

Abschlußbericht
für
das Projekt

**Aufbau eines Directory
Kompetenzzentrums**

an der
Universität Tübingen

Zentrum für Datenverarbeitung,
Universität Tübingen

29. Januar 2001

Inhaltsverzeichnis

| | | |
|----------|--|-----------|
| 1 | Einleitung | 1 |
| 2 | DFN-E-Mail Verzeichnis AMBIX | 2 |
| 2.1 | Status | 2 |
| 2.2 | Öffentliche LDAP-Server | 3 |
| 2.3 | Benutzerzugriffe | 5 |
| 2.4 | WWW-Formular für Selbsteintrag und Datenänderungen | 6 |
| 2.5 | Datenschutzrechtliche Grundlage | 7 |
| 3 | Der zentrale Deutschland DSA und X.500 | 10 |
| 3.1 | Übernahme des zentralen Deutschland-DSA cn=PUMA von der TU Chemnitz | 10 |
| 3.2 | Bereitstellung der MessagingDirect-Software | 11 |
| 3.3 | Umstieg auf den X.500(93) Standard | 12 |
| 3.4 | Status des deutschen Directory-Teilbaums | 13 |
| 3.5 | Status des internationalen Directory | 16 |
| 3.6 | Neustrukturierung des Teilbaums c=DE | 17 |
| 4 | Indizierung von LDAP/X.500 Datenbeständen | 18 |
| 4.1 | Personen und Organisationsindex des Teilbaums c=DE | 18 |
| 4.2 | Unterstützung eines international standardisierten Directory- Index-Systems | 19 |
| 5 | Forschung und Entwicklung | 20 |
| 5.1 | Einbeziehung neuer Betriebssysteme und Plattformen | 20 |
| 5.2 | Aufbau einer PKI auf Basis von LDAP/X.500 | 20 |
| 6 | Support der DFN-Mitglieder | 22 |
| 6.1 | X.500 und LDAP | 22 |
| 6.2 | MessagingDirect/ISODE-Software | 22 |
| 7 | Betriebliche Aspekte | 22 |
| 7.1 | Rechnerinfrastruktur | 22 |
| 7.2 | Maßnahmen gegen das Jahr-2000-Problem | 25 |
| 7.3 | DFN Directory CA | 25 |
| 8 | Vorbereitungen zur Gründung einer GmbH | 25 |

| | | |
|----------|--|-----------|
| 9 | Öffentlichkeitsarbeit | 25 |
| 9.1 | Publikationen | 26 |
| 9.2 | Vorbereitungen zur Gründung eines Deutschen Directory Forums | 26 |
| 9.3 | Internet-Präsenz des Directory Kompetenzzentrums | 27 |
| | Literatur | 28 |

Tabellenverzeichnis

| | | |
|---|---|----|
| 1 | <i>Die vom Projekt betriebenen LDAP-Server für Benutzerabfragen über das WWW</i> | 4 |
| 2 | <i>Adressen der vom Projekt betriebenen DSAs</i> | 12 |
| 3 | <i>LDAP- und WWW-Zugang zu den vom Projekt betriebenen DSAs</i> | 14 |
| 4 | <i>Anzahl der DSAs innerhalb des Teilbaums $c=DE$. Im Aufbau befindliche DSAs in Klammern.</i> | 15 |
| 5 | <i>Anzahl der Organisationseinträge unterhalb $c=DE$.</i> | 15 |
| 6 | <i>Überblick über die Rechnerinfrastruktur</i> | 24 |

Abbildungsverzeichnis

| | | |
|---|--|---|
| 1 | <i>Anzahl der WWW-Zugriffe pro Woche</i> | 5 |
| 2 | <i>Das WWW-Formular zur Modifikation von Benutzerdaten</i> | 8 |
| 3 | <i>Das WWW-Formular zum Selbsteintrag von Benutzern</i> | 9 |

1 Einleitung

Das Projekt *Aufbau eines Directory Kompetenzzentrums* ist der Nachfolger der Projekte *AMBIX-D* [1], *AMBIX-II* [2] und *Ausbau und Nutzung des DFN-E-Mail-Verzeichnisses* [3].

In den Projekten *AMBIX-D* und *AMBIX-II* standen die Klärung organisatorischer und datenschutzrechtliche Fragen bezüglich des Aufbaus und Betriebs eines X.500 E-Mail-Verzeichnisses sowie die Erstellung eines Prototyps bzw. eines Produktionssystems für die automatische Verwaltung im Vordergrund. Das Projekt *Ausbau und Nutzung des DFN-E-Mail-Verzeichnisses* fokussierte, wie der Name bereits aussagt, stark auf den Ausbau des Verzeichnisses und dessen Nutzung und konnte durch verstärkte Öffentlichkeitsarbeit und die Bereitstellung von Arbeitserleichterungen weitere Organisationen für die aktive Teilnahme gewinnen. Aufbauend auf diesen umfangreichen Vorarbeiten und der dabei gesammelten Erfahrungen und Kompetenzen wurden im aktuellen Projekt alle X.500-Aktivitäten des DFN gebündelt und zusammengefaßt. Neben dem Betrieb und der Pflege des AMBIX-Verzeichnisses wurden vom Projekt zwei weitere Aufgaben übernommen, die vorher von Projekten an der TU Chemnitz¹ erfüllt wurden, nämlich der Betrieb des zentralen Deutschland-DSA `cn=PUMA,c=DE` sowie die zentrale Verteilung der MessagingDirekt-Software. Darüberhinaus leistet das Projekt als Kompetenzzentrum den Support der DFN-Mitglieder in allen Fragen im Bereich LDAP und X.500. Zur Jahreswende 1999/2000 wurde die Umstellung des zentralen Deutschland-DSAs auf eine aktuelle X.500-Implementation des Herstellers MessagingDirect vorgenommen, die durch die Jahr-2000-Unverträglichkeit der bis dato eingesetzten Quipu-DSA-Software notwendig wurde.

Schließlich hat sich das Projekt weiterhin an der Forschung beteiligt und die aktuellen Entwicklungen auf den Gebieten X.500 und LDAP verfolgt und mitgestaltet.

Diese hier kurz skizzierten Entwicklungen fanden gleichzeitig mit einer dramatischen Steigerung der allgemeinen Beliebtheit von verzeichnisbasierten Diensten statt, insbesondere mit den Technologien LDAP, Novell Directory Service und Microsoft Active Directory. Es kann als ein Glücksfall angesehen werden, daß die konsequente Förderung durch den DFN und das BMBF in diesem boomenden Bereich zu einer wertvollen Expertise geführt hat. Dies führte zu idealen Voraussetzungen für die nun geplante Gründung einer auf diesem Gebiet tätigen GmbH.

¹Projekt "Directory Infrastruktur" (7/96-12/97) und Projekt "ISODE-Referenzzentrum" (7/96-6/98)

2 DFN-E-Mail Verzeichnis AMBIX

2.1 Status

Einer der Hauptaufgaben des Projekts lag in der Pflege und der Erweiterung des DFN-E-Mail-Verzeichnisses AMBIX, welches gegenwärtig die Directory-Teilbäume

- l=DFN, c=DE
- l=Einzelpersonen, c=DE
- l=Schulen, c=DE

umfaßt.

Während der Laufzeit des Projekts konnte der Umfang des AMBIX-Datenbestands im Teilbaum l=DFN, c=DE von 35.000 auf 62.000 Personeneinträge gesteigert und damit nahezu verdoppelt werden. Als besonders positiv ist dabei zu vermerken, daß 77% der eingetragenen Personen der Veröffentlichung ihrer Daten explizit zugestimmt haben und dadurch weniger als ein Viertel über einen Ablauf der sechswöchigen Widerspruchsfrist aufgenommen wurden. Die Anzahl der Strukturdatensätze hat sich während der Laufzeit des Projekts von 4.350 auf 4.899 erhöht.

Die Steigerung sowohl der Personen- als auch der Strukturdatensätze ist zum Teil auf die Übernahme der Daten des außer Betrieb gestellten DSA der Universität Köln zurückzuführen. Ende des Jahres 1999 wurden desweiteren bereits Vorgespräche bezüglich einer eventuellen Übernahme des Datenbestandes des DSAs der Universität Frankfurt geführt.

Auch in dem nach Bundesländern und Gemeinden strukturierten Teilbaum l=Einzelpersonen, c=DE (428 Strukturdatensätze), in den Privatpersonen ohne Zugehörigkeit zu einer Organisation, insbesondere die WiNShuttle-Kunden eingetragen werden, stieg die Anzahl der Einträge auf 860. Der Großteil der hier eingetragenen Personen gelangte dabei über den Mechanismus des Selbsteintrages, unter Nutzung des hierzu eingerichteten WWW-Formulars, in das Verzeichnis. Von Seiten WiNShuttles, für deren Kunden dieser Teilbaum ursprünglich eingerichtet wurde, erfolgte bis dato leider nur eine einzige Datenlieferung über Privatpersonen. Andere WiNShuttle-Kunden-Klassen wurden überhaupt nicht geliefert, trotz mehrmaliger Nachfrage.

Für die Aufnahme der im Offenen Deutschen Schulnetz (ODS) registrierten Schulen in das AMBIX-Verzeichnis wurden dem Projekt von den Verantwortlichen des ODS Datenmaterial zur Verfügung gestellt. Nach geeigneter Aufbereitung und Konversion konnten diese Daten zum Anlegen der Struktureinträge

der Schulen verwendet werden. Analog zu den Privatpersonen wurde auch für die Schulen eine Einteilung des Teilbaums `l=Schulen,c=DE` nach Bundesländern und Gemeinden gewählt.

2.2 Öffentliche LDAP-Server

Benutzerzugriffe via WWW werden über den sogenannten *WWW-Forwarder* angenommen, der unter der Adresse `http://as.directory.dfn.de:8889` erreicht wird. Dieser *WWW-Forwarder* dient als Weiche zur Verteilung der Last der HTTP-Anfragen auf diverse WWW-LDAP-Gateways. Dieses Load Balancing kann so gesteuert und der Leistungsfähigkeit des Hosts entsprechend angemessen verteilt werden.

Bei den für die Benutzeranfragen bestimmten Servern handelt es sich um Standardone LDAP-Server (SLAPD) aus dem bewährten LDAP-3.3-Paket der University of Michigan. Als Hosts dienen ein Linux-PC (Pentium II/333MHz) und eine HP 9000 Workstation (712/80, HPUX 10.20). Der Referenzbestand wird weiterhin auf einem X.500-DSA gepflegt. Tab. 1 gibt einen Überblick über die vom Projekt für das AMBIX-Verzeichnis betriebenen Server und die zugehörigen LDAP-Web-Gateways TWEBS.

| Host | SLAPD-Port | TWEB-Port | Subtree |
|-----------------------|------------|-----------|--------------------------|
| as.directory.dfn.de | 10110 | 10111 | l=DFN,c=DE |
| as.directory.dfn.de | 10210 | 10211 | l=DFN,c=DE |
| hp02.directory.dfn.de | 10110 | 10111 | l=DFN,c=DE |
| hp02.directory.dfn.de | 10210 | 10211 | l=DFN,c=DE |
| as.directory.dfn.de | 10310 | 10311 | l=Einzelpersonen,c=DE |
| hp02.directory.dfn.de | 10310 | 10311 | l=Einzelpersonen,c=DE |
| as.directory.dfn.de | 10810 | 10811 | l=Schulen,c=DE |
| as.directory.dfn.de | 10510 | 10511 | l=Namensindex,l=DFN,c=DE |
| as.directory.dfn.de | 10610 | 10611 | l=Namensindex,l=DFN,c=DE |
| as.directory.dfn.de | 10710 | 10711 | l=Orgindex,c=DE |

Tabelle 1: Die vom Projekt betriebenen LDAP-Server für Benutzerabfragen über das WWW

2.3 Benutzerzugriffe

Der Zugriff auf die AMBIX-Daten durch die Benutzer erfolgt über das konfigurierbare und intelligente WWW-LDAP-Gateway TWEB. Die Anzahl der zugelassenen Benutzerzugriffe lag während der Projektlaufzeit im Mittel bei ca. 21.500 Zugriffe pro Woche. Weitere 2000 - 3000 Zugriffe werden jede Woche aufgrund der durch den Datenschutz auferlegten Zugriffsbeschränkungen abgelehnt. Der unauthorisierte Zugriff auf die Daten über X.500-Protokolle (DAP, DSP, DISP) oder LDAP kann dem Benutzer ebenfalls aufgrund der datenschutzrechtlichen Vorgaben nicht gewährt werden. Die letzte Aktualisierungsaktion, welche Anfang

Zugriffsstatistik (31.12.1995 - 22.05.2000)

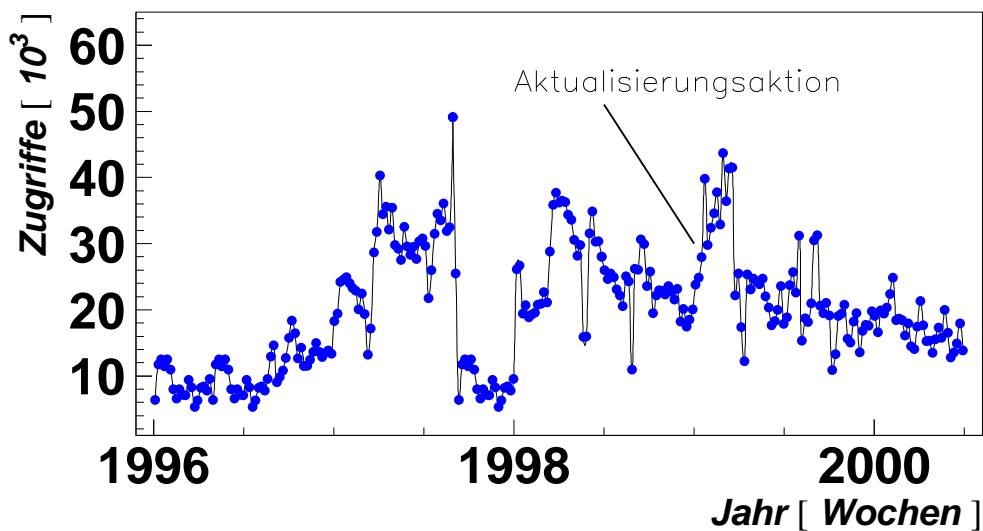


Abbildung 1: Anzahl der WWW-Zugriffe pro Woche

1999 durchgeführt wurde und in deren Rahmen alle bei AMBIX eingetragenen Benutzer aufgefordert wurden die Aktualität ihrer Einträge zu überprüfen führte, wie Abb. 1 entnommen werden kann, zu einem sehr deutlichen Anstieg der Benutzerzugriffe. Seit Mitte 1999 sinken die Benutzerzugriffe tendenziell etwas ab. Für die zu gründende GmbH kann hieraus die Notwendigkeit abgeleitet werden verstärkt Werbung für die angebotenen Dienste zu betreiben. Dem Projekt war bislang das Verfolgen einer entsprechenden Marketingstrategie, auch aus finanziellen Gründen, nicht möglich.

2.4 WWW-Formular für Selbsteintrag und Datenänderungen

In Hinblick auf die Steigerung der Benutzerfreundlichkeit wurden zwei WWW-Formulare entwickelt. Das erste bietet den Benutzern die Möglichkeit Daten selbst in das Verzeichnis einzutragen, sofern die entsprechende Organisation es an dieser Stelle erlaubt. Das zweite Formular ermöglicht es einem bereits eingetragenen Benutzer selbst Modifikationen an seinen Daten vorzunehmen. Beide WWW-Formulare sind in der Programmiersprache PERL entwickelte CGI-Skripte. Vom Benutzer können sie im Browser aus dem TWEB heraus über einen Button aufgerufen und ausgefüllt werden. Eingabe und Formatfehler, die beim Ändern oder Ausfüllen auftreten, werden durch eine sofortige formale Prüfung erkannt und dem Benutzer angezeigt, so daß sie korrigiert werden können. Erst wenn keine Fehler mehr im Formular vorhanden sind, gelangt der Benutzer auf eine Kontrollseite. Hier können die angegebenen Daten, deren Aussehen und die Funktion der HTML-Verweise (z. B. auf die Homepage des Benutzers) überprüft werden. Auf dieser Seite kann der Benutzer nun die Änderungen bzw. den Eintrag seiner Daten veranlassen oder das Skript verlassen. Im ersten Fall werden die Daten in eine Datei gespeichert, im zweiten Fall verworfen.

Um Mißbrauch auszuschließen wird bei Personendatenänderungen an die bereits bekannten E-Mail Adressen des Benutzers eine E-Mail verschickt. Diese Mail enthält einen eindeutigen Einmalschlüssel, mit dem eine Authentifizierung des Benutzers und die Zuordnung zur bei AMBIX verbliebenen Datei ermöglicht wird. Um die Änderungen zu aktivieren, muß vom Benutzer wenigstens eine dieser E-Mails innerhalb einer bestimmten Zeitspanne an das Projekt zurückgeschickt werden. In regelmäßigen Abständen werden diese zurückgeschickten Bestätigungsmails abgearbeitet und die Änderungen aus den zugeordneten Dateien bearbeitet. Daten, für die nach der konfigurierten Zeit noch keine Bestätigung vorliegt, werden verworfen und die zugeordneten Dateien gelöscht.

Alle wichtigen Parameter dieses Scripts sind frei konfigurierbar. Zu nennen sei hier vor allem die Zeitspanne, nachdem die in der Datei gespeicherten Änderungen ihre Gültigkeit verlieren, sowie das Ausgabeformat der Datei. Für die automatische Verarbeitung der erzeugten Dateien wurden weitere Programme neu entwickelt und in die bestehende Software integriert.

Im Falle eines Selbsteintrages durch einen Benutzer wird die Kontaktperson (DS-Manager) der jeweiligen Organisation via E-Mail über diesen Vorgang unterrichtet. Von Seiten der Organisation kann dann ein Veto gegen diesen Selbsteintrag erhoben werden.

Sowohl das Änderungsformular als auch das Selbsteintragsformular werden

rege von den Benutzern genutzt und haben sich in der Praxis bewährt. Seit Mai 1999 wurden über die beiden Formulare 1850 Personeneinträge angelegt bzw. aktualisiert.

Neben den Benutzern profitiert auch das Projekt von den WWW-Formularen, da aufgrund der integrierten Prüfung der eingetragenen Werte die vom Benutzer gemachten Angaben keine formalen Fehler enthalten und so die Verarbeitung dieser Daten erleichtert wird.

Die Anzahl der Fälle in denen das Formular mißbräuchlich eingesetzt wurde, in denen also ein Benutzer nicht die eigenen, sondern die Daten eines anderen Benutzers modifizieren wollte, ist erfreulich gering.

2.5 Datenschutzrechtliche Grundlage

Die dem Projekt als Arbeitsgrundlage dienende Datenschutzexpertise stammt aus dem Jahre 1993. An einer Novellierung und Anpassung der Expertise an die veränderte deutsche und europäische Gesetzgebung besteht mehr denn je dringender Bedarf. Eine Entspannung bei den geltenden Richtlinien würde nicht nur die Möglichkeiten schaffen, die Attraktivität angebotener Dienste zu steigern, sondern darüber hinaus die Entwicklung neuer Dienste, wie zum Beispiel eines LDAP-Proxies gestatten. Sinnvollerweise sollte diese Anpassung nach der in Kürze zu erwartenden Novellierung des Bundes-Datenschutzgesetzes erfolgen. Allgemein scheint die Frage des Schutzes von Verzeichnisinhalten mittlerweile von den Datenschützern moderater und realistischer eingeschätzt zu werden.

Diese Software hat gerade unser Labor verlassen. Sie sollte fehlerfrei funktionieren. Sollten Sie dennoch Fehler finden, so zögern Sie nicht, sich bei uns unter folgender E-Mail-Adresse zu melden: ambix-d@directory.dfn.de

Hinweis: Die Daten auf das Personalverzeichnisformular werden von Sie betriebsführenden mit Ihrer ID und Nachnamen gespeichert!

AMBIX-Personenformular für

Markus Sauer



[Hinweise zum Ausfüllen des Formulars](#)

- Eintrag [ändern](#)
- Eintrag in X.500 und in der internen Datenbank (**nicht E-Mail-Adresse**) [löschen](#)
- Eintrag in X.500 und in der internen Datenbank **komplett** [löschen](#)

Organisation:

AMBIX

Unterorganisation:

Nachname:

Vorname(n):

Akad. Titel:

E-Mail-Adresse(n):

Telefonnummer(n):

Faxnummer(n):


Arbeitsgebiet:

Homepage(s):


Abbildung 2: Das WWW-Formular zur Modifikation von Benutzerdaten


Hinweis: Die Zugriffe auf das Personenänderungsformular werden aus Sicherheitsgründen mit Uhrzeit und Rechnername geloggt!


AMBIX-Personenformular für


[Hinweise zum Ausfüllen des Formulars](#) 


Eintrag neu anlegen


Organisation:  Berufsakademie Karlsruhe


Unterorganisation:  Fachrichtung Handel


Nachname: 


Vorname(n): 

Akad. Titel: 

E-Mail-Adresse(n): 

Telefonnummer (n): 

Faxnummer (n): 

Arbeitsgebiet: 


Homepage(s): 

Abbildung 3: Das WWW-Formular zum Selbsteintrag von Benutzern

3 Der zentrale Deutschland DSA und X.500

3.1 Übernahme des zentralen Deutschland-DSA cn=PUMA von der TU Chemnitz

Der Betrieb des zentralen Deutschland-DSAs cn=PUMA wurde am 25. Januar 1999 von der TU Chemnitz übernommen. Um die Übergabe vorzubereiten fanden zwei Treffen zwischen dem “alten“ und dem neuen DSA Manager am 4. und 5. August sowie vom 8. bis 10. Dezember 1999 in Chemnitz statt. Ziel des ersten Treffens war eine Aufnahme des vorhandenen Datenbestands und der eingesetzten Softwaretools vorzunehmen. Als wichtiges Ergebnis dieses Treffens entstand eine Liste mit Punkten, die erfüllt werden mußten, um eine reibungslose Übergabe und Umstellung des Betriebs des zentralen DSA zu gewährleisten. Im Zeitraum zwischen den beiden Treffen wurden Lösungsmodelle für die Umsetzung der verschiedenen Punkte erarbeitet und beim zweiten Treffen besprochen, sowie auf ihre praktische Durchführbarkeit hin getestet. Für die Übergangszeit wurde in Tübingen ein DSA installiert, der alle Einträge des cn=Puma beinhaltete und via Replikation aktualisiert wurde. Bei der eigentlichen Übersiedelung von Chemnitz nach Tübingen mußten dann lediglich die *PresentationAddress* der beiden DSAs vertauscht werden.

Für verschiedene andere Dienste wurden Mechanismen zur Weiterleitung der Anfragen installiert. Diese sind in nachfolgender Liste zusammengefaßt.

WWW: auf der alten WWW-Adresse (<http://tricia.hrz.tu-chemnitz.de>) wurde eine Seite mit Hinweisen auf die neuen Adressen installiert, die nach einer Übergangszeit durch einen automatischen *redirect* auf die neue WWW-Adresse (<http://www.directory.dfn.de>) ersetzt wurde,

Web500gw: für eine Übergangszeit wurde auf der Adresse des Chemnitzer Web500gw (<http://x500.tu-chemnitz.de:8888>) das bereits erwähnte Programm WWWForwarder installiert. Damit wurde eine automatische Weiterleitung aller Anfragen auf die Chemnitzer WWW-Seite realisiert. Dort befand sich zu dieser Zeit ein Hinweis auf die neue Eingangsadresse vom TWEB (<http://puma-relay.directory.dfn.de:8901>),

LDAPD: auf der Adresse des LDAPD (tricia.hrz.tu-chemnitz.de, Port 389) wurde der *stand-alone LDAP Server* (SLAPD) der Univeristy of Michian installiert. Dieser Server enthält keinerlei Daten sondern nur einen sog. *referral* auf die Adresse des für Puma in Tübingen installierten LDAPD (puma-relay.directory.dfn.de, Port 1389). Damit werden alle

LDAP-Anfragen automatisch nach Tübingen weitergeleitet. Der SLAPD (in Chemnitz) soll abgeschaltet werden, nachdem dort die Anzahl der Anfragen auf ein Minimum zurückgegangen sind.

Die Bekanntgabe der neuen *PresentationAddress* von `cn=Puma` an den X.500(88)-Root DSA `cn=Giant Tortoise` und damit an alle anderen Länder-DSAs erfolgte automatisch. Direkte Eingriffe der Administratoren waren nur bei DSAs notwendig, die den Root-EDB direkt von Puma bezogen. Alle deutschen DSA Administratoren wurden in einer Mail auf die Umstellung der Adresse hingewiesen und gebeten, gegebenenfalls eine manuelle Umstellung an ihren DSAs vorzunehmen sowie die Aktualität ihrer DSA-Einträge zu überprüfen. Nur ungefähr die Hälfte der angeschriebenen Administratoren haben entsprechende Informationen an das Projekt zurückgeschickt.

Alle Änderungen in Bezug auf den `cn=Puma` wurden DANTE, dem Betreiber der internationalen Wurzel des X.500-Projekts NameFLOW bekannt gegeben, so daß dort die entsprechenden Informationen aktualisiert werden konnten. Bei einem Vortrag auf dem NameFLOW-Meeting in Utrecht (18. Jan. 1999) wurden nochmals alle Änderungen bekanntgegeben. Diese Gelegenheit wurde ebenfalls dazu genutzt, das DFN-Projekt AMBIX im internationalen Rahmen zu präsentieren sowie die internationalen Kontakte zu pflegen. In Hinblick auf die bevorstehende Umstellung auf die 93er Version des X.500 Standards wurde zwischen DANTE, dem schweizer Forschungsnetz SWITCH und dem Projekt die Durchführung von 93er Tests vereinbart.

3.2 Bereitstellung der MessagingDirect-Software

Neben der Betreuung des zentralen Deutschland-DSAs wurde vom Projekt auch die Bereitstellung der MessagingDirect(früher ISODE)-Software von der TU Chemnitz übernommen, sowohl der frei verfügbaren Versionen als auch der kostenpflichtigen IC-Releases die im Rahmen einer DFN-Lizenz DFN-Mitglieds-Institutionen kostenfrei zur Verfügung stehen. Hierfür wurde ein FTP-Server eingerichtet, der unter der Adresse

`ftp://ftp-isode.directory.dfn.de`

erreichbar ist. Freigegebene neue Releases werden durch das Projekt vom MessagingDirect-Server heruntergeladen und nach geeigneter DES-Verschlüsselung auf dem öffentlich zugänglichen FTP-Server des Projekts abgelegt. Das zur Entschlüsselung benötigte Password wird lediglich den berechtigten DFN-Mitgliedsorganisationen mitgeteilt. Neben der freien Version 8 der ISODE-

| Distinquished Name | Naming Kontext | Presentation Address |
|--------------------------------------|-----------------------|--|
| cn=Puma , c=DE | c=DE | '0101'H/Internet= 134.2.217.133+17023 |
| cn=welt.dsa,l=Welt | l=Welt | '0101'H/Internet= 134.2.217.133+18003 |
| cn=dfn.dsa,l=DFN,c=DE | l=DFN,c=DE | '0101'H/Internet= 134.2.217.133+15003 |
| cn=ezp.dsa, l=Einzelpersonen,c=DE | l=Einzelpersonen,c=DE | '0101'H/Internet= 134.2.217.133+16003 |

Tabelle 2: Adressen der vom Projekt betriebenen DSAs

Software sind zum gegenwärtigen Zeitpunkt alle kostenpflichtigen Releases bis hin zum aktuellen Release *IC-R6.0v3 Patchlevel 1* verfügbar.

Auf Nachfrage hat MessagingDirect im Okt. 1999 den bislang nicht im DFN-Vertrag enthaltenen Directory Data Manager (DDM) dem DFN ohne Mehrkosten zur Verfügung gestellt und ist daher seit dem Release IC-R5.0v2 im DFN-Paket enthalten.

3.3 Umstieg auf den X.500(93) Standard

Weil laut Hersteller die bislang für den Deutschland-DSA und für die DSAs des AMBIX-Datenbestands eingesetzte X.500(88) konformen ISODE-Software Quipu nicht jahr-2000-kompatibel ist, wurde für die sichere Gewährleistung des Dienstes eine Umstellung auf die aktuelle Implementation IC-R5.0v2p1 des X.500(93) Standards von MessagingDirect (MD) vor Ende des Jahre 1999 notwendig. Wegen grundlegender Unterschiede, sowohl im Standard, als auch in der Software, mus-

ste eine sehr aufwendige Migration der Serverinhalte durchgeführt werden. Die hierzu notwendigen Schritte wurden als Anleitung in Form eines Kochbuchs [4] zusammengefasst und zusammen mit den hierzu erstellten Software-Tools allen interessierten DSA-Betreibern zur Verfügung gestellt².

Ebenfalls Ende 1999 fanden in Zusammenarbeit mit der Universität Nürnberg-Erlangen, an der DSAs mit Software des Herstellers Syntegra (ehemals Control Data) betrieben werden, intensive Tests bezüglich der Replikation (*shadowing*), also das Kopieren von Daten zwischen verschiedenen Servern, statt. Leider mussten dabei größere Mängel in der Interoperabilität der verschiedenen Implementationen festgestellt werden, die derzeit eine Replikation unmöglich machen.

Während ein *primary shadowing* zwischen DSAs des Herstellers MessagingDirect (MD) problemlos funktioniert, treten leider auch Probleme auf, wenn ein *secondary shadowing*, also die erneute Replikation bereits replizierter Daten, durchgeführt werden soll. Einige Verbesserungen in Hinsicht auf die Replikation wurden von dem seit Ende Januar verfügbaren Release IC-R6.0v3 der MD-DSA-Software erwartet. Seit dem 16. März wird der Deutschland-DSA und alle vom Projekt betriebenen DSAs mit dieser Version betrieben. Mitte Mai wurden erneute Tests der Replikationsmechanismen unter Einbeziehung der aktuellsten Syntegra-Software durchgeführt. An dem Zustand mangelnder Interoperabilität der Produkte in Bezug auf die Replikation hat sich leider nichts geändert.

Aufgrund der momentanen Rechnerinfrastruktur des Projekts (siehe 6) und des Umstandes, daß als geeignete Plattformen für die MD-Software nur Solaris 2.6 und Windows NT in Frage kommen, die bislang eingesetzte Plattform HPUX hingegen nicht mehr unterstützt wird, haben sich die Adressen der vom Projekt unterhaltenen DSAs geändert (siehe Tab.1 und Tab.2).

3.4 Status des deutschen Directory-Teilbaums

Im Zuge der Umstellungen auf X.500(93) wurde Kontakt mit allen bekannten Betreibern von DSAs aufgenommen, zum einen, um die Betreiber über die bevorstehende Umstellung zu informieren, und zum anderen, um einen Überblick über die zukünftige X.500-Landschaft in Deutschland zu erhalten. Tabelle 4 fasst die Anzahl der in c=DE eingebundenen X.500-DSAs zusammen, aufgeschlüsselt nach Herstellern und Software-Versionen. Die angegebenen Zahlen beinhalten keine DSAs, die zusätzlich einrichtungsintern, als Testinstallationen oder als reine Backup- bzw. Shadow-DSAs eingesetzt werden. Einige der aufgeführten DSAs verwalten Daten von mehr als einer Einrichtung. In Klammern sind die im Aufbau befindlichen DSAs angegeben, die noch nicht online sind. Bei weiteren 9 DSAs

²<http://www.directory.dfn.de/dirco/88-2-93/88-2-93.html>, im Anhang beigelegt

| Distinguished Name | LDAP-Zugang | WWW-Zugang |
|------------------------------------|--------------------------------------|--|
| <code>cn=Puma,c=DE</code> | ldap-relay .directory.dfn.de:1122 | puma-relay .directory.dfn.de:8900 |
| <code>cn=welt.dsa,l=Welt</code> | ldap-relay .directory.dfn.de:2233 | puma-relay .directory.dfn.de:8911 |
| <code>cn=dfn.dsa,l=DFN,c=DE</code> | ldap-relay .directory.dfn.de:3344 | puma-relay .directory.dfn.de: 10111 |
| <code>cn=ezp.dsa,l=DFN,c=DE</code> | ldap-relay .directory.dfn.de:4455 | puma-relay .directory.dfn.de:10311 |

Tabelle 3: *LDAP- und WWW-Zugang zu den vom Projekt betriebenen DSAs*

ist der Status noch unbekannt. Derzeit sind unterhalb `c=DE` 2 DSAs eingetragen, die noch mit Implementationen des 88er Standards betrieben werden. Von beiden ist bekannt, dass sie in naher Zukunft durch einen aktuellen X.500(93) MD-DSA ersetzt werden. Laut den Betreibern wurden bislang, entgegen den Befürchtungen der Hersteller, keine Jahr-2000-Unverträglichkeiten beobachtet die über das vorhergesagte Versagen des bei den 88er DSAs eingesetzten Replikationsmechanismus hinausgehen.

Im Falle des Deutschland-DSA `cn=Puma,c=DE` wurde die Umstellung auf X.500(93) genutzt, um alle Organisationseinträge im deutschen Directory-Teilbaum, welche zum Teil seit Jahren ungepflegt waren, zu validieren und, sofern angebracht, zu aktualisieren bzw. zu löschen. Per E-Mail und Telefon wurde hierzu im Dezember 1999 Kontakt zu allen Organisationen aufgenommen. Nach Überprüfung der Richtigkeit und Aktualität der im Eintrag abgelegten Daten durch die kontaktierte Einrichtung wurde der Organisationseintrag in den neuen 93er Deutschland-DSA übernommen. Einträge von Organisationen, bei denen die Kontaktaufnahme gescheitert ist bzw. eine Antwort noch aussteht, wurden

| DSA | MD 93er | Syntegra 93er | MD/Syntegra 88er | Gesamt | Status ? |
|---------------|---------|---------------|------------------|--------|----------|
| Anzahl | 6 (4) | 4 | 2 | 12 (4) | 9 |

Tabelle 4: Anzahl der DSAs innerhalb des Teilbaums $c=DE$. Im Aufbau befindliche DSAs in Klammern.

noch nicht übernommen. Bei dieser Aktualisierungsaktion fanden die in [2] (Anlage B) definierten Richtlinien bezüglich der Qualität von Verzeichniseinträgen Anwendung.

Tabelle 5 gibt einen Überblick über die Anzahl der momentan im deutschen Teilbaum eingetragenen Organisationen. Aufgeschlüsselt wird dabei, ob der Eintrag von $cn=Puma$ oder von einem organisationseigenen DSA verwaltet wird, bzw., ob es sich um einen Aliaseintrag handelt, der auf einen Organisationseintrag im $l=DFN$ -Teilbaum verweist. 96 Einrichtungen, die vor der Umstellung unter $c=DE$ eingetragen waren, haben nicht auf das Anschreiben reagiert, in dem Sie um die Validierung ihres Eintrages gebeten wurden. Diese Einrichtungen wurden Anfang März in einem zweiten Durchlauf erneut angeschrieben, worauf 3 Organisationen um einen Eintrag baten.

| Typ | Puma | Org-DSA | Alias auf $l=DFN$ | Gesamt | Status ? |
|-----------------------|------|---------|-------------------|--------|----------|
| Organisationen | 37 | 13 | 83 | 133 | 93 |

Tabelle 5: Anzahl der Organisationseinträge unterhalb $c=DE$.

Konzeptionell brachte die Umstellung zwei technische Änderungen mit sich. Erstens wird das bislang realisierte Konzept der Regional-DSAs, zumindest bis auf weiteres, wegen einer zu geringen Gesamtanzahl nicht weiter verfolgt. Zweitens muss, aufgrund mangelnder Interoperabilität zwischen den X.500-Implementierungen der unterschiedlichen Hersteller, zur Zeit auf die Replikation von Serverinhalten verzichtet werden. Die Anbindung der in den Einrichtungen

betriebebenen X.500-Server erfolgt in Form von *subordinate References* bzw. von *cross References*.

Zur Entlastung des Deutschland-DSAs bei Benutzeranfragen von Länder-DSAs wird der DSA *cn=welt.dsa,l=Welt* betrieben. Er verfügt über ein eigenes LDAP- und WWW-Gateway und verwaltet die selben Verweise auf Länder-DSAs wie der *cn=Puma,c=DE*.

Das Schema des neuen 93er Deutschland-DSA wurde dahingehend erweitert, dass LDAPv3-Referrals eingetragen werden können. Damit ist ein erster und wesentlicher Schritt in Richtung eines hybriden Directory aus X.500-DSAs und den sehr populären LDAP-Servern getan. Parallel hierzu wurde in die WWW-Gateway Software TWEB die Fähigkeit integriert, LDAP-Referrals zu folgen.

Dieser Referral-Mechanismus wurde erfolgreich mit einem LDAP-Server der Fakultät für Informatik der TU München getestet. Weitere Anfragen bezüglich der Einrichtung eines solchen Verweises auf organisationseigene LDAP-Server liegen dem Projekt bereits vor.

3.5 Status des internationalen Directory

Der internationalen Verknüpfung der Länder-Teilbäume und der Replikation der First-Level-DSAs lag in der 88er Version des X.500-Standards das Konzept des Root-DSAs zugrunde. Der Root-DSA wurde von DANTE im Rahmen des NameFLOW-Paradise Projekts³ gepflegt. Auf dem Deutschland-DSA sind derzeit über Kreuzverweise alle existierenden Länder-DSAs eingetragen. Ihre Anzahl beträgt derzeit 15, wobei es sich bis auf zwei noch um 88er DSAs handelt.

Mitte Januar 2000 fand in London ein von DANTE veranstaltetes internationales Treffen der Betreiber von Länder-DSAs statt. Seitens des Projekts wurde dort über den Status des deutschen Teilbaums und die Entwicklung des Directorys in Deutschland berichtet.

Durch den Wegfall des Root-DSAs im X.500(93), und damit eines zentralen Knoten über den eine Replikation der verschiedenen Länder-Teilbäume ablaufen kann, müssten zwischen den Länder-DSAs jeweils direkte Replikationsvereinbarungen getroffen werden. Bei n involvierten DSAs würde die Anzahl der hierfür notwendig werdenden Vereinbarungen (*shadowing agreements*) $2n$ betragen und der administrative Aufwand dementsprechend sehr hoch sein. Ein von NameFLOW-Paradise vorgestelltes Konzept, das einen zentralen Replikations-DSA beinhaltet, verspricht hierfür eine Lösung anzubieten. Kern dieser Lösung ist dabei, dass die Inhalte alle Länder-DSAs auf diesen Replikations-DSA repliziert und von dort weiter verteilt werden. Die Anzahl der zu vereinbarenden

³<http://www.dante.net/nameflow.html>

Replikationsvereinbarungen würde damit auf $n + 1$ reduziert.

In enger Zusammenarbeit mit NameFLOW-Paradise und den Betreibern des belgischen First-Level-DSA engagiert sich das Projekt seit Anfang des Jahres intensiv bei den Tests dieses Konzeptes. Damit nimmt das Projekt in den internationalen Bemühungen zur Etablierung des Directorys und des X.500(93)-Standards eine zentrale Rolle ein.

3.6 Neustrukturierung des Teilbaums c=DE

Aufgrund der kontinuierlichen Zunahme von Organisationseinträgen im deutschen Teilbaum des X.500 wurde es notwendig, dessen Neustrukturierung zu planen. Hierzu wurden verschiedene Modelle aufgestellt und der deutschen Directory-Betreiber-Gemeinde vorgestellt u.a. im Rahmen eines vor allem zu diesem Thema veranstalteten Symposiums. Zum Abschluß dieser Diskussionen wurde eine Dokument [5]⁴ erstellt, in dem der Ist-Zustand und dessen Probleme, sowie die entsprechenden Standard Texte zu diesem Thema beschrieben, und die mehrheitsfähigste und im Einklang mit den Standards Strukturierung nach geographischen Gesichtspunkten definiert. Schliesslich wird in dem Dokument das Konzept von "Sichtweisen" eingeführt, mittels dessen man andere Strukturierungsmöglichkeiten als Verweise implementieren kann. Die Durchführung dieser Neustrukturierung steht noch aus.

⁴im Anhang beigefügt

4 Indizierung von LDAP/X.500 Datenbeständen

Wie bereits schon länger prognostiziert ist das Interesse an der Indizierung von Serverinhalten allgemein gestiegen, nicht zuletzt, weil eine Indizierung die Möglichkeit schafft, die Inhalte verschiedener Server plattformunabhängig zusammenzufassen und zu erschließen. Durch Indizierung lokaler, nicht verteilter Datenbanken ist eine Integration auch dieser Dateninseln in die Directory-Landschaft realisierbar. Sehr vorteilhaft ist, dass keine schützenswerten Daten auf dem Indexserver abgelegt werden, sondern lediglich Verweise auf die Server bereitgestellt werden, welche diese Daten verwalten. Die Authentifizierung und Autorisierung für den Zugriff erfolgt daher nicht durch den Indexserver, sondern durch den die Daten verwaltenden Server.

4.1 Personen und Organisationsindex des Teilbaums c=DE

Der vom Projekt gepflegte deutschlandweite Personenindex wurde durch die Hinzunahme weiterer X.500/LDAP-Server im Teilbaum c=DE ausgebaut. Momentan integriert der Namensindex 11 LDAP-Server bzw. DSAs und umfaßt ca. 130.000 Verweise auf Personen. Die zur Generierung des Personenindex eingesetzte Software wurde so modifiziert, dass auch ein durchsuchbarer Index der Organisationen und Unterorganisationen im deutschen Teilbaum aufgebaut werden kann. Dieser Organisationsindex⁵ enthält zur Zeit ca. 7.700 Einträge und wird zunehmend von den Benutzern frequentiert.

Für die nahe Zukunft ist geplant, den Index auf von Organisationen eingesetzte NDS-Server (Novell Directory Services) auszudehnen und auch Microsofts Active Directory (AD) einzubeziehen, welches als zentraler Bestandteil des erst seit kurzem verfügbaren Betriebssystems Windows 2000, dem Nachfolger von Windows NT 4, eine zunehmende Bedeutung erlangen wird.

Sowohl der Personen- als auch der Organisationsindex basieren auf dem vom Projekt entwickelten proprietären Modell und sollen baldmöglichst durch die im Rahmen des DESIRE-Projekts entwickelte, international standardisierte Lösung ersetzt werden, die im Folgenden beschrieben wird.

⁵WWW-Zugang unter <http://ambix.directory.dfn.de:10711>

4.2 Unterstützung eines international standardisierten Directory-Index-Systems

Bei einer Evaluierung der verschiedenen Ansätze für Directory-Index-Systeme hat sich ergeben, dass die einzigen als internationaler Standard durchsetzbaren Systeme auf dem IETF Protokoll CIP (*Common Indexing Protocol*) aufbauen. Im Rahmen des EU-geförderten Projekts DESIRE II wurde ein solches System für die europäische Forschungsgemeinde konzipiert und implementiert. Mitarbeiter des Projekts waren an beiden Phasen beteiligt und haben wesentliche Bestandteile der Software entwickelt.

Zusammengefaßt stellt sich das System folgendermaßen dar: Ein Datencrawler zieht die Daten von registrierten DSAs (X.500 oder LDAP) ab und produziert Dateien im Format LDIF (*LDAP Date Interchange Format*). Diese Dateien werden konvertiert zu TIOs (*Tagged Index Objects*), deren Format in CIP definiert wurde. Diese TIOs werden dann an den Index-Server via HTTP verschickt, wo die Daten in eine SQL-Datenbank aufgenommen werden. Diese Netzübertragung kann PGP-verschlüsselt stattfinden. Der Index-Server stellt ein Datenbank-Backend für einen speziell angepassten LDAP-Server dar, der LDAPv3 Clients mit aus den TIO-Daten gebildeten LDAPv3-Verweisen (*referrals*) bedient. Die Clients werden durch die *Referrals* auf den Datenserver verwiesen, der die gesuchten Daten vorhält.

Augenblicklich wird mit diesem System im Rahmen einer ad hoc Arbeitsgruppe, an der neben unserem Projekt die Forschungsnetze der Niederlande, Norwegens und Schwedens beteiligt sind, ein europäischer Index-Dienst aufgebaut. Das Projekt stößt hierbei auf datenschutzrechtliche Probleme: Es macht bei der augenblicklichen Verfahrensweise einer Zugriffsbeschränkung für AMBIX-Daten auf datenschutztreibende Länder, die auf HTTP-Ebene im Web-Gateway TWEB realisiert sind, wenig Sinn, LDAP-Verweise auf den AMBIX-Datenbestand zu erzeugen, da jeder andere LDAP-Client außer dem vom Projekt eingesetzten TWEB keine personenbezogenen Daten geliefert bekommt. Bevor der DFN also mit seinen sehr gut gepflegten White-Pages-Daten am Index-System teilnehmen kann, muss die in 2.5 beschriebene noch ausstehende Klärung der datenschutzrechtlichen Fragen erfolgen.

5 Forschung und Entwicklung

5.1 Einbeziehung neuer Betriebssysteme und Plattformen

Nach der Übernahme des Betriebs und der Betreuung der deutschen Directoryinfrastruktur (vgl. Abs. 3.1) wurde auch SunOS 5.6 (Solaris 2.6) als weiteres Betriebssystem vom Projekt eingesetzt. Diese Plattform wird von MessagingDirect nach wie vor als Referenzsystem für Ihre Software-Produkte angegeben.

Alle verwendeten Software-Produkte, die MessagingDirect IC-Releases, das LDAP-Paket der University of Michigan und TWEB ließen sich auf dieser Plattform mit dem GNU-C-Compiler *gcc* (Version 2.8.0 bzw 2.8.1) problemlos übersetzen und zeigen im täglichen Betrieb keine Stabilitätsprobleme.

Mit der Untersuchung von *Active Directory* (AD), das als zentrales Paket in Microsoft Windows 2000 enthalten ist, sollte erstmals ein Directory-Produkt für ein anderes, Nicht-UNIX-System untersucht werden. Mit AD will Microsoft die gesamte Ressourcen- und Nutzerverwaltung bei Windows 2000 bewerkstelligen sowie über eine LDAP-Schnittstelle die Anbindung an andere Directory-Dienste ermöglichen. Auf dem 5. Workshop „Sicherheit in vernetzten Systemen“ am 4. und 5. März 1998 in Hamburg wurde von Dr. Ralf Schneider ein Vortrag über die Sicherheitsaspekte von AD gehalten⁶. Basis für diesen Vortrag war das Studium verschiedener White-Papers von Microsoft.

Die entgeltige Freigabe von Windows 2000 wurde immer weiter verschoben und fand erst Anfang des Jahres 2000 statt. Da eine Untersuchung der vorhandenen Beta-Releases nicht sinnvoll erschien, konnten nach der Veröffentlichung nur noch erste Versuche mit AD durchgeführt werden. Hauptergebnis dieser Versuche war, dass die LDAP-Schnittstelle standardkonform implementiert wurde, die Integration von Windows 2000 Rechnern in die bisherige Infrastruktur also möglich ist.

5.2 Aufbau einer PKI auf Basis von LDAP/X.500

Das Projekt hat sich auf dem Gebiet Public Key Infrastructure (PKI) vor allem mit einer Directory-gestützten PKI für die PGP-Verschlüsselungstechnologie beschäftigt. Andere Technologien (wie S/MIME und SSL) wurden zwar ebenfalls untersucht, jedoch ohne entsprechende Implementierungsarbeiten. Für PGP wurde einerseits ein Datenmodell definiert und in einem LDAP-Server implementiert, andererseits eine vorläufige Policy für einen Keyserver aufgestellt, sowie Verfahrensweisen für Datenlieferungen an diesen Keyserver definiert, die eine reibungs-

⁶ erschienen im DFN-Bericht Nr. 85, DFN-CERT & PCA (Hrsg.), März 1998

lose Kommunikation mit datenliefernden Zertifizierungsstellen (CAs) ermöglicht. Hierzu wurde ein ASCII-Datenlieferungsformat definiert, entsprechende Software implementiert, sowie eine Anleitung für CAs erstellt. Somit wurde alle Voraussetzungen für den Betrieb eines LDAP-basierten Keyservers geschaffen.

6 Support der DFN-Mitglieder

6.1 X.500 und LDAP

Seitens des Projekts wurde Unterstützung sowohl beim Aufbau als auch dem Betrieb eigener X.500/LDAP-Verzeichnisdienste in den DFN-Institutionen angeboten und geleistet. Sehr oft wurde von den DFN-Organisationen Hilfe bei der Entscheidung für den Einsatz eines LDAP-Servers oder eines DSAs gesucht.

Insbesondere bei der Umstellung der in den Organisationen eingesetzten X.500(88)-DSAs wurde umfangreicher Support und individuelle Hilfestellung geleistet. Alle für die Migration notwendigen Schritte wurden in Form des bereits erwähnten Kochbuchs zusammengefaßt und allen interessierten DSA-Administratoren zur Verfügung gestellt.

6.2 MessagingDirect/ISODE-Software

Das Projekt diente als zentraler Ansprechpartner bei allen Fragen über Installation und Betrieb der vom Projekt den DFN-Mitgliedern zur Verfügung gestellten ISODE/MessagingDirect-Software. Konnten Fragen nicht vom Projekt selbst beantwortet werden, wurde Kontakt zum Support Team von MessagingDirect aufgenommen und der entsprechende Support vermittelt.

7 Betriebliche Aspekte

7.1 Rechnerinfrastruktur

Zum Betrieb des AMBIX-Verzeichnisses, der WWW, FTP und DNS-Dienste, des Deutschland- und der anderen DSAs stehen dem Projekt insgesamt sechs Maschinen zur Verfügung. Tab. 6 beschreibt die einzelnen Rechner und ihre derzeitigen Funktionen. Zur Verkürzung der Schreibweise wurde bei den Rechnernamen die Domain `directory.dfn.de` nicht angegeben.

Aufgrund von Umstellungen im Zuge der Maßnahmen gegen das Jahr-2000-Problem und des hohen Betriebsalters, insbesondere der HP-Workstations und der von der TU Chemnitz übernommenen `sun01`, wurden einige Dienste im Laufe der Zeit auf andere Maschinen umgesiedelt. Viele der älteren Maschinen zeigen zum Teil erhebliche Verschleißerscheinungen, so dass zur Aufrechterhaltung der Dienste eine baldige Erneuerung des Rechnerbestandes angeraten erscheint. Insbesondere die `sun01` ist aufgrund schwerwiegender Festplattenprobleme momentan weder zum Betrieb noch zur Entwicklung einsetzbar. Dem Projekt steht

somit für die wichtige Plattform Solaris bereits seit längerer Zeit nur eine Maschine zur Verfügung. Die `hp01`, auf welcher bis zum Umstieg auf X.500(93) die DSAs des AMBIX-Verzeichnisses betrieben wurden, wird derzeit nicht für Dienste eingesetzt. Installation und Betrieb der aktuellen X.500 Implementationen von MessagingDirect ist auf der Plattform HP-UX 10.20 leider nicht mehr möglich.

| Name | Typ/OS/Anschaffung | Funktion | Bemerkung |
|-------|--|---|--------------------------------------|
| sun01 | Sun Ultra-1 / Solaris 2.6 / 1996 | | alter Puma-Host, Festplattenprobleme |
| sun02 | Sun Ultra-60/ Solaris 2.6 / 1998 | Host für Puma und AMBIX-DSAs, Entwicklung, X.500(93)-Test | Referenzplattform |
| as | PC PentiumII 400MHz / Linux (Kernel 2.0.36) / 1998 | Server für AMBIX-Daten und Indizes, X.500-PGP-Keyserver | |
| is | PC PentiumII 400MHz / Linux (Kernel 2.0.36) / 1998 | FTP-, WWW-, Mail-Server, DNS | |
| dns | HP WS9000 712/60 / HP-UX 10.20 / 1995 | Logging-Server | Festplattenprobleme |
| hp01 | HP WS9000 715/80 / HP-UX 10.20 / 1994 | interne AMBIX DV | |
| hp02 | HP WS9000 712/80 / HP-UX 10.20 / 1995 | zusätzlicher Server für AMBIX-Daten | |

Tabelle 6: Überblick über die Rechnerinfrastruktur

7.2 Maßnahmen gegen das Jahr-2000-Problem

Im Zuge der durch das Jahr-2000-Problem notwendig gewordenen Arbeiten wurden auf allen vom Projekt eingesetzten Rechnern Jahr-2000-feste Versionen der jeweiligen Betriebssysteme installiert. Neben der Umstellung aller X.500-Server auf die aktuelle MessagingDirect Implementation des X.500(93)-Standard, wurde auch die gesamte Software der AMBIX-Datenverarbeitung sowie die interne AMBIX-Datenbank auf ihre Jahr-2000-Festigkeit hin überprüft. Weiterhin wurden durch die Umstellung auf 93er DSAs notwendig gewordene Anpassungen der AMBIX-Software durchgeführt.

7.3 DFN Directory CA

Zur Verschlüsselung von Daten sowie der Signatur von Nachrichten wird vom Projekt und den Mitarbeitern PGP eingesetzt. Anfang 1999 wurde die DFN-DIRECTORY CA für PGP-Schlüssel aufgebaut. Diese CA folgt den Richtlinien der DFN-PCA und ist von der DFN-PCA zertifiziert. Sie ist ausschließlich für die Mitarbeiter des Directory Kompetenzzentrums zuständig, und zertifiziert nur deren Schlüssel.

8 Vorbereitungen zur Gründung einer GmbH

Es haben während des Projektzeitraums eine ganze Reihe von Gesprächen zwischen Vertretern des Projekts, des DFN-Vereins und der Universität Tübingen gegeben, in denen verschiedene in Dokumenten beschriebene Modelle diskutiert wurden: Die erste in Betracht gezogene Möglichkeit war ein der Universität angegliedertes Institut. Dies wurde wegen zu langer Realisierungszeit verworfen. Das zweite Modell sah eine GmbH vor, mit der Universität und dem DFN-Verein als Gesellschafter. Aus diesem Modell verabschiedete sich die Universität. Schliesslich scheiterte auch der Versuch eine GmbH mit dem DFN als Hauptgesellschafter zu gründen. Obwohl, wie eingangs erwähnt die Marktlage für eine auf Directories spezialisierte Firma sehr gut ist, konnte das Projektziel der Gründungsvorbereitung nicht erreicht werden.

9 Öffentlichkeitsarbeit

Neben der Tagung *Zukunft von Directory in Deutschland*, welche vom Projekt in Tübingen veranstaltet wurde, nahmen Mitarbeiter an Veranstaltungen der Firmen Telemation und Siemens teil. Weiter wurden von Mitarbeitern Vorträge bei

Sitzungen der IETF, der Teletrust AG 7 und der BelWü Netzdienste AG gehalten. Im Rahmen von NameFLOW/Paradise wurden die deutschen Directorybelange vom Projekt bei mehreren Meetings vertreten.

Der gestiegene Bekanntheitsgrad des Projekts wird durch einen Online-Artikel⁷ des Magazins FOCUS zum Thema Suche nach Email-Adressen belegt, in dem das AMBIX-Verzeichnis als *die* Suchmaschine für Adressen im akademischen Bereich bezeichnet wird.

9.1 Publikationen

Zur Publikation der vom Projekt verfaßten Texte wurden die Reihen *DS-Info* und *DS-Info Technical Paper* geschaffen. Beide Reihen sind als Forum für speziell den deutschen Teilbaum des Directory betreffende Fragen gedacht und stehen für die Veröffentlichung von Beiträgen projektfremder Autoren offen. Alle Papiere sind frei über den vom Projekt betriebenen WWW-Server zu beziehen⁸. Die Reihe *DS-Info* dient dazu, Dokumente zu allgemeinen directoryspezifischen Themen zu veröffentlichen, während in der Reihe *DS-Info Technical Paper* auch Probleme rein technischer Art behandelt und Musterlösungen diskutiert werden. Die Technical Paper werden in Form von Drafts mit Versionsnummern versehen, so dass sie bereits im Stadium des Entstehens zur Verfügung gestellt und weiterentwickelt werden können.

9.2 Vorbereitungen zur Gründung eines Deutschen Directory Forums

Im Rahmen der Vorbereitungen zur Konstituierung eines Deutschen Directory Forums wurde durch das Projekt vom 1.-2. September 1999 in Tübingen eine Konferenz zum Thema *Zukunft von Directory in Deutschland*⁹ veranstaltet. Eingeladen waren neben den DFN-Mitgliedern, auch Hersteller von Directory Software und alle interessierten Personen aus Forschung, Wirtschaft und Industrie. Neben der notwendigen Umstellung auf den X.500(93)-Standard war die schon seit längerem geforderte Neustrukturierung des Teilbaums c=DE [5] (Anhang C), die Richtlinien für die Namensgebung [6] und die Einführung von allgemeinen Qualitätsrichtlinien für Verzeichniseinträge [7] Gegenstand der zum Teil sehr lebhaften Diskussionen. Das Protokoll der Tagung ist als Anlage D beigefügt. Die

⁷<http://focus.de/D/DD/DD157/dd157.htm>

⁸<http://www.directory.dfn.de/ds-info>

⁹<http://www.directory.dfn.de/dirco/betreibertreffen>

Veranstaltung wurde von allen Teilnehmern als erfolgreich bezeichnet und allgemein wurde der Wunsch nach weiteren Treffen geäußert.

9.3 Internet-Präsenz des Directory Kompetenzzentrums

In Hinblick auf das zukünftige Directory-Kompetenzzentrum wurde vom Projekt eine eigene Infrastruktur aufgebaut. Beim DFN-Verein wurde die Zuweisung einer aussagekräftigen Sub-Domain `directory` unterhalb von `dfn.de` beantragt und realisiert. Von der Universität Tübingen wurde ein separater IP-Adressbereich (`134.2.217.x`) bereitgestellt, so daß nun alle Rechner des Projekts bzw. des Directory Kompetenzzentrums unterhalb der Domain `directory.dfn.de` mit einer IP-Adresse `134.2.217.x` angesprochen werden können. Zur Vereinfachung der Administration der Sub-Domain wird vom Projekt ein eigener DNS-Server (`dns.directory.dfn.de`) betrieben.

Für das Directory Kompetenzzentrum wurde ein WWW-Server unter der Adresse

`http://www.directory.dfn.de`

aufgebaut. Das Angebot auf diesem WWW-Server wird ständig erweitert und aktualisiert und umfaßt alle vom Projekt bearbeiteten Teilgebiete. Weiter unterhält das Projekt einen FTP-Server mit Zugängen unter:

`ftp-ambix.directory.dfn.de`

`ftp-dirco.directory.dfn.de`

`ftp-isode.directory.dfn.de`

`ftp-puma.directory.dfn.de`

Hier werden den Benutzern Dokumente, Tools und nicht zuletzt die MessagingDirect-Software zur Verfügung gestellt.

Literatur

- [1] Projekt AMBIX-D,
"Abschlußbericht",
Tübingen, Nov. 1995
- [2] Projekt AMBIX-II,
"Abschlußbericht",
Tübingen, April 1996
- [3] Projekt Ausbau und Nutzung des
DFN-E-Mail-Verzeichnisses,
"Abschlußbericht",
Tübingen, Aug. 1998
- [4] Sauer, M.,
"Das 88-2-93 Kochbuch",
DS-Info Technical Paper 2.3,
Tübingen, Okt. 1999
- [5] Gietz, P.,
"Zur Neustrukturierung des Deut-
schen Teilbaums im X.500/LDAP
Directory",
DS-Info 2,
Tübingen, Okt. 1999
- [6] Gietz, P.,
"Richtlinien für die Namensgebung
von Organisationen im deutschen
Teilbaum des Directory",
DS-Info 4,
in Vorbereitung
- [7] Sauer, M.,
"Richtlinien für die Qualität von
Einträgen im Teilbaum c=DE",
DS-Info 3,
Tübingen, Okt. 1999

Die Reihen DDS-Info und DDS-Info Technical Paper können über <http://www.directory.dfn.de/ds-info> bezogen werden.