltes DIrectory System)*, deutsches Pilotprojekt von der GMD (Gesellschaft für Mathematik und Datenverarbeitung) im Auftrag des DFN.

1989 NYSERNet, internationales White Pages Pilot Projekt von der USA initiiert, 90 DSAs in 12 Ländern.

1991 PARADISE *(Piloting A ResArchers DIrectory System in Europe)*, Europäisches Pilotprojekt, 325 DSAs in 25 Ländern, 800 000 Einträge.

1992 NADF *(North American Directory Forum)*, nationales Projekt der USA.

1993 NameFlow–Paradise, Fortführung des Projekts PARADISE durch DANTE.

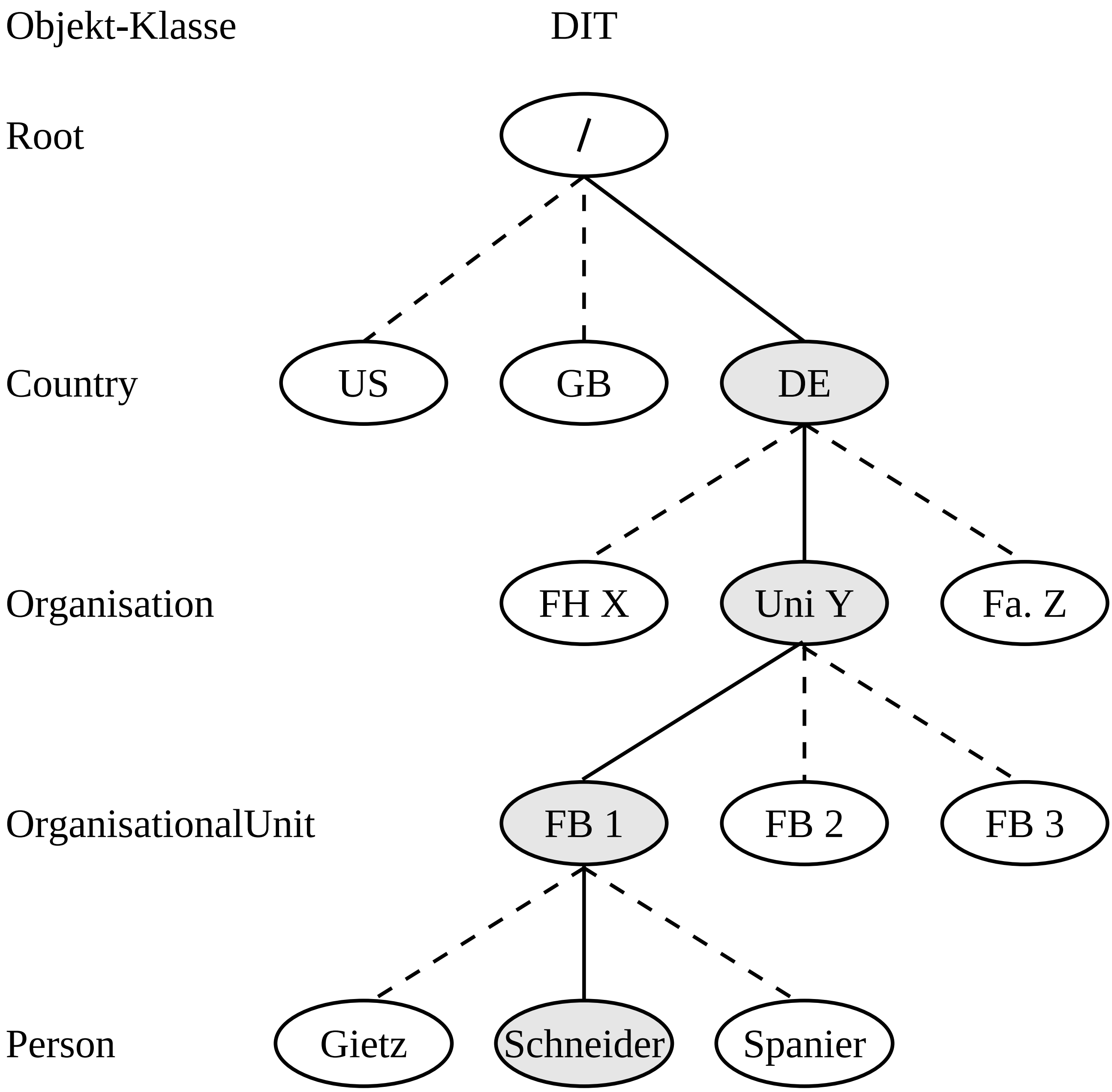
1993 „Betrieb und Betreuung des zentralen DSA (First Level DSA) in Deutschland" an der TU Chemnitz, deutscher Teilbaum des X.500 für den DFN.

1994 DFN–Projekt AMBIX, Aufbau eines zentralen DFN–E–Mail Verzeichnis unterhalb des deutschen Teilbaums.

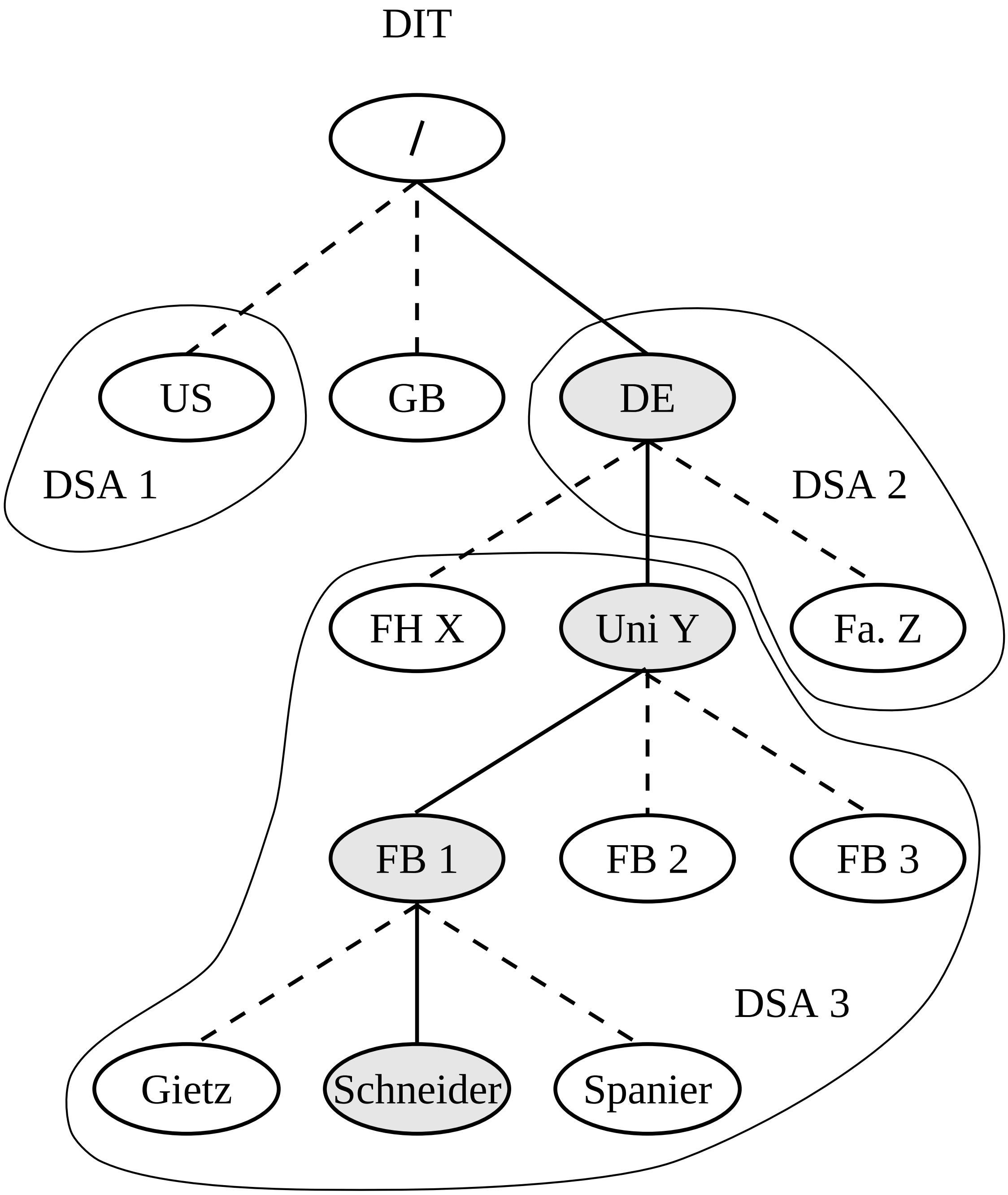
Eigenschaften des X.500

- weltweit verteilbar auf *Directory System Agents* (DSA)
- Aufnahme unbegrenzter Datenmengen
- hierarchisch strukturiert *(Directory Information Tree = DIT)*
- weltweit gleichartiger Zugriff mittels *Directory User Agents* (DUA)
- Kommunikation über spezielle Protokolle:
  - DSA ⇔ DSA: *Directory System Protocol* (DSP)
  - DSA ⇔ DUA: *Directory Access Protocol* (DAP)
  - einfache Programmierschnittstelle für DUAs: *Lightweight Directory Access Protocol* (LDAP)
- Mechanismen zur
  - Authentifizierung
  - Zugriffskontrolle
  - Replikation
- temporäre Inkonsistenz wird in Kauf genommen
- kein *record locking*
- Lese– und Suchoperationen gegenüber Schreiboperationen bevorzugt

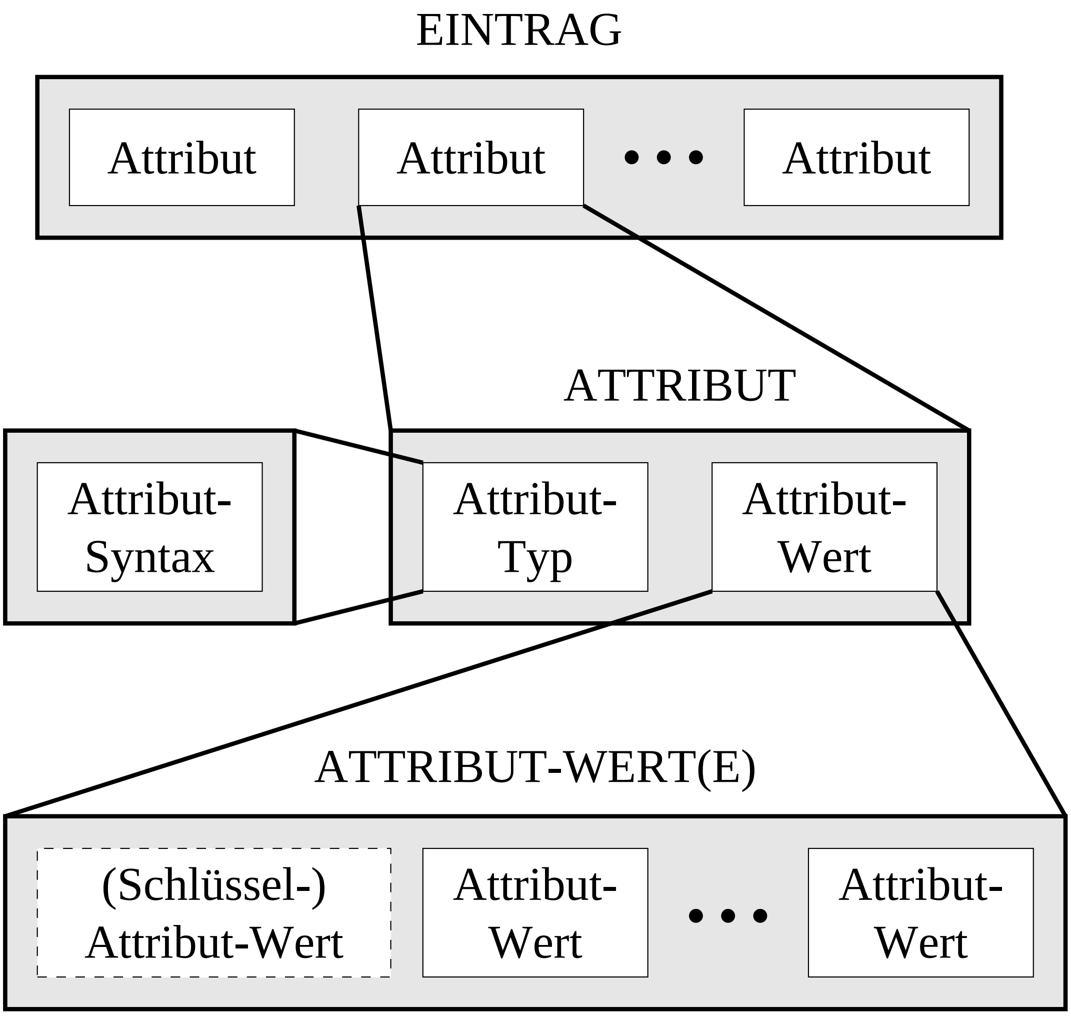
Directory Information Tree (DIT)



Verteilung des DIT auf DSAs



Struktur eines Eintrages



Namen

DIT	RDN	DN
/		
DE	c=DE	c=DE
Uni Y	o=Uni Y	c=DE, o=Uni Y
FB 1	ou=FB 1	c=DE, o=Uni Y ou=FB 1
Schneider	cn=Schneider	c=DE, o=Uni Y ou=FB 1, cn=Schneider

Sicherheitsaspekte im X.500

Authentifizierung (X.509):

simple bind: Einfache Authentifizierung mittels Passwort und DN, Daten werden unverschlüsselt übers Netz transferiert.

protected simple bind: Passwort wird verschlüsselt. Passwort, DN sowie eine Zufallsnummer und/oder eine Zeitangabe werden durch eine oder zwei *One–Way Functions* verschlüsselt.

strong bind: Strenge Authentifizierung, Verschlüsselung mittels *Public Key Cryptosystem* (PKCS).

Zugriffskontrolle:

Access Control List (ACL): (88er Standard, quipu–DSA) Liste, die festgelegt, wer welche Operationen auf bestimmte Einträge anwenden darf.

Basic Access Control Scheme: (93er Standard) Erlaubt sehr detailierte Definition der Zugriffsbeschränkungen und erlaubten Operationen.

Simplified Access Control: Untermenge des *Basic Access Control Scheme*.

Replikation

- Jeder Eintrag wird von genau einem Master–DSA verwaltet, hier ist das Original gespeichert.
- Beliebig viele DSAs können eine Kopie des Eintrages speichern.
- Ziel der Replikation:
  - großflächige Verteilung der Daten
  - schneller Zugang für DUA

X.500: Anwendung

Das X.500 stellt Daten zur Verfügung; dieses sind für

„menschliche“ Benutzer Informationen z.B. über

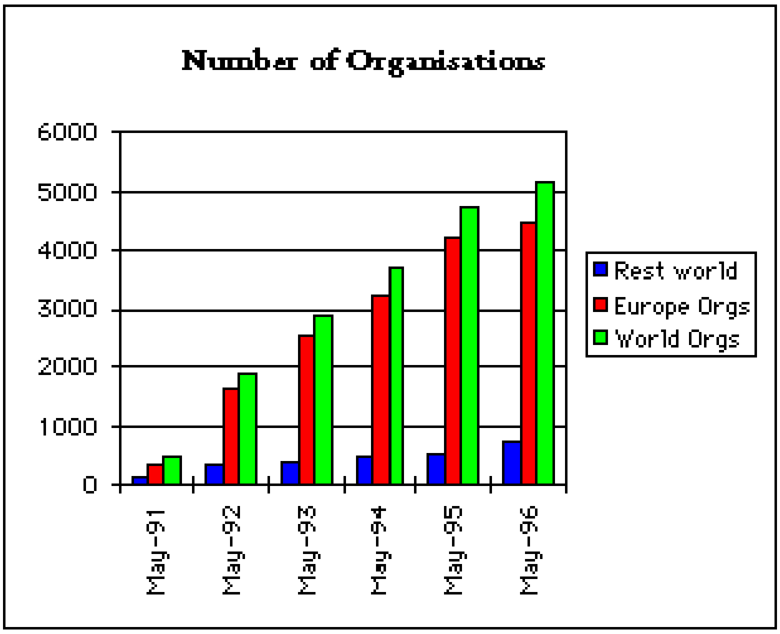
- Organisationen,
- Personen,

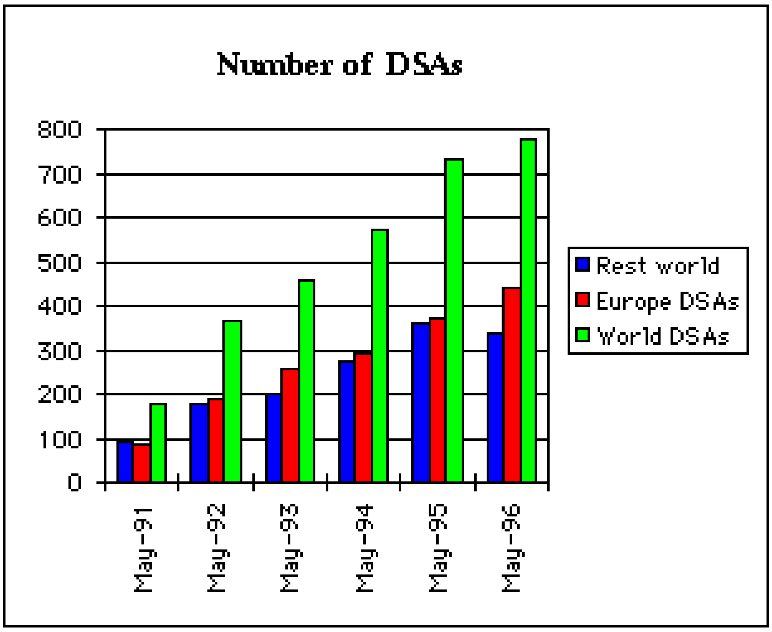
wie z.B. Telefonnummern, Adressen, E–Mail-Adressen etc.

Applikationen Informationen z.B.

- zum *Name Mapping* für X.400 E–Mail–Dienste,
- zum *Message Handling*,
- über *Public Keys* und deren Zertifikate,
- zum Datei–Transfer (FTAM = *File Transfer Access Management*),
- über Mailing Listen.

Daten im X.500





Quelle: DANTE: NameFLOW–Paradise Annual Report 1995–1996
(http://www.dante.net/np/report/ar/ar95.html)

X.500 in Zahlen*

in der Welt:

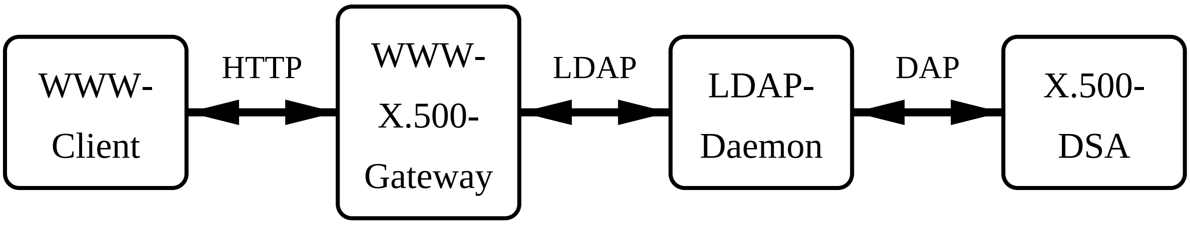
	Organisationen	DSAs
First Level	8	58
Europa	4434	398
USA	249	218
restliche Welt	455	103
Gesamt	5146	777

in Deutschland:

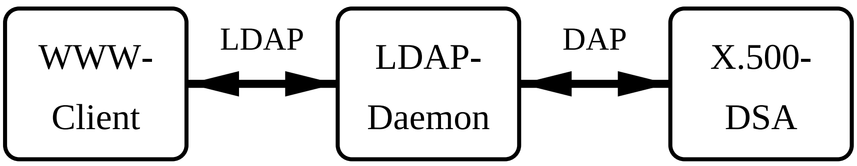
DE–Level DSAs	46
Gesamtzahl der Einträge	150,000
davon Personeneinträge	50,000
Gesamtzahl der Zugriffe pro Tag	90,000
davon Zugriffe von Personen	20,000
Zugriffe von Anwendungen	70,000

*Stand Mitte 1996

Integration in das WWW



- WWW–X.500–Gateway (Web500gw), Frank Richter, TU–Chemnitz
- TWEB (Tübinger Webgateway), Kurt Spanier, Universität Tübingen, Weiterentwicklung des Web500gw
- WWW entwickelt sich zum alleinigen Benutzer–Zugang zum X.500
- geordnete Datenbank im WWW–Chaos
- Vorteile des X.500 bleiben erhalten



- Softwarehersteller (z.B. Netscape, Microsoft, AT&T) kündigen Unterstützung für LDAP an

TWEB
I. Konfigurierbarkeit

- Technische Konfiguration:
  - Zuordnung LDAPD zu DSA
  - Gateway–Basisport
  - Zugriffskontrolle:
    - Abwehr von Such–Roboter: *robots exclusion protocol*
    - unterschiedliche Rechte für interne und externe Benutzer
    - STRICT–BASEDN: Gateway zeigt nur Daten unterhalb eines Teilbereichs des DIT an

- Gestalterische Konfiguration:
  - Darstellung der Attribute
  - Selektive Ausgabe, Attribute, Label, Reihenfolge
  - sprachspezifische Texte

- Politische Konfiguration:
  - Zugriffskontrolle, Allow–/Deny–Domain
  - Modify–Zugriff abschaltbar
  - Einschränkung der Listen
  - zusätzliche Erklärungstexte

TWEB
II. Gatewayswitching

- Lastverteilung vor dem DSA Zugriff
- „Corporate Identity“ bei Darstellung und Zugriff
- Zwei Methoden des Gatewayswitching:
  - statische Konfiguration
  - dynamische Konfiguration, LabeledURI Attribut

III. Erweiterte Funktionalität für AMBIX

- WWW–Selbsteintrag

AMBIX

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

AMBIX
Ziele und Ausgangslage

Ziele:

- Aufbau eines deutschlandweiten elektronischen E–Mail Verzeichnisses auf Basis des X.500, auch für Forschung treibende Organisationen außerhalb des DFN–Vereins
- "White Pages Service", Suche nach Personen unabhängig von der Organisationszugehörigkeit
- "Yellow Pages Service", Auflistung nach Organisationen (Mitarbeiterverzeichnis)
- Zugang über WWW (TWEB), Zugriffskontrolle

Ausgangslage:

- unklare datenschutzrechtliche Lage
- geringer Datenbestand im X.500 durch frühere Projekte
- fehlende Aktualität der Daten
- Komplexität von X.500 $\Rightarrow$ wenige Organisationen mit eigenem DSA

Datenschutz

Problematik, Interessenskonflikt

+ Wunsch nach Mitarbeiterverzeichnis
– Schutz der persönlichen Daten des Einzelnen
– Befürchtung: Werbung durch E–Mail

Vorkehrungen

- Diskussion der Aspekte des Datenschutzes bei der Konzeption von AMBIX
- Datenschutzexpertise*
- Minimalset an personenbezogenen Daten
- Widerspruchsverfahren
- Rechte der Betroffenen: Auskunft, Berichtigung, Sperrung, Löschung
- Weitergabe der Daten nur an Länder mit adäquaten Datenschutzbestimmungen
  - Rechner muß im DNS eingetragen sein
  - Ablehnung von Anfragen aus „kommerziellen“ Domains
  - Abwehr von Robotern

*ftp://ambix.uni-tuebingen.de/pub/Expertise.ps.Z

Die AMBIX–Maschine

Implementation einer netzwerkfähigen Client–Server Maschine

Eingabe:

- Struktur– und Personendatenmeldungen der Organisationen
- Datenänderungen durch Organisationen
- Selbsteintrag mittels WWW–Formular
- Widerspruch, Zustimmung und Datenänderung von Betroffenen mittels E–Mail–Formular

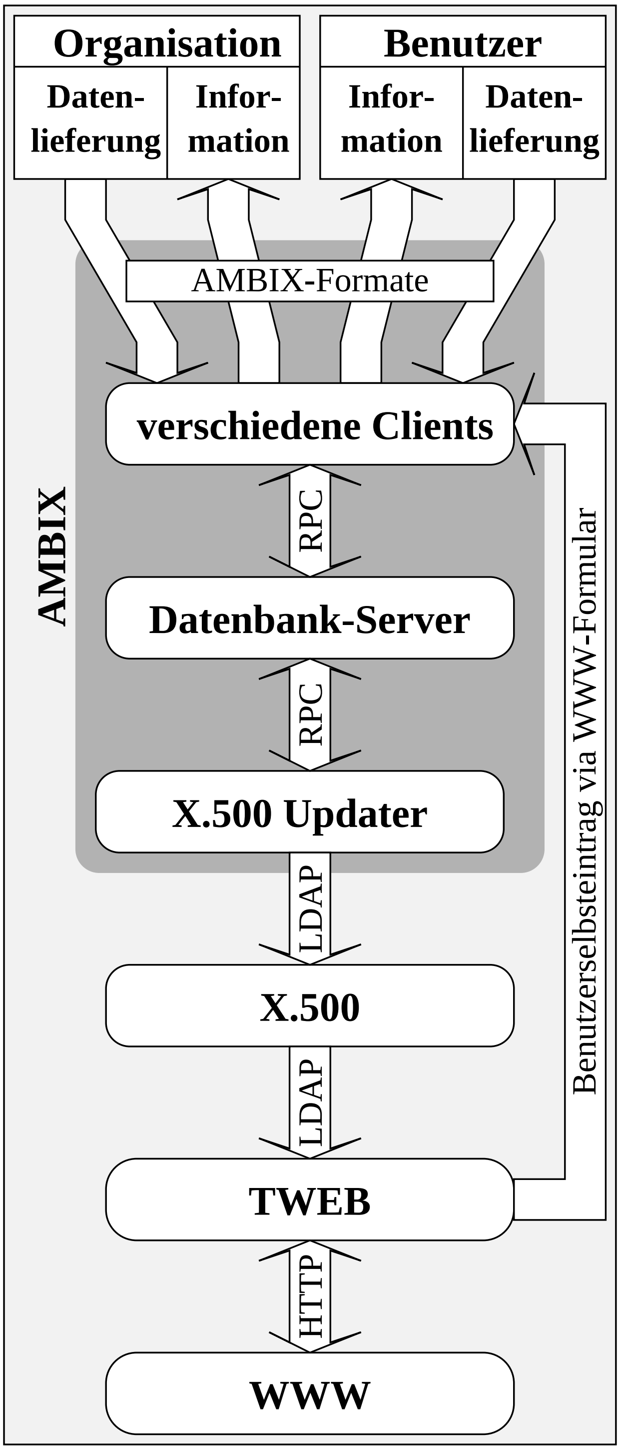
Verarbeitung:

- formale Prüfung aller Daten
- Konvertierung von Telefon– und Faxnummern in einheitliches Format
- regelmäßige Überprüfung der E–Mail–Adressen
- Protokollierung aller Vorgänge

Ausgabe:

- Fehlerprotokoll an Organisationen bei Datenlieferungen
- Information der von den Organisationen gemeldeten Personen
- Reaktion auf fehlerhafte E–Mail–Formulare der Betroffenen
- Meldung der neuen Selbsteinträgerdaten an die Organisationen
- Aktualisierung des X.500 Datenbestandes

AMBIX als Brücke zum X.500



Infrastruktur

- ASCII–Format für alle Eingabedaten
- Anonymous FTP–Server mit *incoming*–Bereich für Struktur– und Personendatenlieferung durch die Organisationen
- Ansprechpartner für AMBIX an den beteiligten Organisationen
  - Passwort zur Authetifizierung bei der Datenlieferung
  - DS–Manager Eintrag im X.500 für jeweilige Organisation
  - Mitglieder einer projektspezifischen Mailing–Liste
- Berücksichtigung von Anregungen der Administratoren bei der Weiterentwicklung

Widerspruchsverfahren

- Personendatenlieferung durch die Organisation
- Speicherung der Daten in der projektinternen Datenbank
- Information der Betroffenen über
  - das Projekt AMBIX
  - die Übermittlung Ihrer Daten durch die Organisation
  - die gelieferten Daten (Datenänderungsformular)
  - die Möglichkeit der Änderung, Sperrung bzw. Löschung
- Beginn der Widerspruchsfrist (6 Wochen)
- Veröffentlichung im X.500 erfolgt nach
  - einer Einverständniserklärung
  - einer Korrektur der Daten
  - dem Ablauf der Widerspruchsfrist
- Widerspruchsverfahren kann abgestellt werden, wenn eine schriftliche Einwilligung zur Veröffentlichung im X.500 bereits vor der Übermittlung der Daten besteht.

Datenänderungsformular

```
========================= FORMULAR [#00030/2] ANFANG ======================

### Nr.: [#12345678] (UNBEDINGT mitschicken)
                                                    (zutreffendes ankreuzen)

 -  Ich bin damit einverstanden, dass meine untenstehenden
    Daten im X-500-Directory veroeffentlicht werden . . . . . .  ( )

 -  Ich habe in den unten stehenden Daten Korrekturen vorgenommen.
    Bitte fuehren Sie diese Korrekturen vor der Veroeffentlichung
    aus . . . . . . . . . . . . . . . . . . . . . . . . . . . .  ( )

 -  Ich widerspreche der Veroeffentlichung meiner Daten im
    X-500-Directory und verlange deren Loeschung bis auf
    meine Mailadresse aus Ihrer Datenbank . . . . . . . . . . .  ( )

 -  Ich widerspreche der Veroeffentlichung meiner Daten im
    X-500-Directory und verlange die Loeschung aller meiner
    Daten aus Ihrer Datenbank . . . . . . . . . . . . . . . . .  ( )

                             X.500 Daten

Organisation:      Univeritaet Tuebingen
                   ou= Physik
                   ou= Physikalisches Insitut

Nachname:          Mustermann

Vorname(n):        Karl

Titel:             Dr.

Telefonnummer(n):  +49 7071 29-71234, +49 7071 29-75678

Fax:               +49 7071 29-9876

E-Mail-Adresse(n): karl.mustermann@uni-tuebingen.de

================================ FORMULAR ENDE ============================
```

Sicherheitsaspekte bei AMBIX

X.500

- Authentifizierung im X.500 nur über vorhandene Einträge im Verzeichnis möglich
- nicht jeder Nutzer des Verzeichnisses ist im X.500 eingetragen
- Zugriffsbeschränkungen im X.500 reichen nicht aus
- keine Daten (Ausnahme Strukturdaten) an andere DSA
- Daten nur an das AMBIX WWW–Gateway (TWEB)
- Authentifizierung des TWEB mittels *protected simple bind* beim DSA

AMBIX

- Sicherheitsmaßnahmen RPC—Schnittstelle: Zeitstempel und Checksumme
- TCP–Wrapper: Überwachung und Beschränkung des Zugangs zu TCP–Servern
- PortMapper: Überwachung und Beschränkung des Zugangs zu RPC–Diensten
- Secure Shell: Strenge Authentifizierung beim Login, verschlüsselte Datenübertragung (PKCS)

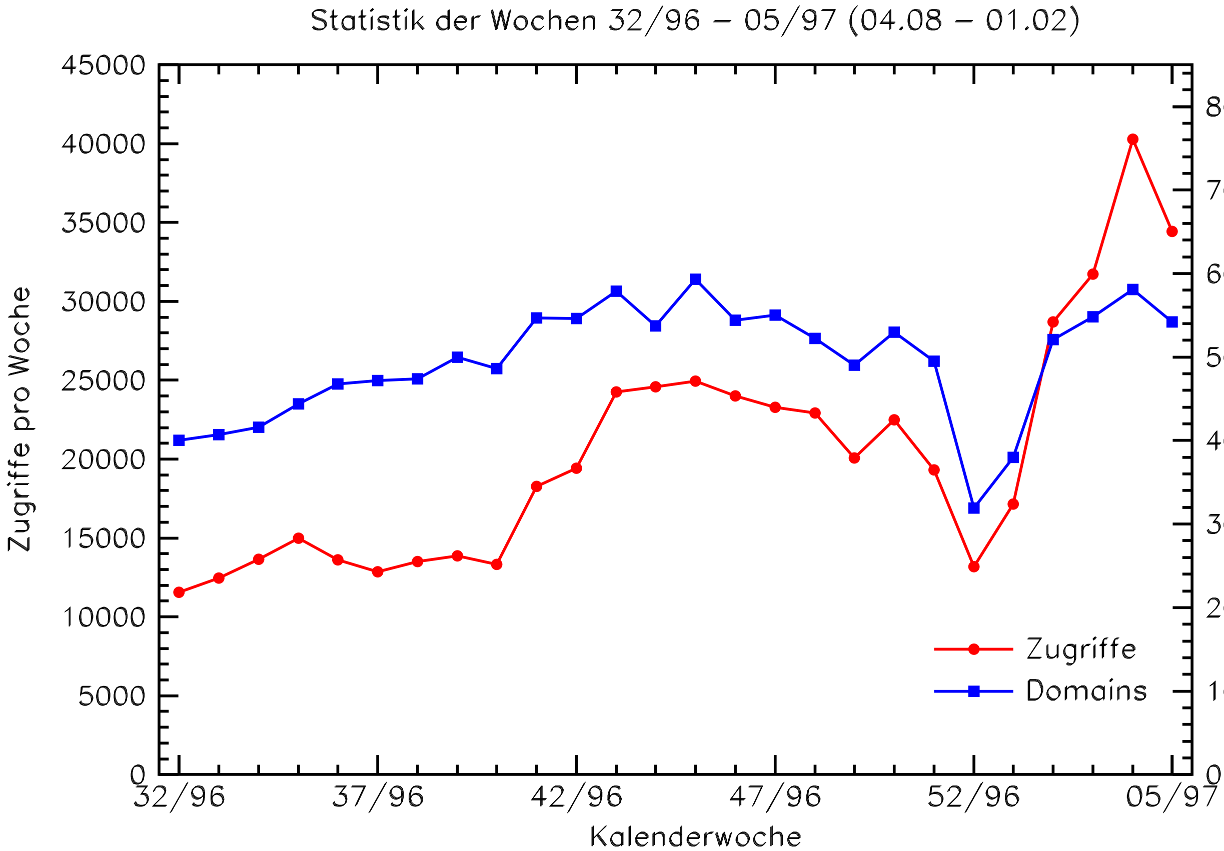
Statistik zum DFN–E–Mail–Verzeichnis*

- Bestand im X.500:
  - 116 Organisationen
  - 4144 Strukturdatensätze
  - bis zu 4 Hierarchieebenen
  - Verweis von AMBIX auf 23 Organisationen die eigenen Datenbestand pflegen (Gatewayswitch)
  - 24653 Personeneinträge
- ca. 15 Selbsteinträger pro Tag†
- steigende Zugriffszahlen

*Stand 3. Februar 1997

†gemittelt Januar 1997

Zugriffsstatistik



Ausblick

- Arbeitserleichterungen für die beteiligten Organisationen:
  - Konvertierungshilfen zur Anbindung der organisationseigenen Datenbanken zur Benutzerverwaltung
  - Erleichterung des Datenabgleichs X.500 $\Leftrightarrow$ Benutzerdatenbank
  - WWW–basierte Administrations–Tools
- AMBIX–Interface für Organisationen mit eigenem DSA
- Gesamtsuche im Verzeichnis
- Ergänzung der Strukturdaten, Aufnahme neuer Organisationen
- Aufbau einer Infrastruktur zur Schlüsselverwaltung von asymmetrischen Verschlüsselungsverfahren

Infrastruktur für Schlüsselverwaltung

- Darstellung der entsprechenden Attribute im X.500:
  - PEM (*Privacy Enhanced Mail*) $\Rightarrow$ X.509
  - PGP (*Pretty Good Privacy*)
    - bisher nur Vorschläge von der *Internet Engineering Task Force* (IETF)
    - es existiert eine proprietäre „Tübinger“ Lösung
- Aufbau einer sicheren Kommunikationsstruktur zur Anlieferung der Schlüssel
- enge Zusammenarbeit mit den DFN–PCA Projekt an der Universität Hamburg
- Konzeption und Implementation von Anwendungen die auf die Schlüssel im Verzeichnis zugreifen

Warum X.500?

- weltweit verteiltes, einheitliches System
- objektorientiert
- Client–Server Struktur
- beliebige Verteilbarkeit lokaler Daten
- standardisierte Schnittstellen
- komfortabler Zugang via WWW
- steigende Akzeptanz

Warum AMBIX?

- Vorzüge des X.500 für Forschung treibende Organisationen
- kein Betrieb eines eigenen DSAs nötig
- Datenschutzkonformität
- datenschutzrechtliche Verantwortung beim DFN–Verein
- Zugriffsbeschränkung
- Selbsteintrag
- Aktualisierung

Möglichkeiten der Beteiligung

Datenlieferung

- mit Personendaten:
  - Organisation liefert Struktur– und Personendaten
    - Selbsteintrag erlaubt
    - Selbsteintrag nicht erlaubt
- ohne Pesonendaten (nur Selbsteintrag):
  - Organisation liefert nur Strukturdaten
  - AMBIX ermittelt Strukturdaten
  - Selbsteintrag
    - Organisation überprüft und korrigiert Daten
    - Organisation überprüft und korrigiert nicht

Datenänderung:

- durch Organisation und Benutzer
- nur durch Organisation
- nur durch Benutzer
  - Organisatioswechsel erlaubt
  - Organisatioswechsel nicht erlaubt

WWW–Verweis:

- Organisation verweist auf AMBIX
- AMBIX verweist auf Organisation

Kontakt

E–Mail: ambix-d@mail500.uni-tuebingen.de

URL: http://ambix.uni-tuebingen.de/