Aufbau eines Directory–Kompetenzzentrums an der Universität Tübingen

X.500–AK der 29. DFN–Betriebstagung
15. September 1998

Dr. Ralf Schneider,
Zentrum für Datenverarbeitung, Universität Tübingen

Inhalt

Status Projekt AMBIX

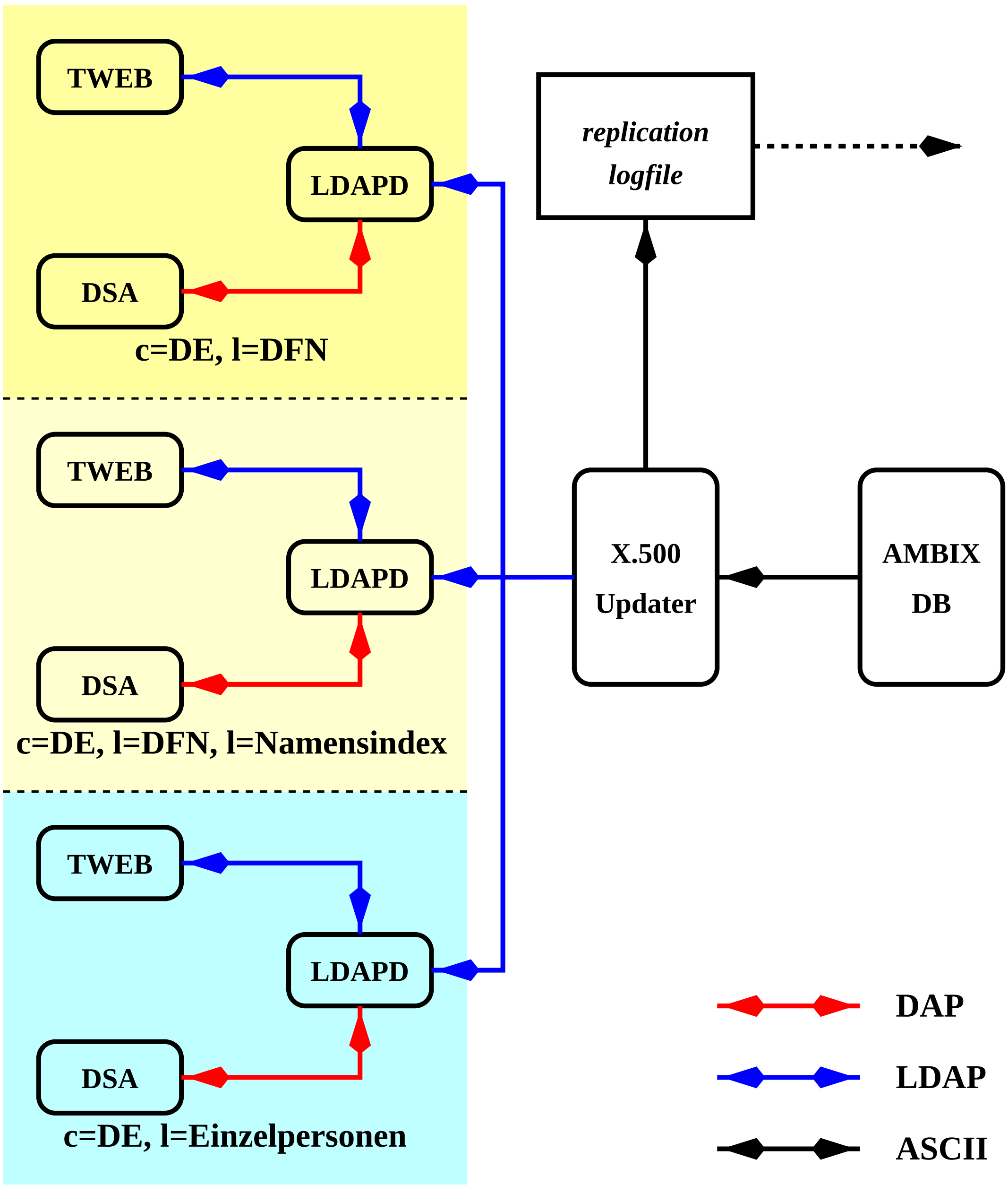
•

Aufbau und Betrieb eines
Directory–Kompetenzzentrums

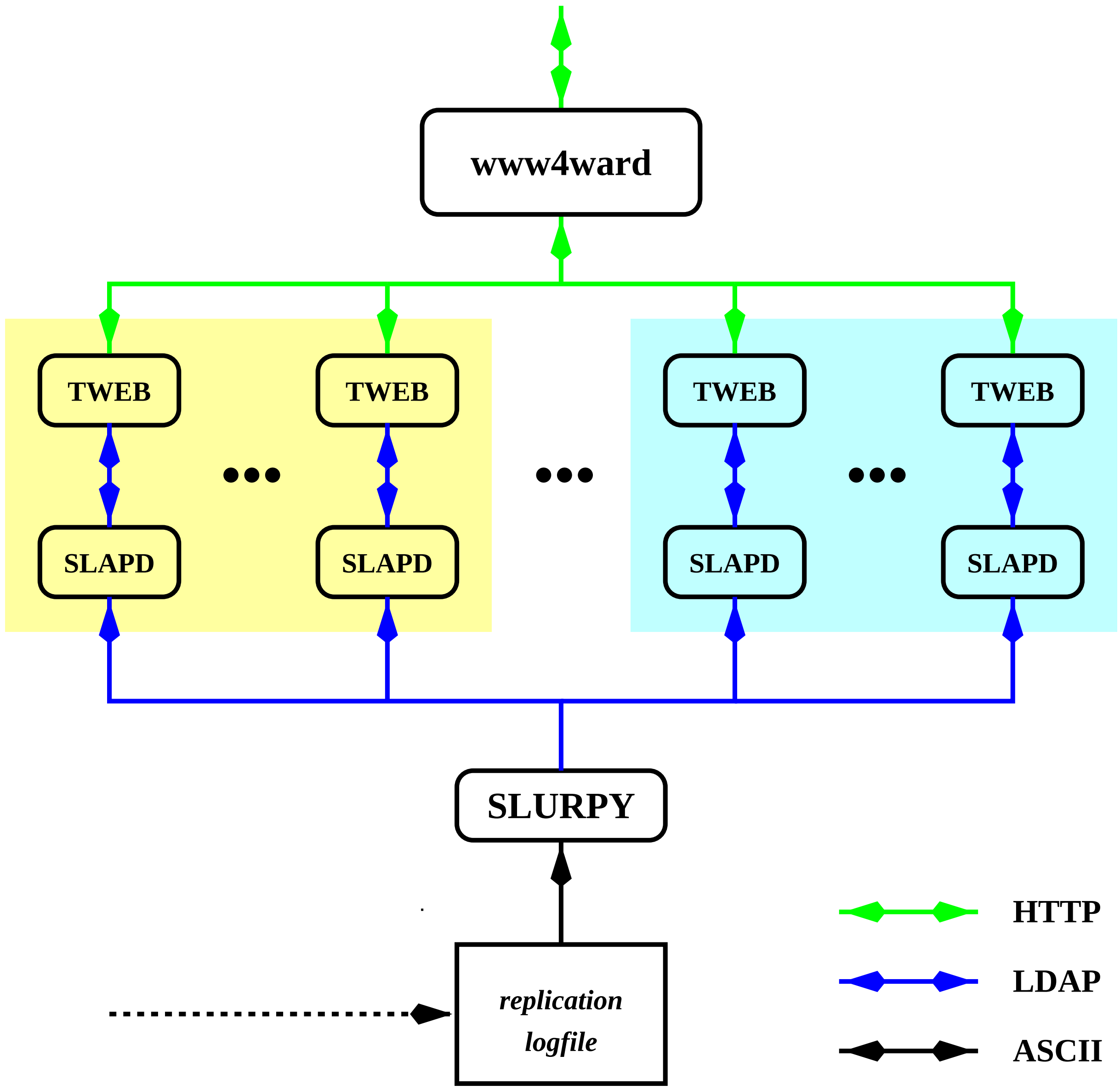
Status AMBIX

- Arbeitserleichterungen für Organisationen
  - verschiedene Modi der Datenlieferung
    - Widerspruchs–Modus
    - Direkt–Modus
    - Modus der unvollständigen Datenlieferung
    - Gesamt–Update–Modus
  - Datenkonvertierung
  - Organisationsdatenänderung via WWW
- Entwicklung und Einsatz eines Konzepts zur Datenverteilung
- organisationsunabhängige Suchmöglichkeit (Namensindex, Finger–Service)
- Integration von PGP– und PEM–Schlüsselverwaltung im X.500
- Kooperation mit DFN–PCA

Datenverteilung I
Referenzdatenbestand (DSA)



Datenverteilung II
Benutzeranfragen (SLAPD & TWEB)



Zertifikate im X.500

- PEM ⇒ Standard ⇒ kein Problem
- PGP ⇒ kein internationaler Standard!
- proprietäre Lösungen, z.B. Tübingen

Objektklasse:	`pGPSecurityObject`	
Attribute:	`pGPKey`	`IA5String`
	`pGPKeyRev`	`IA5String`
	`pGPKeyID`	`CaseIgnoreString`
	`pGPUserID`	`CaseIgnoreString`

- Nachteil: bei mehreren Zertifikaten keine eindeutige Zuordnung
- Definition eines Standards; Attribut mit Meta–Syntax

  Mailing-Liste:

  `ambix-pgp@mail500.uni-tuebingen.de`

  Administrator der Liste (Dr. Kurt Spanier):

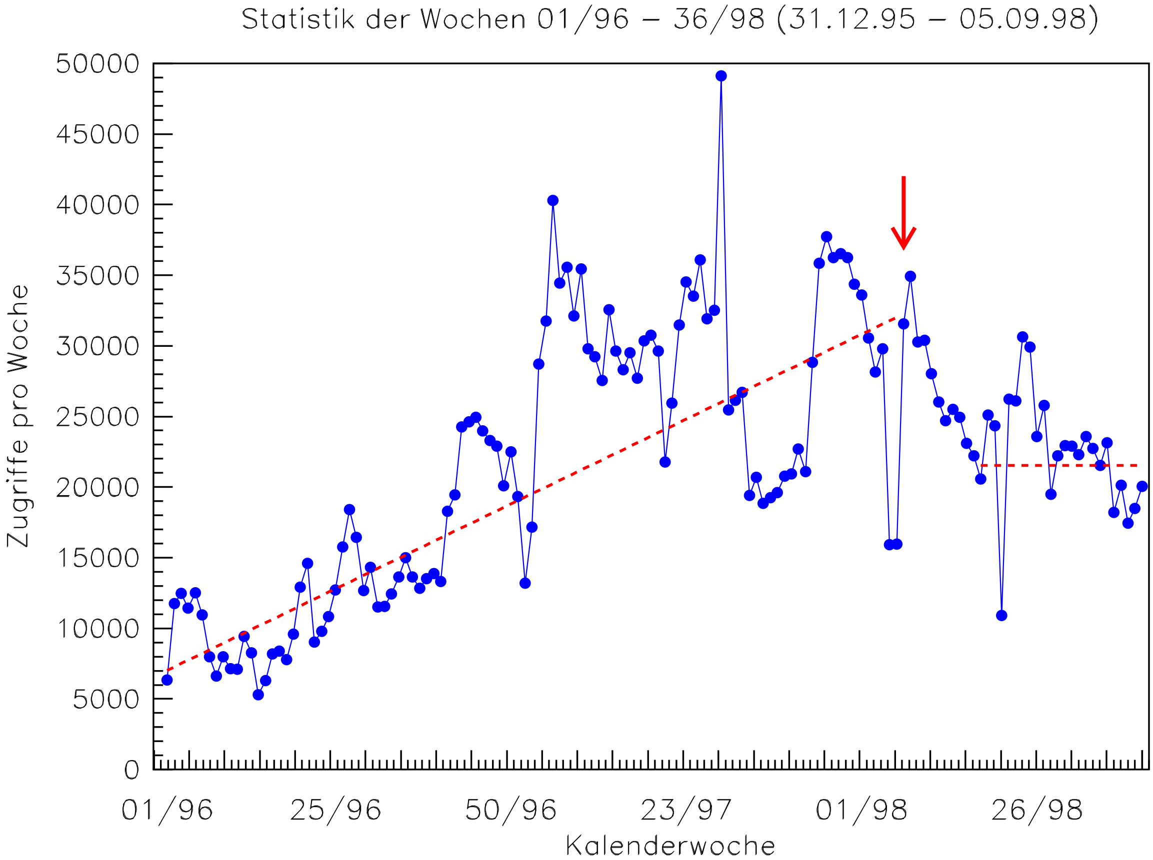
  `ambix-pgp-request@mail500.uni-tuebingen.de`

Statistik I*

- Bestand im X.500:
  - l=DFN
    - ◇ 120 Organisationen (davon 38 aktiv)
    - ◇ 4.350 Strukturdatensätze
    - ◇ bis zu 4 Hierarchieebenen
    - ◇ Verweis auf 25 Organisationen
    - ◇ 35.036 Personeneinträge (3 × vgl. 06/96)
    - ◇ ≃ 62% explizite Zustimmung
  - l=Einzelpersonen
    - ◇ 16 Bundesländer, 412 KFZ–Gebiete
    - ◇ 344 Personeneinträge
    - ◇ seit 1. Juli 1998 Selbsteintrag möglich
    - ◇ bisher 26 Selbsteinträge, Tendenz ↗
- Kontakt zu weiteren 4 Organisationen (aktive Beteiligung)
- AMBIX–DB
  - Widerspruchsfrist: 1.503 Personen
  - „Kiel–Modus“: 4.269 E–Mail–Adressen

*Stand 8. September 1998

Statistik II



- seit 1. Jan. 1996 (Stand 5. September 1998):
  - 3.470.268 Zugriffe, davon 375.444 keine Personendaten
  - 8.215 verschiedene Domains
- Woche 36/1998 (30.08 – 05.09):
  - 21.655 Zugriffe, davon 1.611 keine Personendaten
  - 554 verschiedene Domains

Aufbau und Betrieb eines Directory–Kompetenzzentrums

AMBIX–Datenbestand

•

Index–System

•

Zertifikatverzeichnisdienst

•

First–Level–DSA

•

Betriebssysteme

•

Directory–Produkte

Index–System! Wieso?

Problem: Suche

- X.500 verteilte Datenbank (DSAs)
- Erreichbarkeit einzelner DSAs
- gleiche Objektarten auf verschiedenen Hierachieebenen
- keine Beschränkung der Such–Tiefe
- $\Rightarrow$ Dauer !
- Replikation (RFC 1276, X.525) keine Lösung

White Pages IETF, Nov. 1993 (RFC 1588)
Frage: WP–Dienst; wie? Resultat: 4 Empfehlungen!

- *interoperation protocol*
- verschiedene Methoden zur Datenerfassung und Suche
- zentrales Management des X.500 Systems !?
- Unterstützung für Zertifikate

Index–System

- X.500 Index DSA (Paul Barker, März 1995)
  Mixtur aus Aliases und Replikation
- IndeX.500 (David Chadwick, Dante in Print #19, Mai 1996)
  Prinzip von Whois++ auf X.500
  Centroid–DSA hält DSA–Adressen und Liste der Attributwerte
- Schweden–Index (Roland Hedberg, August 1996) $\mapsto$ TISDAG
- Technical Infrastructure for Swedish Directory Access Gateways
  (TISDAG; http://tisdag.bunyip.com/) $\hookrightarrow$ CIP
- Centroid500 (Nils Meulemans, Dezember 1996)
  vgl. IndeX.500 aber Centroid zeigt auf Position im DIT
- Common Indexing Protocol (CIP; z.Z. 7 IETF Drafts)
  allgemeines Protokoll für verschiedene WP–Dienste
  (X.500, LDAP, Whois++, ...)
  Tagged Index Objects anstelle von Centroids

Zertifikatverzeichnisdienst

- Aufbau eines Zertifikatverzeichnisdienstes (X.500)
- Zertifikate, CRLs
- abgelaufene und gesperrte Zertifikate (Überprüfbarkeit)
- PGP, PEM, SSL, S/MIME, ...
  (Absprache mit DFN–PCA)
- evtl. SigG/SigV konform
- Evaluierung spezifischer Anwendungen
- Beobachtung der Entwicklungen auf dem Gebiet Security–Standards (IPv6, Secure–DNS, ...)

Betrieb und Betreuung des zentralen DSA (First–Level–DSA) in Deutschland

- Übernahme PUMA (bisher TU–Chemnitz)
  - Aufrechterhaltung des Directorybetriebs
  - Bereitstellung der internationalen Anbindung
- Umstellung auf den 93er Standard,
  Koordination und Management des *root naming context*
- Teilnahme an nationalen und internationalen Projekten (bsp. NameFLOW LDAP–Pilot)
- Bereitstellung der ISODE Software
- Bereitstellung der Informationen im WWW
- Betreuung und Beratung in directory–spezifischen Fragen
- 2000?

root naming context

Aktuell („88er Standard“):

- keine Replikation, ein First–Level–DSA pro Land
- *Quipu Knowledge Model*,
  Root–DSA, EDB–Update (RFC 1276)

93er Standard:

- Replikation, mehrere First–Level–DSAs
- DISP, DOP
- Master und Shadow First–Level–DSAs
- gemeinsame Verwaltung, multilaterale Vereinbarungen
- $\mapsto$ Probleme ?!

Lösungsvorschläge

- *Managing the X.500 Root Naming Context*
  (David Chadwick, RFC 2120, März 1997)
  - ein Master–Root–DSA
  - $\Rightarrow$ nur bilaterale Vereinbarungen
  - *one–level search* $\mapsto$ mehr Information im Ländereintrag
  - Konzept ist übertragbar auf Länderebene
- *Global Directory Service Backbones and Multi Master Operation – a contribution* (Alan Lloyd, April 1998, http://www.opendirectory.com/Whitepapers/addmds.htm)
  - Erweiterung und Ergänzungen am Standard
    - ADDMD *(Administrative Directory Management Domain)*
    - PRDMD *(Private Directory Management Domain)*
    - First–Level–DSAs
    - DSP *(Directory System Protocol)*

Definition First–Level DSA*

(...)

A first level DSA is characterized as follows:

a) it does not hold a superior reference;
b) it may hold one or more naming contexts immediately subordinate to the root of the DIT (as master or shadow DSA for the naming context); and
c) it holds a subordinate reference (of category master and/or shadow) for each naming context immediately subordinate to the root of the DIT that it does not itself hold

The administrative authorities for first level DSAs are jointly responsible for the administration of the immediate subordinates of the root of the DIT. The procedures governing this joint administration are determined by multilateral agreements which are outside the scope of the Directory Specification.

(...)

*vgl. X.501 (93) Abs. 18.5

Weitere Betriebssysteme / Produkte

- bisher „AMBIX–Software“ für UNIX (HP–UX)
- andere UNIX–Derivate (Sun–OS, LINUX, ...)
- M$ NT
  - NT–Portierung SLAPD
  - NT–Version des ISODE LDAP/X.500 Enterprise Directory Server (EDS)
  - Novell Directory Service (NDS)
  - Active Directory (AD), zentraler Bestandteil von NT 5.0
- Netscape Directory Server (NDS)
- Fragestellungen:
  - ? Systemanforderungen
  - ? Performance
  - ? Integration in AMBIX

Active Directory

- zentraler Bestandteil von NT 5.0
- Datenmodell X.500
- Zugang zu AD
  - LDAPv2, LDAPv3 (!?)
  - RPC
  - kein DAP, DSP, DISP und DOP
- *Application Programming Interfaces* (APIs)
  - *Active Directory Service Interface* (ADSI)
  - LDAP C API (RFC 1823)
  - *Windows Messaging* API (MAPI)

Novell Directory Service

- Datenmodell X.500
- LDAPv2, LDAPv3
- Abweichungen auf Protokollebene
  - NDS: **.** $\Leftrightarrow$ LDAP: **,**
  - `RS.ZDV.UT` $\mapsto$ `cn=RS.ou=ZDV.o=UT` (Schema)
  - `RS+ZDV` $\mapsto$ `cn=RS.ou=ZDV` (Schema)

Zusammenfassung

- Status AMBIX
- Erweiterung des Datenbestands
- Aufbau eines deutschlandweiten Index–Systems
- Aufbau eines öffentlichen Zertifikatverzeichnisdienstes (evtl. SigG/SigV konform)
- Evaluierung verschiedener Directory–Produkte, verschiedene Plattformen
- Betrieb (Master) First–Level–DSA
- $\Rightarrow$ Kompetenzzentrum für directory–spezifische Fragen