AMBIX:

DFN-weite Unterstützung elektronischer Kommunikation

Vortrag gehalten im Plenum der 25. DFN-Betriebstagung
am 15. Oktober 1996

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

Was ist X.500?

X.500 - Ein OSI-Standard

- Mechanismus zur weltweiten Verteilung von Daten
- Directory-Service
- internationaler Standard
- Teilbereich von OSI (Open Systems Interconnection)
- Konform mit dem OSI-7-Schichten-Modell

X.500 - die Gremien

- 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 wird X.500 von DANTE (Delivery of Advanced Network Technology to Europe) koordiniert.
- In Deutschland ist der DFN-Verein (Deutsches Forschungs Netzt) für die Einführung und den Betrieb von X.500 zuständig.

X.500 Projekte

- 1989 NYSERNet White Pages Pilot Project, international
- 1992 NADF (North American Directory Forum), USA
- 1991 PARADISE (Piloting A ReseArchers Directory Service in Europa)
- 1993 NameFlow-Paradise von DANTE (Delivery of Advanced Network Technology to Europe)
- 1986 VERDI von der GMD im Auftrag des DFN.
- 1993 „Betrieb und Betreuung des zentralen DSA (First-Level-DSA) in Deutschland“, DFN
- 1994 AMBIX (Aufnahme von Benutzern in das X.500-Directory)

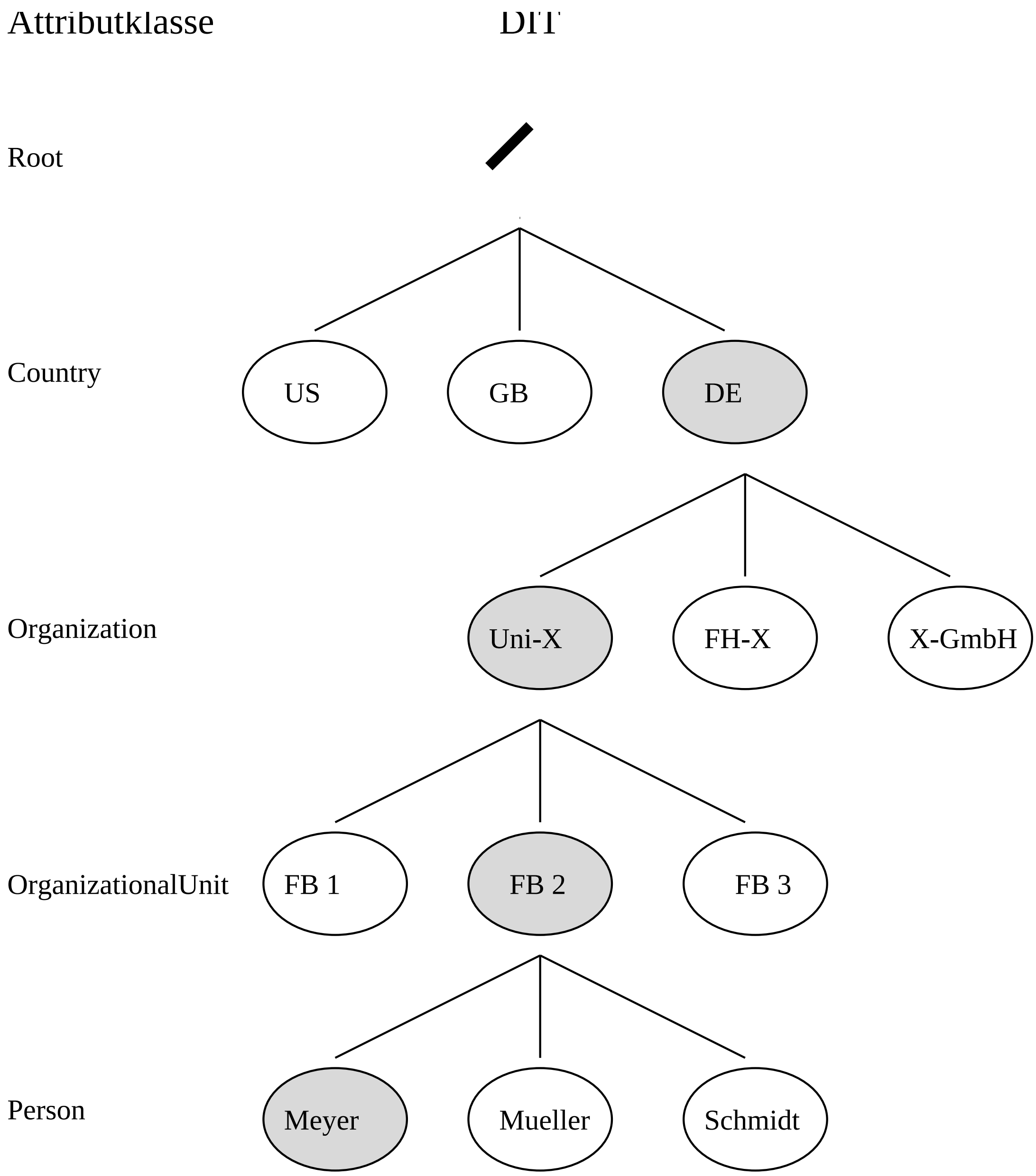
X.500 - Abbildung von Wirklichkeit

- offen definiert
- lokal beliebig erweiterbar
- keine Beschränkungen bezüglich der Datenmengen
- beliebige Daten sind speicherbar

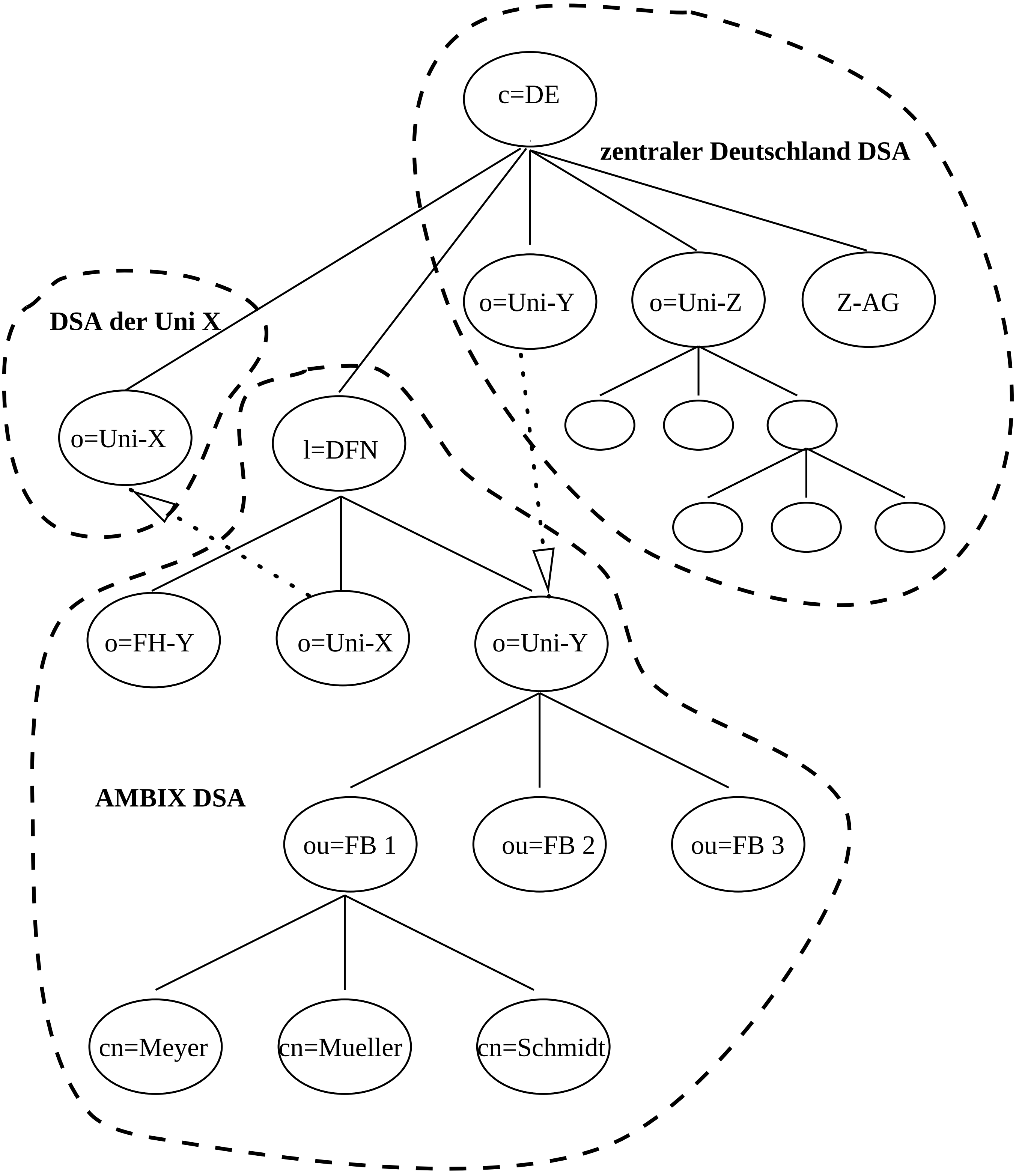
Eigenschaften von X.500

- hierarchisch strukturiert
- Baumstruktur (*directory information tree*, DIT)
- Vererbbarkeit von Attributwerten entlang der DIT-Hierarchie
- weltweit verteilt auf *directory system agents*, (DSA)
- weltweit gleichartig zugreifbar über *directory user agents*, (DUA)
- DSAs und DUAs kommunizieren über Protokolle miteinander
- wichtigstes Protokoll für Softwareentwicklung ist das *lightweight directory access protocol* (LDAP)
- automatische Replikationsmechanismen
- temporäre Inkonsistenz
- kein *record locking*
- Authentifizierungsmechanismen
- Zugriffskontrolle mit ACL-Attributen *(access control list)*
- Lese- und Suchoperationen gegenüber Schreiboperationen bevorzugt

Der Directory Information Tree: DIT



Verteilung des DITs auf die DSAs

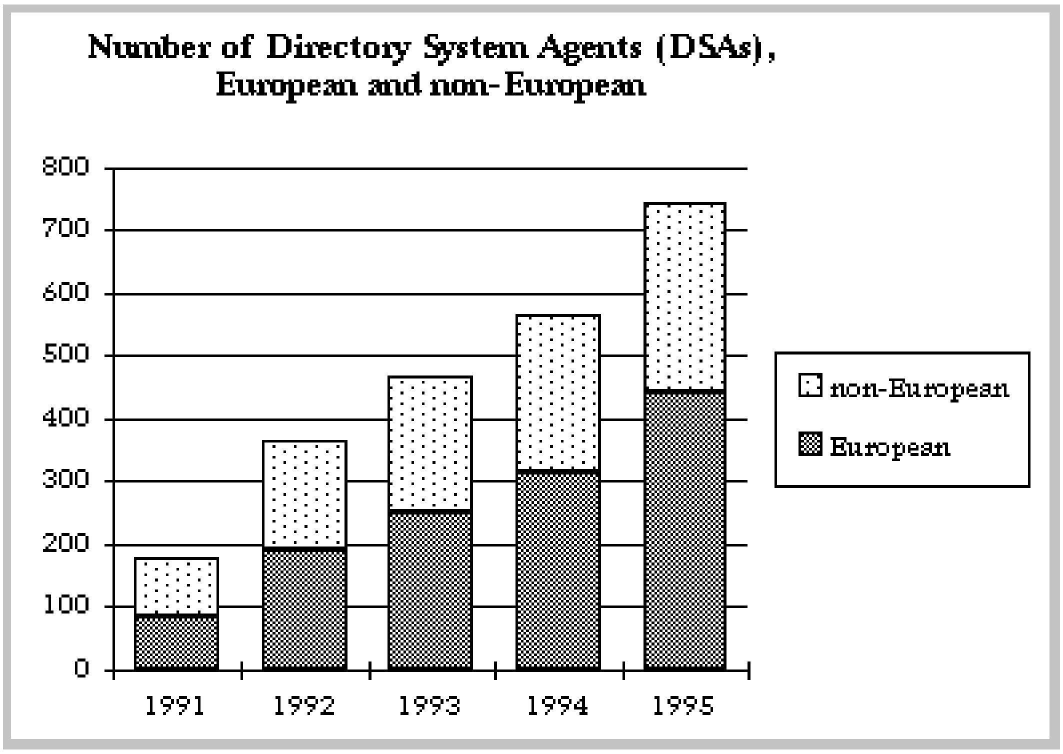


X.500 - Die Anwendung

X.500 liefert Daten

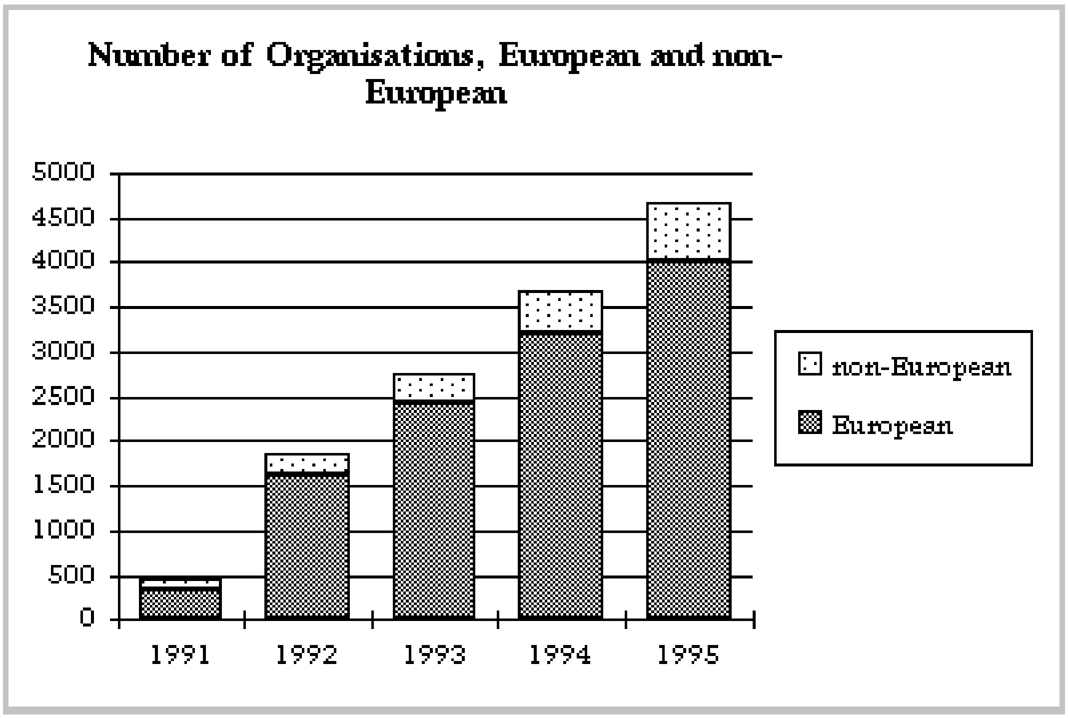
- für menschliche Benutzer
  - über Organisationen
  - über Personen
- für Applikationen
  - zum *message handling*
  - zum *name mapping* für X.400 E-Mail-Dienste
  - *public keys* und deren Zertifikate
  - zum Datei-Transfer (*file transfer access management*, FTAM)

Anzahl der DSAs im X.500



Quelle: DANTE, http://www.dante.net/np/growth.html

Anzahl der Organisationen im X.500



Quelle: DANTE, http://www.dante.net/np/growth.html

Heutiger Stand

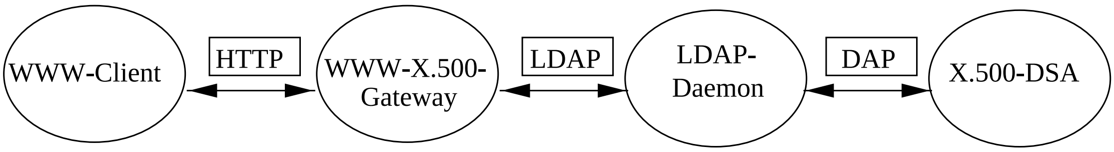
- Ca. 2 Million Personendatensätze,
- in ca. 6.200 Organisationen aus 38 Ländern,
- von ca. 800 DSAs verwaltet.

X.500 in Deutschland

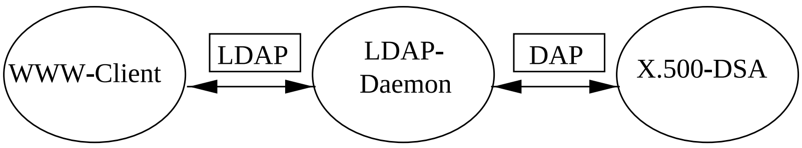
Das Ergebnis einer Umfrage im Februar 1996 (Zahlen gerundet):

Einträge	
• Anzahl der Gesamteinträge	100.000
- davon Personeneinträge	45.000
Zugriffe pro Tag	
• auf Personen	53.000
- davon von Personen	18.000
- davon von Applikationen	35.000
• sonstige Zugriffe von Applikationen	36.000
Anzahl der Master-DSAs	46

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

Gatewayswitching mit TWEB

- „Corporate Identity“: Darbietung und Zugriff
- Lastverteilung vor dem DSA-Zugriff
- Netzwerk und DSAs werden entlastet
- Zwei Methoden des Switching:
  - statische Konfiguration
  - dynamische Konfiguration

AMBIX

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

Ausgangslage vor AMBIX

- Die datenschutzrechtliche Lage war unklar
- Frühere Projekte haben nur wenig Daten ins X.500 gebracht.
- Die vorhandenen Daten sind schnell veraltet.
- Wegen der Komplexität von X.500 waren wenig Organisationen bereit, eigene DSAs zu betreiben.

Datenschutzproblematik

- Interessenkonflikt:
  - Mitarbeiterverzeichnis
  - Datenschutzinteresse der Betroffenen
- Hauptproblem: Werbung durch E-Mail

Vorkehrungen zum Datenschutz

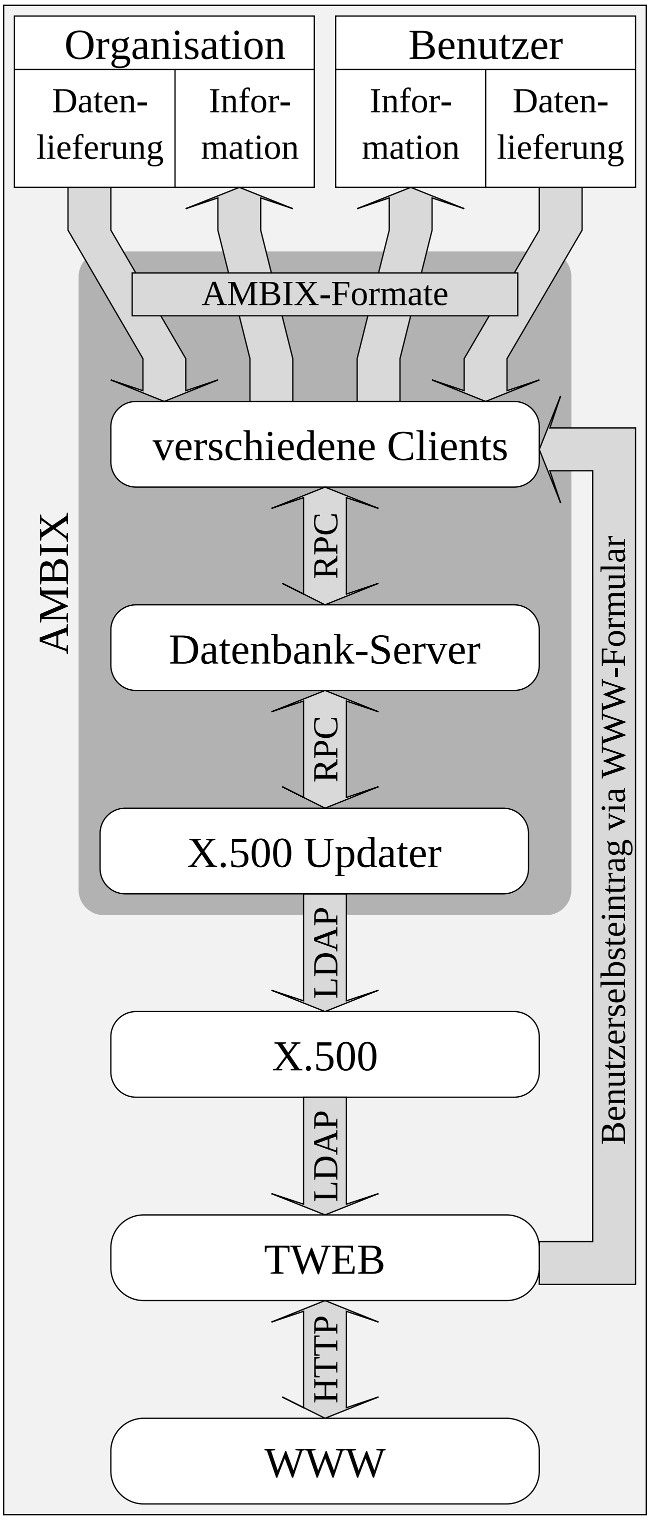
- Datenschutzdiskussion bei Konzeption von AMBIX
- Datenschutzexpertise (ftp://ambix.uni-tuebingen.de/pub/Expertise.ps.Z)
- Minimalset von Datenfeldern
- Widerspruchsverfahren
- Rechte der Betroffenen auf Auskunft, Veränderung, Sperrung und Löschung ihrer Daten
- Rechner muß im DNS eingetragen sein
- Personendaten nur an Rechner aus datenschutztreibenden Ländern
- nicht an kommerzielle Domains
- Erkennen und Abwehr von Robotern

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-Mailadressen 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



Die Infrastruktur

- Es sind ASCII-Formate für Eingabedaten:
  - für Strukturdatenlieferungen
  - für Personendatenlieferungen
- Ein Anonymous-FTP-Server mit *incoming*-Bereich
- Ansprechpartner für AMBIX an den Mitgliedsorganisationen
  - Paßwort zur authentifizierten Datenlieferungen
  - DS-Manager im X.500
  - Mailing-Liste
- Anregungen der Administratoren werden bei der Weiterentwicklung berücksichtigt.

Das 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:        Universitaet Tuebingen
                     ou= Biologie
                     ou= Biologisches Institut

Nachname:            Niemand

Vorname(n):          Ohne Vornamen

Titel:               Priv.Doz.

Telefonnummer(n):    +49 7071 29-9999, +49 7071 29-8888

Fax:                 +49 7071 29-7777

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

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

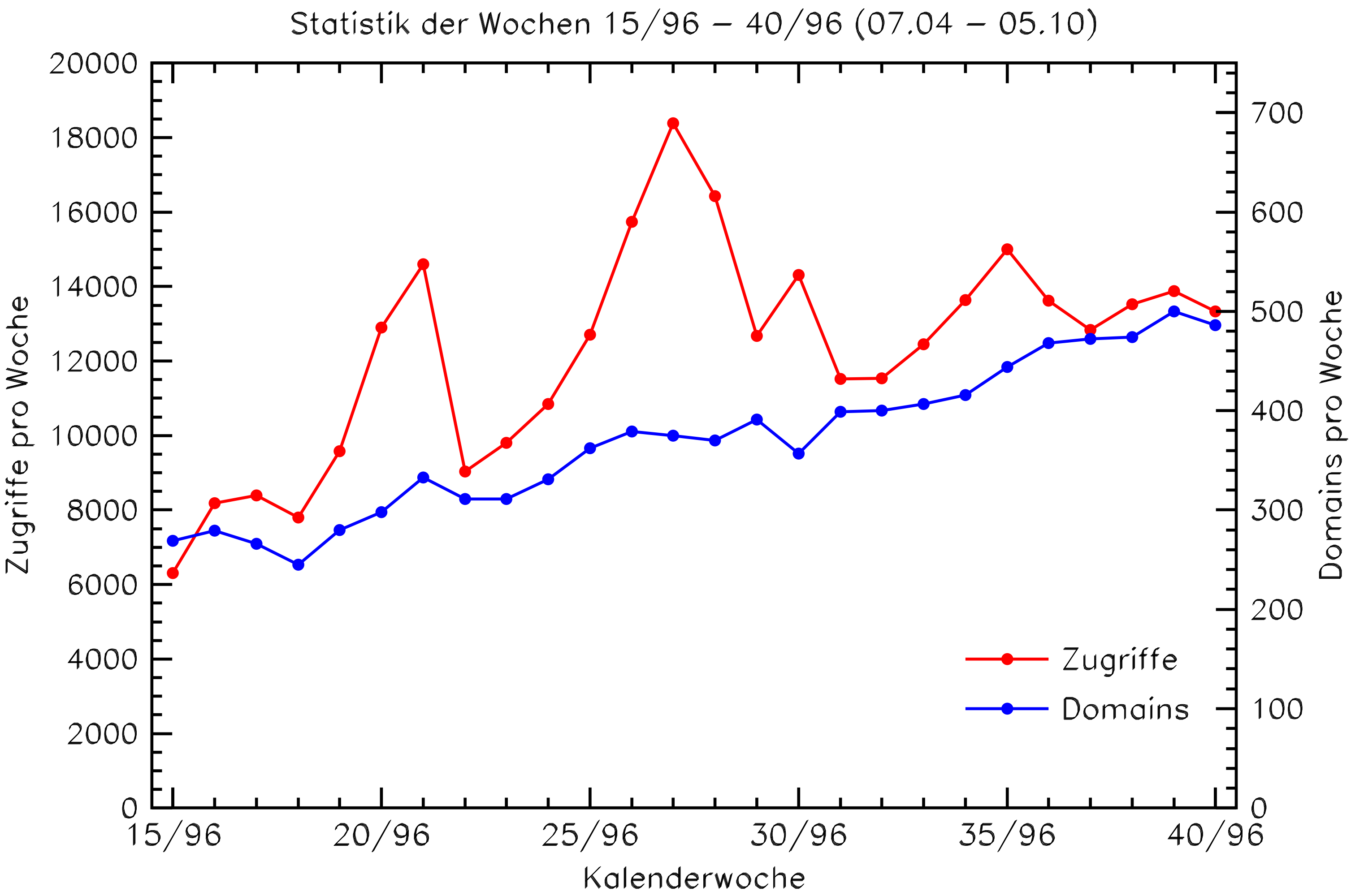
Widerspruchsverfahren

- Personen werden von Organisation gemeldet
- Die Daten werden vorläufig in der internen Datenbank gespeichert
- Die Betroffenen werden von AMBIX informiert über
  - das Projekt,
  - die Übermittlung ihrer Daten durch ihre Organisation,
  - ihre Möglichkeit der Datenänderung, Sperrung bzw. Löschung.
- Die Widerspruchsfrist beginnt.
- erst nach Einverständniserklärung, Datenkorrektur oder Ablauf der Widerspruchsfrist werden die Daten im X.500 veröffentlicht
- Bei schriftliche Einwilligung vor der Datenlieferung, kann das Widerspruchsverfahren entfallen

Daten im DFN-E-Mailverzeichnis

- Insgesamt sind 113 Organisationen im DFN-Verzeichnis aufgenommen.
- Die Organisationsstruktur enthält ca. 3.700 Strukturdatensätze.
- 22 weitere Organisationen pflegen eigene Datenbestände worauf im DFN-Verzeichnis ein „see-also"-Verweis zeigt.
- Insgesamt sind ca. 15.000 Personendatensätze im DFN-Verzeichnis.
- Täglich kommen ca. 10-20 Selbsteinträger hinzu.
- Ca. 18.000 weitere Personendatensätze sind über die Verweise zugänglich.
- Durchschnittlich wird ca. 2.500 mal pro Arbeitstag auf das DFN-Verzeichnis über das WWW-Gateway zugegriffen.

Zugriffsstatistik



Ausblicke

- Erleichterungen für beteiligte Organisationen
  - Konvertierhilfen
  - Anbindungen an die Benutzerdatenbanken
  - WWW-basierte Administrationstools
- AMBIX-Interface für andere DSA-Betreiber
- Verwaltung von Public Keys für asymmetrische Verschlüssellungsverfahren
- Gesamtsuche im Verzeichnis
- Ergänzung der Strukturdaten

Warum X.500?

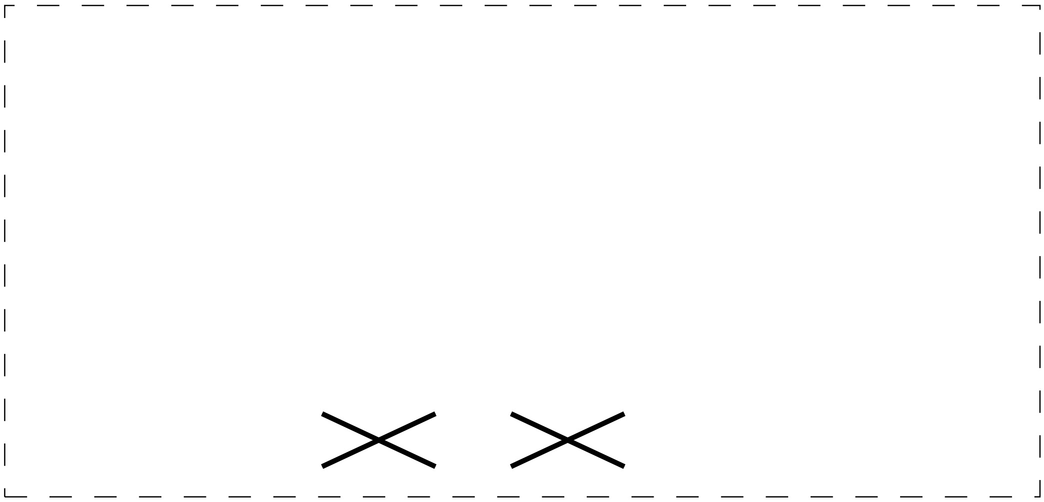
- Weltweit verteiltes einheitliches System
- Objektorientiert
- Client-Server-Struktur
- Lokale Daten beliebig auf Rechner verteilbar
- Sauber definierte Schnittstelle für Recherchen
- Komfortabler Zugang via WWW
- Zunehmende Akzeptanz sowohl bei Datenanbieter als auch bei Datensuchenden

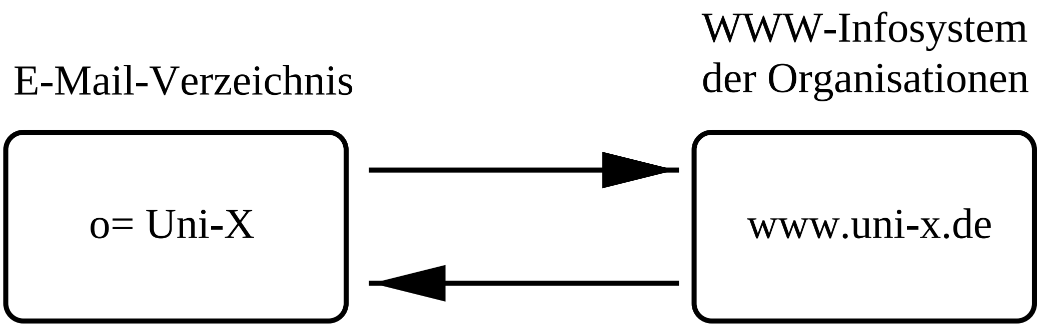
Warum AMBIX?

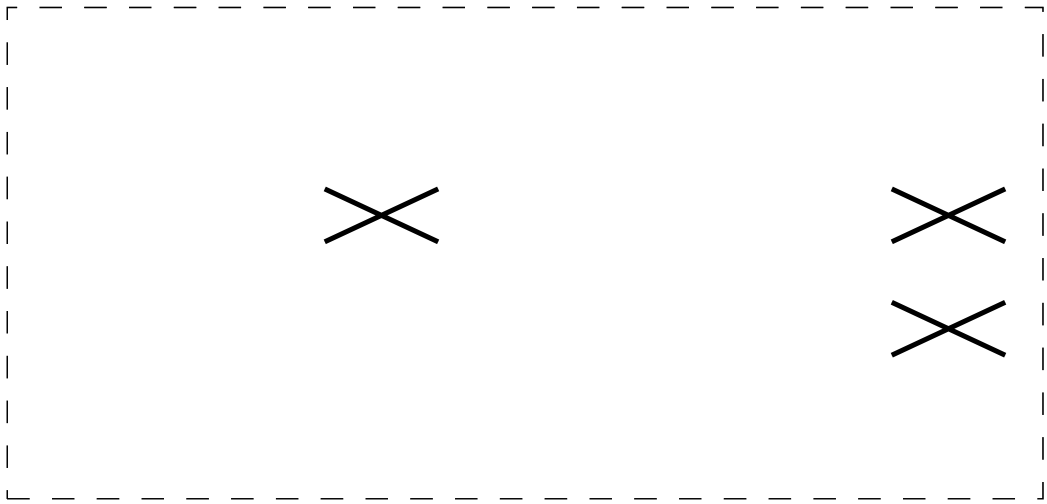
- Alle Vorzüge des X.500 für DFN-Mitgliedsorganisationen
- Das Betreiben eines eigenen DSAs entfällt
- Datenschutzkonformität
- Zugriffsbeschränkung
- Selbsteintragsmöglichkeit der Benutzer
- Kommunikation mit den Benutzern wird abgenommen
- Automatisierte Aktualisierung der Daten

Möglichkeiten der Beteiligung

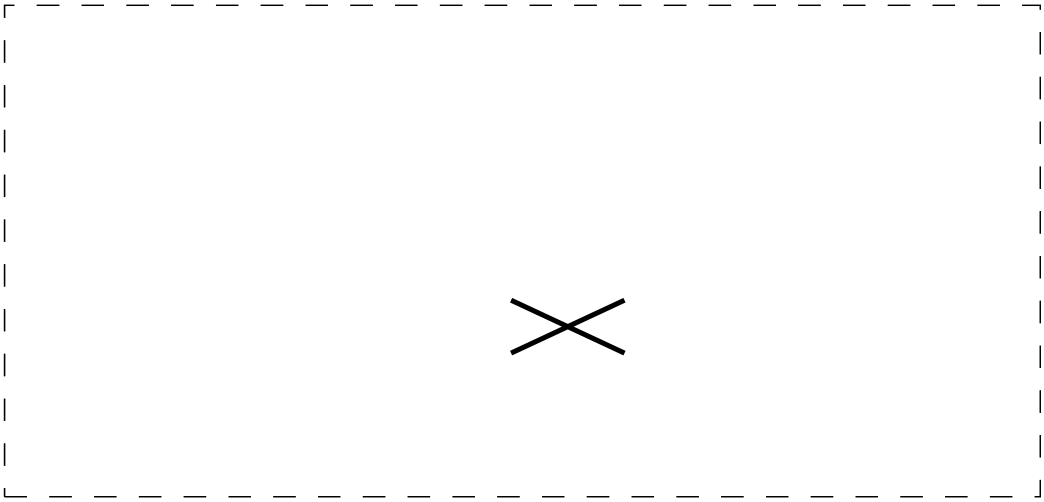
Datenlieferung	**AMBIX** Struktur	**Organisationen** Struktur	Personen	**Benutzer** Personen
Neuanmeldung				
Änderung				
Verweise				



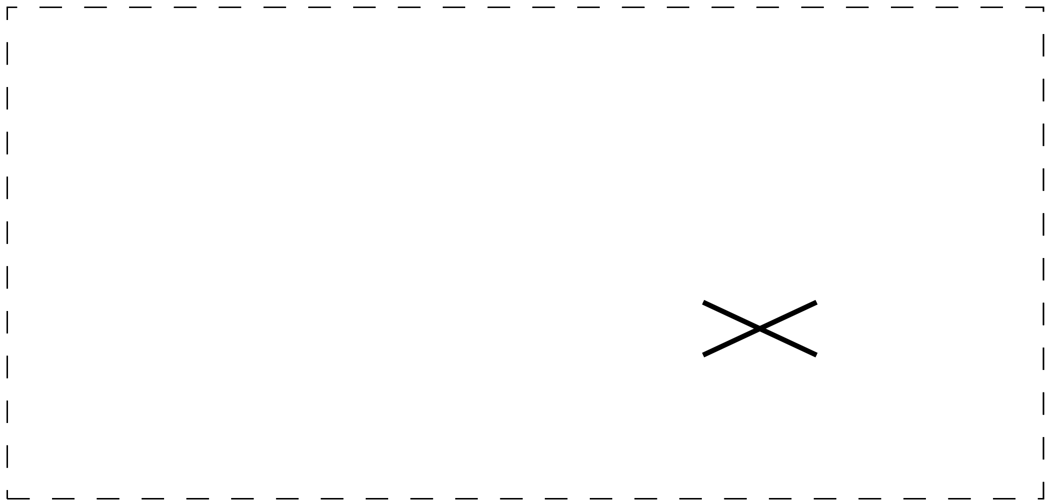

WWW-Infosystem
der Organisationen
E-Mail-Verzeichnis
o= Uni-X
www.uni-x.de



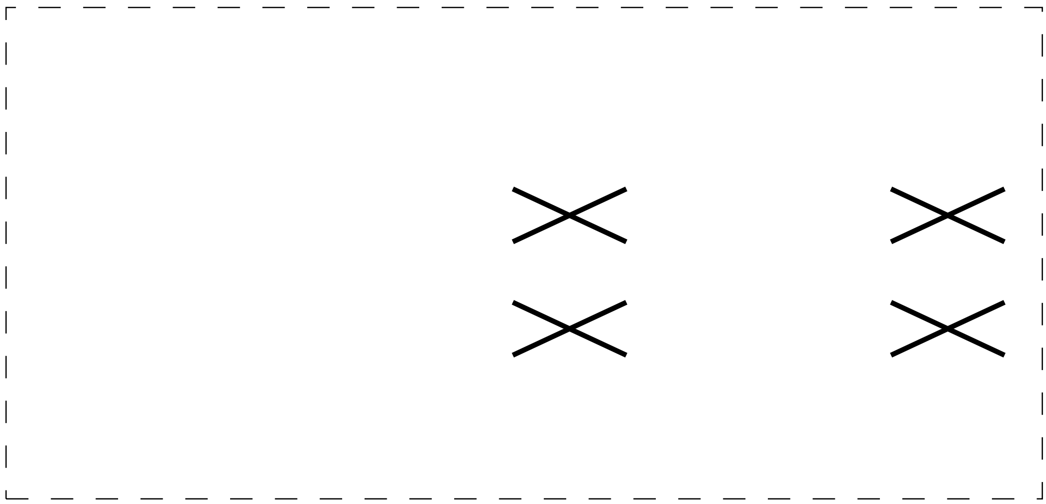
- Ambix ermittelt Strukturdaten
- Benutzer tragen sich via WWW-Formular ein
- und ändern Ihre Daten per E-Mail-Formular



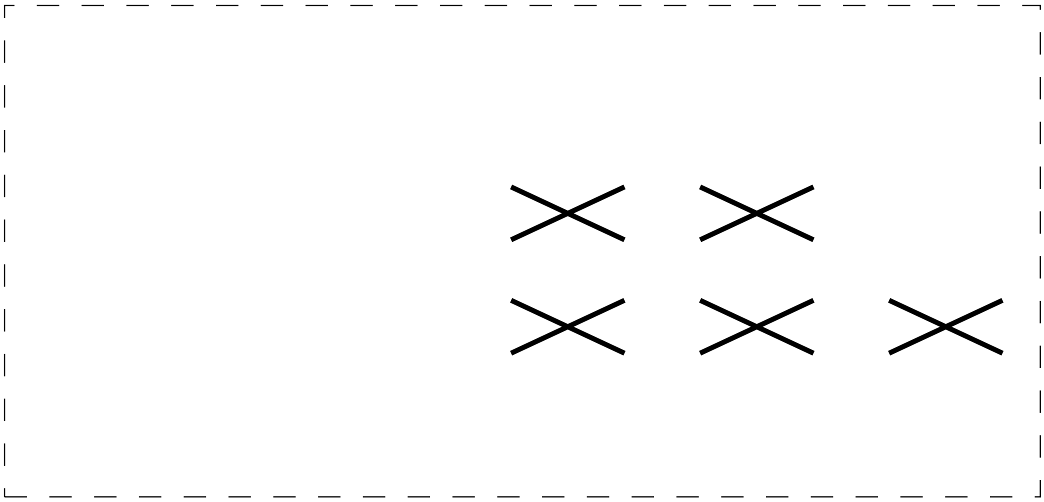
- Organisationen korrigieren vorgelegte Struktur



- Organisationen prüfen und korrigieren die Selbsteinträge



- Organisationen definieren und pflegen Struktur
- Benutzer tragen sich via WWW-Formular ein
- Benutzer ändern Ihre Daten per E-Mail-Formular



- Organisationen definieren und pflegen Struktur
- Organisationen liefern und aktualisieren Personendaten
- Benutzer ändern Ihre Daten per E-Mail-Formular

- zusätzlich wird Selbsteintrag der Benutzer erlaubt

Diskussion

Kontakt

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