DS-Info 2

Zur Neustrukturierung des deutschen Teilbaums im X.500/LDAP Directory

Peter Gietz

DS-Info 2
29. Oktober 1999

DS-Info ist eine Schriftenreihe, die von DFN Directory Services zu directoryrelevanten Themen herausgegeben wird. PDF–, Postscript– und HTML–Versionen sind zu beziehen unter: `http://www.directory.dfn.de/ds-info`

DFN Directory Services
Zentrum für Datenverarbeitung der Universität Tübingen
Wächterstraße 76, D-72074 Tübingen

Tel: +49 7071 29 –70334, –70335, –70336
Fax: +49 7071 29 5912
E-mail: `ds-info@directory.dfn.de`

Homepage: `www.directory.dfn.de`
DN: `o=DFN Directory Services, c=DE`

Abstract

Aufgrund der kontinuierlichen Zunahme von Organisationseinträgen im deutschen Teilbaum des X.500 wird dessen Neustrukturierung zwingend notwendig. In diesem Text wird angestrebt, durch Einführung von zusätzlichen Gliederungsebenen eine neue Struktur zu definieren, die den antizipierten Bedürfnissen der Zukunft gerecht werden kann. Nach einer Beschreibung des Ist-Zustands und seiner Probleme und nach Referierung einiger bisheriger Arbeiten zum Thema wird eine Strukturierung nach geografischen Gesichtspunkten definiert. Schließlich wird das Konzept der „Sichtweisen", also Aliase, die gleichartige Organisationseinträge gruppieren, beschrieben und ihre Anwendung im deutschen Teilbaum definiert.

Status des Dokumentes

Die erste Version dieses Dokuments (Draft v1) war Diskussionsvorlage für das von DFN Directory Services ausgerichtete Betreibertreffen „Zukunft von Directories in Deutschland", das am 1. und 2. September 1999 in Tübingen stattfand. In der folgenden Version (Draft v2) wurden die dort gefaßten Beschlüsse sowie weitere Anregungen eingearbeitet. Diese Version wurde beim X.500-AK der 31. DFN-Betriebstagung vorgestellt. Da sich dort keine Mehrheit für einen Gegenvorschlag ergeben hat, soll die hier vorliegende, überarbeitete Version als verbindliche Vorgabe für die Neustrukturierung der Hierarchie-Ebene `c=DE` dienen.

Inhaltsverzeichnis

1 Die Problemstellung

Die Anzahl der Organisationen, welche Daten im deutschen Teilbaum des X.500 ablegen wollen, steigt stetig. Mittlerweile gibt es zusätzlich zu den 122 im Projekt AMBIX[1] [1] verwalteten Organisationen, die wegen besonderer datenschutzrechtlicher Grundlage bisher in einem eigenen Teilbaum unter `l=DFN` gesammelt werden, weitere 138 Organisationen unter `c=DE`. In naher Zukunft werden knapp 100 kleine und mittlere Unternehmen neu hinzukommen. Die stetige Zunahme von Organisationseinträgen wird zukünftig sinnvolles Browsen unter `c=DE` unmöglich machen. Das vorliegende Dokument soll dieses Problem lösen, indem es eine Untergliederung der Ebene `c=DE` des *Directory Information Trees* (DIT) vorschlägt. Diese neue Struktur hat naturgemäß Auswirkungen auf den *Distinguished Name* (DN) der einzelnen Einträge, da dieser aus den jeweiligen *Relative Distinguished Names* (RDN) der Einträge innerhalb der hierarchischen Baumstruktur besteht. Der DN bildet sozusagen den Pfad eines Eintrags entlang der Directory-Struktur.

Für eine bessere Benutzbarkeit sollen zusätzlich zu der Neustruktur sogenannte „Sichtweisen“ eingeführt werden, die verwandte Einträge in Form von Aliasverweisen zusammenfassen.

Wie die sehr heftig geführte Diskussion über die Neustrukturierung zeigt, hat jedes Lösungsmodell seine Vor- und Nachteile und keine Lösung wird alle Interessen berücksichtigen können. Je mehr Strukturelemente eingeführt werden, um so kürzer werden die Listen unterhalb eines Eintrags aber um so länger werden auch die DNs der Einträge. Der hier erarbeitete Vorschlag geht davon aus, daß der DN nur selten per Hand geschrieben werden muß und die Länge des DNs deshalb weniger ausschlaggebend ist.

Ein weiteres Problem im deutschen Teilbaum des Directory ist, daß der Datenbestand sehr heterogen ist und nur ein Teil gepflegt wird; der andere Teil besteht aus veralteten Informationen. Außerdem sind manche Einträge nur Testeinträge oder Einträge von Organisationen mit keiner oder fast keiner zusätzlichen Information. Um dieses Problem anzugehen, wurde ein separates Dokument erstellt [2], in dem Richtlinien für Minimalanforderungen an Einträge (Minimaldatensätze, obligatorische Einträge) und an DSAs formuliert werden.

2 Voraussetzungen und Vorarbeiten

2.1 Der X.500(93) Standard

Im X.500(93) - in unserem Zusammenhang sind von Bedeutung: [3, 4, 5, 6] - werden keine eindeutigen Regeln für die Struktur des *Directory Information Tree* (DIT) gegeben sondern lediglich Definitionsmechanismen hierfür. Zunächst werden bestimmte Objektklassen als *Structural Object Class* (SOC), also Strukturelemente ausgewiesen[2]. Eine SOC spezifiziert das Objekt in der *„real world“*, welches im Directory abgebildet werden soll, also z.B. eine Organisation, eine Person, etc. Jeder Eintrag muß mindestens eine SOC enthalten, es können auch mehrere SOCs in einem Eintrag vorkommen (z.B.: *person* und *organizationalPerson*). Alle in X.521 definierten Objektklassen sind SOCs.

Durch eine SOC werden zwei weitere strukturrelevante Dinge definiert:

- Eine *DIT Content Rule*[3] (DCR),

[1] Siehe www.directory.dfn.de/ambix. AMBIX ist das Vorgängerprojekt von DFN Directory Services (DDS)
[2] X.501 12.1, 14.7.8.
[3] X.501 12.7.2, 14.7.2.

durch die definiert wird, welche Attribute in einem Eintrag vorhanden sein müssen, welche vorhanden sein dürfen, sowie welche zusätzlichen Objektklassen (*Auxiliary Object Class*[4]) vorhanden sein dürfen.

- Eine oder mehrere *Name Forms*[5] (NF), durch welche die Konstruktion des RDN bestimmt wird. Die für einen Eintrag ausgewählte NF wiederum definiert eine oder mehrere *DIT Structure Rules*[6] (DSR). Die für einen Eintrag ausgewählte DSR - *Governing DIT Structure Rule* genannt - bestimmt, wo im DIT der Eintrag plaziert werden darf, indem in ihr Regeln für mögliche übergeordnete Einträge definiert sind.

Neben diesen Definitionsmechanismen gibt der Standard zusätzlich einen Vorschlag für „*nameforms and DIT structures*“, ergänzt durch ein sehr anschauliches Diagramm[7]. Dieser Vorschlag ist allerdings nicht integraler Bestandteil des Standards, sollte aber trotzdem, da er bereits angewandt und in bestehende Software integriert wurde, befolgt werden, wenn nicht sehr gute Gründe dagegen sprechen. Es werden dort auch Structure Rules zur Objektklasse *locality* beschrieben, wonach eine *locality* unterhalb von country, einer weiteren *locality*, einer *organization* oder einer *organizationalUnit* stehen darf. Der DN eines Eintrags mit der Objektklasse *locality* kann entweder mit den Attributen *localityName* oder *stateOrProvinceName* gebildet werden. Im letzteren Fall darf ein solcher Eintrag aber nur direkt unter *country* stehen[8].

2.2 Arbeiten der IETF zum Thema

Neben einer Reihe von RFCs, die generell in das Problem eines Internet Directory auf X.500-Basis einführen und entsprechende allgemeine Strategien hierfür anbieten (siehe z.B.: [7, 8, 9, 10]), wurden in der IETF auch Dokumente veröffentlicht, die direkt DIT-Strukturierung thematisieren.

2.2.1 RFC 1255

Das erste dieser Dokumente, RFC 1255 [11], ist ursprünglich außerhalb der IETF entstanden, nämlich als Dokument des North American Directory Forum, und erst später in seiner letzten Version zu einem RFC gemacht worden. Es hat die Strukturierung und die Namensregeln für den Teilbaum `c=US` zum Thema und definiert u.a. die verschiedenen Strukturebenen unterhalb `c=US`, wobei zwischen einem *national level* (die USA), einem *regional level* (die Bundesstaaten) und einem *local level* (die *counties*, also Verwaltungsbezirke) unterschieden wird. Die Namen und Anzahl der Einträge dieser Strukturierungshierarchien konnten Veröffentlichungen des US Department of Commerce entnommen werden.

2.2.2 RFC 1617

RFC 1617 [12] definiert eine Reihe von Richtlinien zur Directory-Namensgebung und -Strukturierung, wobei der Fokus wie üblich auf einen White-Pages-Dienst gerichtet ist. Es werden genaue Anweisungen für den *toplevel*, die *country*- und *organization*-Ebene gegeben, und u.a. die Frage der Einordnung internationaler und multinationaler Organisationen behandelt.

[4] X.501 8.3.3.
[5] X.501 12.6.2, 14.7.6
[6] X.501 12.6.5-6, 14.7.1
[7] X.521 Annex B
[8] X.501 Annex B.12 „*Alternate Structure Rule for Locality*“.

Bezüglich der Country-Ebene wird ausgesagt, daß deren Strukturierung Aufgabe der einzelnen nationalen Standardisierungsgremien sei. Dennoch wird, sozusagen als Übergangslösung bis zum entsprechenden Handeln dieser Gremien, folgende Struktur vorgeschlagen: Direkt unterhalb der *country*-Ebene sollten nur *localities*, die Bundesstaaten oder vergleichbare geografische Einteilungen repräsentieren, stehen, sowie Organisationen, die eine „nationale Signifikanz“ besitzen. Kleinere Organisationen sollen in die Locality-Struktur eingegliedert werden. Als Beispiel wird neben dem bereits erwähnten RFC 1255 noch das australische Pendant, RFC 1562 [13], angegeben.

Bezüglich der Namensgebung wird eindeutig der volle ausgeschriebene Name einer Organisation als RDN-bildender Attributwert vorgeschrieben.

2.2.3 LDAP

Der IETF-Standard LDAP hat nicht nur das X.500 Datenmodell übernommen, sondern auch die meisten SOCs, wie sie in X.501, Annex A aufgeführt sind. In der neuesten Version LDAPv3[14], werden in einem eigenen Dokument [15] die entsprechenden Definitionen (als „SHOULDs“) wiedergegeben, wobei die Objektklasse *locality* auch das alternative Namensattribut `st` (*stateOrProvinceName*) enthält. Dieses Namensattribut enthält als Wert „den *vollen* Namen eines Staates oder einer Provinz“[9]. Das Namensattribut *locality* enthält demgegenüber, genereller, den „Namen einer Lokalität wie z.B. eine Stadt, ein Bezirk oder eine sonstige geografische Region“[10].

2.2.4 Domain Components

Schließlich wurde in der IETF ein ganz neuer Strukturierungsplan vorgestellt und als *informational* RFC 2377 [16] veröffentlicht. Hier wird das oben beschriebene X.500 Namensschema als Hindernis für die weitere Verbreitung directory-fähiger Anwendungen gebranntmarkt. Dies ist sicherlich auf die Schwierigkeiten v.a. in den Vereinigten Staaten zurückzuführen, Firmennamen rechtlich eindeutig zu registrieren. Desweiteren wird kritisiert, daß die verwendeten Attribute verwirrend und unflexibel seien.

Als Alternative zum alten X.500 Schema, oder auch nur als dessen Erweiterung, wird ein ganz neuer Weg beschritten. Die oberen Ebenen der Struktur sollen nicht mehr nach den Namensattributen *countryName*, *localityName*, oder *organizationName* benannt werden. An deren Stelle soll das schon in RFC 1279 [17] definierte und in RFC 1274 [18] in die Gruppe der im internationalen Pilotbetrieb zu verwendeten Attribute aufgenommene Attribut *domainComponent* (DC) treten, welches das DNS-System abbildet. In diesen beiden alten RFCs wurde DC der Objektklasse *domain* zugeordnet und war nicht für die Bildung der DIT-Struktur gedacht, sondern nur für die Aufnahme von DNS-Information. Dasselbe Attribut DC taucht wieder in RFC 2247 [19] auf, wo es zusätzlich zur *Structural Object Class domain* der *Auxiliary Object Class dcObject* zugeordnet wird. Letztere kann zu jedem Eintrag hinzugefügt werden. in RFC 2247 erfährt die Objektklasse *domain* wesentliche Erweiterungen; sie soll verwendet werden, wenn der Eintrag keiner SOC zuzuordnen ist, ansonsten soll *dcObject* der SOC hinzugefügt werden.

Der Vorteil dieses Namensschema ist, daß es keinerlei Registrierungsprobleme gibt, da die Registrierung der DCs bereits bei der DNS Domain-Vergabe passiert ist. Der Nachteil ist, daß die Namen nicht mehr aussagekräftig sind. Sicherlich

[9] Par. 5.9. Hervorhebung durch PG
[10] Par. 5.8.

wird dieses Namensschema in Zukunft eine größere Rolle spielen, nicht zuletzt weil es von Micro$oft unterstützt wird. Ob es das alte und wenigstens in der alten Welt bewährte X.500 Namensschema ersetzen wird, kann bezweifelt werden. Anzustreben ist eine Koexistenz beider Schemata, mit gegenseitiger Verweisung. Dies ist jedoch nicht Gegenstand dieses Dokuments, in dem erst einmal das X.500 Namensschema zur Grundlage genommen wird.

2.3 Namensrichtlinien

Die Namensgebung für die oberste Hierarchieebene unterhalb der Wurzel, also der *country*-Ebene ist im Standard[11] festgelegt, wonach als Attributwert ein Landeskürzel nach ISO 3166 [20] vorgeschrieben ist (`c=DE`).

Die augenblickliche Namensgebung der RDNs von Organisationseinträgen unter `c=DE`, entspricht den bereits 1992 aufgestellten Richtlinien [21], die nun in einer aktualisierten Version vorliegen [22]. Die wichtigste dieser Regeln, die sich mit den internationalen Vorgaben in RFC 1617 [12] und RFC 2256 [15] deckt, ist, daß der Name aus der gebräuchlichen ausgeschriebenen Namensform bestehen soll, und daß Abkürzungen möglichst zu vermeiden sind.

2.4 Der Ist-Zustand

Augenblicklich gibt es im deutschen Teilbaum des DIT neben den Organisationseinträgen schon eine gewisse Unterstrukturierung, die auf die Arbeit des bereits erwähnten AMBIX-Projekts zurückzuführen ist. Es wurden drei inhaltliche, nicht geografisch definierte *localities* eingeführt:

2.4.1 l=DFN

Wegen der Anwendung eines Widerspruchverfahrens und den daraus folgenden besonderen datenschutzrechtlichen Voraussetzungen, mußten die von AMBIX verwalteten Personendaten aus DFN-Mitglieds-Organisationen besonders geschützt werden. Vor allem mußte verhindert werden, daß die Daten aus Ländern ohne adäquate Datenschutzgesetzgebung abgerufen werden können. Aus diesem Grund wurden alle Daten in einem eigenen, mit besonderen Zugriffskontrollen versehehen Teilbaum gesammelt. Der Natur des Email-Verzeichnisses für DFN-Mitgliedsorganisationen entsprechend, wurde dieser Teilbaum unter dem Eintrag `l=DFN` angelegt.

2.4.2 l=Einzelpersonen

Das Projekt AMBIX veröffentlicht auch Daten von Benutzern des DFN Internetproviderdienstes WinShuttle[12], die der Aufnahme ins X.500 explizit zugestimmt haben. Hierfür wurde eine weitere *locality* eingeführt: `l=Einzelpersonen`. Bei einer nicht vorhandenen geografischen Unterstrukturierung war das die naheliegenste Wahl. Mittlerweile werden unter `l=Einzelpersonen` alle Personen, also auch Kunden von anderen Internetprovidern eingetragen, die keiner im X.500 eingetragenen Organisation angehören bzw. die zusätzlich zu ihrem „dienstlichen“ Eintrag einen „privaten“ Eintrag haben möchten. Diese *locality* ist weiter in Bundesländer und KFZ-Gebiete unterstrukturiert. Erst unterhalb der KFZ-Gebiete werden die Personeneinträge gesammelt.

[11] X.520 5.3.1.

[12] Siehe http://www.shuttle.de/

2.4.3 l=Schulen

Für die Aufnahme von Einträgen für Schulen, die dem Offenen Deutschen Schulnetz (ODS)[13] bzw. WinShuttle angeschlossen sind, wurde eine weitere *locality* (`l=Schulen`) eingeführt. Diese *locality* ist ebenfalls weiter in Bundesländer und KFZ-Gebiete unterstrukturiert, bevor die Organisationseinträge der einzelnen Schulen gesammelt werden. Unterhalb dieser Organisationseinträge sind sowohl Unterorganisationseinträge als auch Personeneinträge für Lehrer und Schüler möglich. Dieser Teilbaum des Verzeichnisses befindet sich erst in einem frühen Aufbaustadium und ist noch nicht öffentlich sichtbar.

2.5 Diskussionsstand

Schon 1994 auf der DSA-Betreiber-Tagung in Köln wurde über eine Neustrukturierung diskutiert, wobei sich zwei Lager bildeten. Die einen wollten dem X.500-Standard gemäß nur geografische Untergliederungen zulassen, also eine Aufteilung in Bundesländer und als zweite Hierarchieebene Städte. Die anderen meinten, den im X.500 (als Objektklasse) definierten Begriff *locality* auch in einem übertragenen Sinn auffassen zu dürfen und darunter auch inhaltliche Unterteilungskriterien, wie „Bildungseinrichtungen“ etc. verstehen zu können. Der „Sündenfall“ hat ja auch bereits stattgefunden durch die Einführung der *localities* `l=DFN`, `l=Einzelpersonen` und `l=Schulen` . Nach einer längeren Stagnation der Diskussion will nun dieses Dokument zu einer abschließenden Handlungsrichtlinie finden. Anfang September 1999 wurde beim DSA-Betreiber-Treffen in Tübingen[14] ein erster Strukturierungsvorschlag vorgetragen, bei dem die Unterstrukturierungen nach inhaltlichen Kriterien (z.B. l=Universitäten, l=Schulen, etc.) gemacht werden werden sollte. Die große Mehrzahl der Teilnehmer lehnte diesen Vorschlag jedoch ab, weil es sehr schwierig sei, für jede Organisation eine adäquate Kategorie zu finden, besonders in Hinblick auf rechtliche Eindeutigkeit und Unanfechtbarkeit. Sozusagen als zweiter Anlauf wird nun in diesem Dokument eine diesbezüglich eindeutigere geografische Lösung vorgestellt, die sich außerdem wesentlich näher an den X.500 Standard sowie an die meisten Vorschläge aus der IETF hält.

Es ist wichtig, daß die gefundene Lösung einen möglichst breiten Konsens findet. Auch in Bezug auf die Einführung von Public-Key-Infrastrukturen ist diese Frage von Relevanz, da auch dort DNs gebildet und zertifiziert werden. Es ist anzustreben, daß auch diese DNs nach den hier vorgegebenen Richtlinien gebildet werden.

3 Neustrukturierung der Einträge unter c=DE

Um eine Überflutung der `c=DE`-Ebene mit zu vielen Einträgen zu vermeiden, werden geografisch definierte *localities* im deutschen Teilbaum eingeführt[15]. Es wird eine zweigliedrige Unterstrukturierung definiert, die Bundesländer und Städte abbildet, so daß sich insgesamt 3 Ebenen ergeben, unter denen Organisationseinträge abgelegt werden können. Da eine im Standard vorgesehene Objektklasse zum Einsatz kommt, kann weiterhin jeder Client auf ein so strukturiertes Verzeichnis zugreifen.

3.1 Die Ebene direkt unter c=DE

Direkt unter `c=DE` sollen nur noch solche Organisationen eingetragen werden,

[13] Siehe http://ods.schule.de/

[14] Siehe das Protokoll unter http://www.directory.dfn/dirco/betreibertreffen/PG99-115.Sept99-prot.html.

[15] Die gesamte Neustruktur ist im Anhang A.1 grafisch dargestellt.

die eine nationale Relevanz haben, was durch Größe, Bekanntheitsgrad, oder internationale bzw. überregionale Präsenz definiert wird. Mitentscheidend für eine Eingliederung in die oberste Hierarchieebene ist nicht nur die Anzahl der Mitarbeiter, Studierenden, etc., sondern auch die Anzahl der gepflegten Personeneinträge[16]. Unter diese Kriterien fallen z.B. große Konzerne (z.B. IBM Deutschland), große Verbände und Vereine, die auf nationaler Ebene tätig sind (z.B. Deutsches Rote Kreuz), die großen[17] allgemeinen Hochschulen (z.B. Universität Heidelberg), einige große Fachhochschulen (z.B. FH Köln), sowie überregionale Forschungsanstalten (z.B. MPG, FhG) und Großforschungseinrichtungen (z.B. FZ Jülich). Außerdem wird eine Organisation `o=Bund` angelegt, unter dem Bundesministerien, Bundesämter und sonstige national tätigen Verwaltungsorgane eingeordnet werden.

Zusätzlich zu diesen Organisationseinträgen werden für jedes Bundesland, sowie für die unter 4 und 5 beschriebenen Anwendungen *localities* angelegt.

3.2 Die Ebene der Bundesländer

Direkt unter `c=DE` wird für jedes Bundesland eine *locality* mit dem namensgebenden Attribut *stateOrProvinceName* eingeführt. Unter diesen *localities* sollen Organisationen eingetragen werden, die eine bundeslandesweite Relevanz haben, wie z.B. Landesversicherungsanstalten und kleinere Hochschulen. Außerdem wird hier ein weiterer Eintrag eingerichtet (etwa o=Landesverwaltung), unter der Landesämter und -Behörden, sowie die Landesregierung eingetragen werden können.

Diese, die Bundesländer abbildenden *localities* sollen im DN-bildenden Namen die ausgeschriebene Namensform enthalten, also z.B. `st=Baden Wuerttemberg`. Als Alternativname wird die Namensabkürzung zwingend vorgeschrieben, z.B. `st=BW`. Weitere Attribute, können diesen *localities* hinzugefügt werden.

3.3 Die Ebene der Städte

Unter jedem der Einträge für die Bundesländer wird eine zweite Strukturierungsebene von *localities* mit dem namensgebenden Attribut *localityName* eingeführt, welche die Städte abbilden.

Unter diese *localities* werden alle übrigen Einträge eingegliedert, die nicht in die unter 3.1 und 3.2 beschriebenen oberen zwei Ebenen hineinpassen, also kleine und mittlere Betriebe, Schulen, Vereine und Privatpersonen. Für letztere Gruppe wird anstelle des Organisationseintrags eine *locality* `l=Privatpersonen` eingerichtet.

Es werden nur solche Städte in die Struktur aufgenommen, die ein Amtsgericht/Registergericht mit Handelsregister beheimaten. Jede Firma in Deutschland kann einer solchen Stadt zugeordnet werden. Allerdings sind die Firmennamen innerhalb eines Handelsregisters nicht zwingend eindeutig, sondern nur innerhalb des Firmensitzes. Deshalb muß der RDN-bildende Firmennamen den Firmensitz mitenthalten, wenn sich dieser vom Handelsregisterort unterscheidet. Z.B.:
Für Firma X aus Hirschau:

```
o="Firma X, Hirschau",
l=Tuebingen, l=Baden-Wuerttemberg,
c=DE
```

Für Firma Y aus Tübingen:

```
o=Firma Y, l=Tuebingen,
l=Baden-Wuerttemberg, c=DE
```

In Fällen, wo es eine offensichtliche Diskrepanz gibt zwischen Handelsregisterort und

[16] Zur Definition von „gepflegt“ vergleiche [2].

[17] Als „groß“ werden hier Hochschulen angesehen, die mehr als 5000 Studierende haben.

KFZ-Kennzeichen-Gebiet, können zusätzlich durch KFZ-Kennzeichen-Gebiet definierte Städte oder Kreise in die Struktur aufgenommen werden, um dort Schulen und Privatpersonen einzutragen. Firmen dürfen allerdings nicht unter solchen zusätzlichen Städte-Knoten eingetragen werden, sondern immer nur unter dem Handelsregisterort.

Die bereits vorhandenen *localities* `l=Einzelpersonen` und `l=Schulen` werden nach einer Übergangszeit aufgelöst, und die dort gesammelten Einträge unter die Städte eingeordnet.

Diese die Städte abbildenden *localities* sollen im RDN-bildenden Namen die ausgeschriebene Namensform enthalten, also z.B. `l=Tuebingen`. Die Namensergänzungen von Städten zur Unterscheidung von gleichnamigen Orten gehört zur ausgeschriebenen Namensform und muss dem RDN-bildenden Namen hinzugefügt werden, z.B. `l=Frankfurt/Main`. Als Alternativname sollten allgemein bekannte Namensabkürzung, vorzugsweise das KFZ-Kennzeichen aufgenommen werden, also z.B. `l=Tue` für Tübingen und `l=F`, sowie `l=Fft/M` für Frankfurt/Main . Weitere Attribute können diesen *localities* hinzugefügt werden.

3.4 Die Einordnung der AMBIX-Daten

Der Bereich unter `l=DFN` wird ebenfalls nach einer nochmaligen Klärung der datenschutzrechtlichen Frage aufgelöst und die Organisationen in die entsprechenden Stellen in der Neustruktur eingeordnet. Gegebenenfalls können AMBIX-Organisationen durch entsprechende *access control* auf Organisationseintragsebene weiterhin Zugriffsbeschränkungen unterliegen.

4 „Sichtweisen“, ein im DIT verankerter Index

Um die Einträge für die Benutzung noch besser zu erschließen, werden weitere, thematisch definierte *localities* als Sichtweisen direkt unter `c=DE` eingeführt. In diesen *localities* werden Kataloge von Alias-Einträgen verwaltet, die auf die eigentlichen Einträge zeigen. Diese *localities* haben also keinerlei Relevanz bei der Bildung von DNs. Um diese „Sichtweisen-Localities“ von den oben beschriebenen Bundesländer-Localities mit echten Daten zu trennen, wird ihr DN aus dem Namensattribut *localityName* (im Gegensatz zu *stateOrProvinceName* für die Bundesländer) gebildet.

4.1 Die Kategorien

Folgende Sichtweisen aif Organisationseinträgen sind zunächst einzurichten:

- `l= Universitaeten`
- `l= Fachhochschulen`
- `l= Forschungseinrichtungen`
- `l= Bibliotheken`
- `l= Schulen`
- `l= Volkshochschulen`
- `l= Wirtschaftunternehmen`
- `l= Verwaltung`
- `l= Verbaende und Vereine`
- `l= Medizinische Einrichtungen`

Diese Sichtweisen werden weder geografisch, noch inhaltlich weiter untergliedert. Zur Verhinderung von Namenskollisionen bei den Aliaseinträge werden nötigenfalls weitere Bestandteile des DNs in den RDN eingetragen, z.B.:

```
o="Landesdatenschutzbeauftragter,
Baden-Wuerttemberg", l=Verwaltung,
c=DE.
```

Die Aliase können sowohl auf Einträge unterhalb der geografischen *localities*, als auch auf Einträge direkt unterhalb von `c=DE` verweisen.

Zur Erleichterung für nicht deutsche Benutzer wird als Alternativnamen die englische Übersetzung der Kategorien eingetragen.

Zusätzlich zu den oben aufgelisteten inhaltlichen Kategorien, wird eine Sichtweise

- `l=Staedte`

eingerichtet, unter der alphabetisch alle in der Bundesländerstruktur eingetragene Städtenamen mit entsprechenden Verweis eingetragen werden. Dies ist gedacht für Benutzer, die eine gesuchte Stadt nicht einem Bundesland zuordnen können.

Auch weitere Sichtweisen sind denkbar, z.B. eine Sichtweise zur Gruppierung aller Organisationen mit einem gepflegten Personenverzeichnis. Die hier beschriebenen sowie alle in Zukunft neu von DDS eingeführten Sichtweisen werden in einem fortlaufend aktualisierten DS-Info Technical Paper [23] dokumentiert.

4.2 Technische Realisierung

Um einen automatischen Aufbau dieser Sichtweisen zu ermöglichen, muß jeder Organisationseintrag mit einer neu zu definierenden Objektklasse *aliasCategoryObject* versehen werden, die das *multi value* Attribut *aliasCategory* ermöglicht. Die dort als Attributwerte eingetragenen Kategorien verweisen indirekt auf die Stelle in der Sichtweisen-Hierarchie[18]. So muß z.B. der Eintrag für die Universität Tübingen folgendes Attribut enthalten:

```
aliasCategory= Universität
```

Auch Unterorganisationseinträge, die eine eigenständige Institution abbilden, wie zum Beispiel ein Klinikum unterhalb einer Universität, müssen solche Sichtweisen-Attribute enthalten. So muß z.B. der Eintrag `c=DE,o=Freie Universität Berlin, ou=FB Humanmedizin, ou=Augenklinik` folgendes Attribut enthalten:

```
aliasCategory= Medizinische
Einrichtung
```

Der Eintrag `c=DE, l=Baden-Wuerttemberg, l=Tuebingen` muß enthalten:

```
aliasCategory= Stadt
```

Es ist dann Aufgabe der entsprechenden Software, solche Kategorien mit den Sichtweisen zu mappen. Ein entsprechender Thessaurus für die Kategoriebezeichnungen, der Grundlage für die Mappingtabellen ist, wird vom DDS erstellt und in [23] veröffentlicht. Sichtweisen lassen sich hierdurch flexibel gestalten und bei einer Umstrukturierung der Sichtweisen muß nicht notgedrungen jeder Organisationseintrag geändert werden.

4.3 Sichtweisen und andere Indexmechanismen

Die „Sichtweisen-Localities“ erfüllen in gewisser Weise denselben Zweck wie Indices. Allerdings läßt das hier vorgeschlagene Modell darüber hinaus auch echte Indices zu. Es können weiterhin alle echten Einträge von Indexmaschinen indiziert werden. Dies ist jedoch nicht Gegenstand dieses Dokuments.

[18] Zur Definition von Attribut und Objektklasse siehe Anhang A.2.

5 Ein Teilbaum für applikationsrelevante Einträge

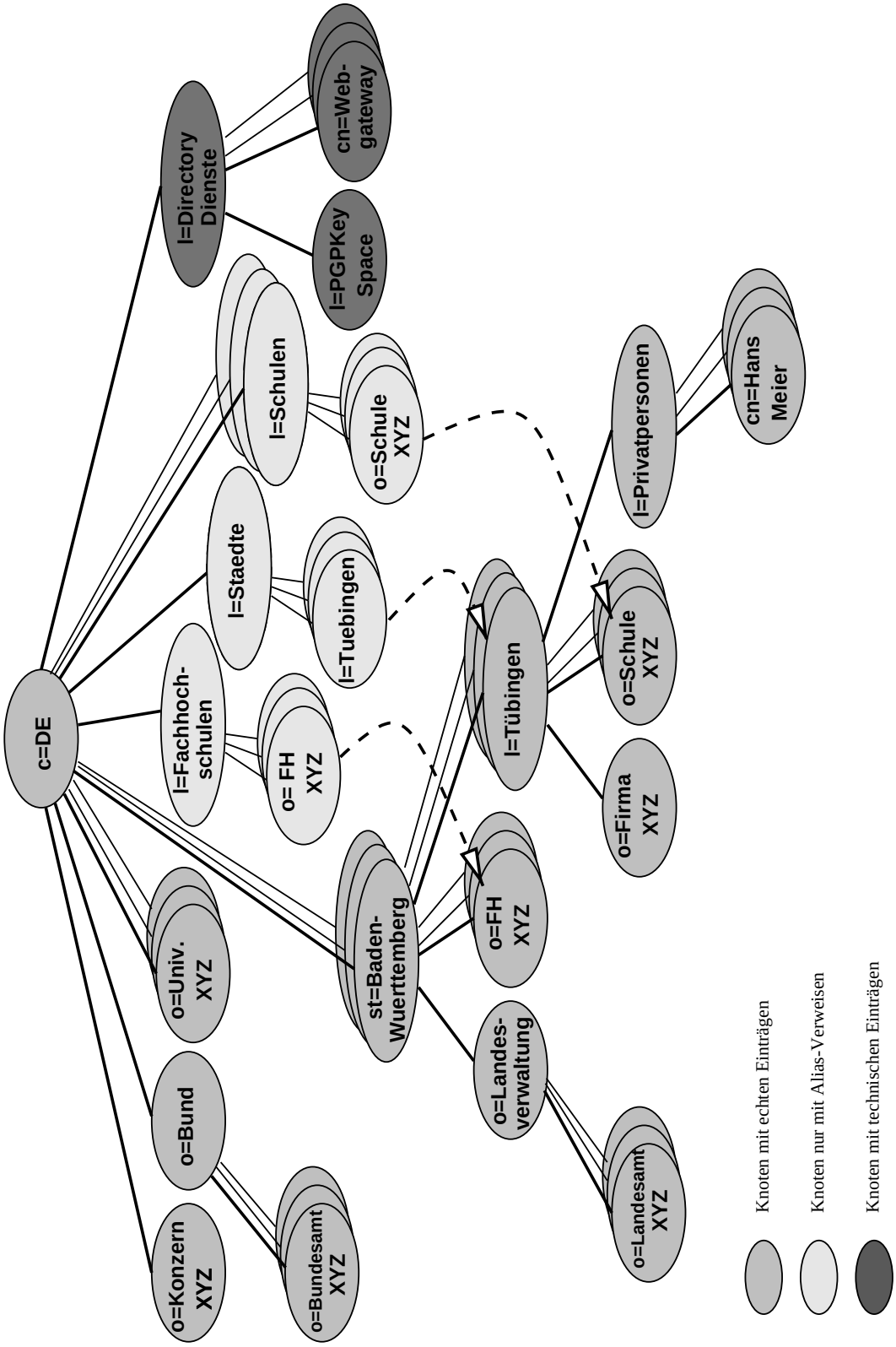
Für verschiedene Applikationen (Mailrouting, PGP-Key-Space, Webgateway, etc.) wurden direkt unter `c=DE` Spezialeinträge gemacht, in denen für diese Anwendungen Informationen abgelegt wurden. Damit solche Einträge nicht beim Browsen im DIT stören bzw. verwirren, sollen sie in einem eigenen Teilbaum gesammelt werden. Auch hierfür wird eine *locality* mit *localityName* als namensgebenden Attribut eingeführt:

- `l=Directory Dienste`.

Zur Erleichterung für nicht deutsche Benutzer wird als Alternativnamen `l=Directory Services` eingetragen.

A Anhänge

A.1 Grafische Darstellung der Neustruktur von c=DE



A.2 Definition der Objektklasse aliasCategoryObject

Für die Implementierung der Sichtweisen werden ein neues Attribut *aliasCategory* und eine dazugehörige *auxiliary* Objektklasse *aliasCategoryObject* eingeführt. Im Folgenden werden die in X.501 [4] definierten *attributeTypeDescription*[19] und *objectClassDescription*[20] für diese beiden Neudefinitionen gegeben. Einmal in der ASN.1-Form und einmal in der von der IETF WG Schema Registration (schema) vorgeschlagenen Form, die sich bei LDAP-RFCs durchgesetzt hat, obwohl das entsprechende Dokument [24] sich noch im Draft-Status befinded.

Die OIDs müssen nachgereicht werden, da DDS im Augenblick nur über einen sehr exotischen OID Baum[21] verfügt. DDS wird sich um einen eigenen OID Teilbaum bemühen, aus dem zukünftig alle directoryrelevanten OIDs für Deutschland geschöpft werden sollen. Alle vom DDS definierten OIDs werden in [25] veröffentlicht.

A.2.1 ASN.1 Definitionen

```
aliasCategory ATTRIBUTE           ::=  {
    WITH SYNTAX                        PrintableString{ub-business-category}
    EQUALITY MATCHING RULE             caseIgnoreMatch
    SUBSTRINGS MATCHING RULE           caseIgnoreSubstringMatch
    ID                                 <to be asigned> }


aliasCategoryObject OBJECT-CLASS  ::=  {
    SUBCLASS OF                        {top}
    KIND                               auxiliary
    MAY CONTAIN                        {aliasCategory}
    ID                                 <to be asigned> }
```

A.2.2 Definitionen nach dem Formatvorschlag der Schema Registration WG

```
( n.n.n.n NAME 'aliasCategory' EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.44{128} )

( n.n.n.n NAME 'aliasCategoryObject' SUP top AUXILIARY
    MAY ( aliasCategory ) )
```

[19] X.501 14.7.4; 12.4.6.
[20] X.501 14.7.5; 12.3.3.
[21] 0.9.2625.45050260321.1

A.3 Die Objektklasse locality

Objektklasse locality			
Subklasse von	*top*		
Attribut	**Inhalt**	*must*	*may*
description	Beschreibung		x
localityName	Name einer geografischen Lokalität		x
stateOrProvinceName	Name eines Bundeslandes, o.ä.		x
streetAddress	Straßenname und Hausnummer		x
seeAlso	Verweis auf anderen Eintrag		x
searchguide	Suchfilter-Informationen		x

Abkürzungsverzeichnis

AMBIX	Aufnahme von Mailbenutzern in das X.500 Directory
DCR	DIT Content Rule
DDS	DFN Directory Services
DIT	Directory Information Tree
DN	Distinguished Name
DNS	Domain Name System
DSA	Directory System Agent
DSR	DIT Structure Rule
FH	Fachhochschule
FhG	Fraunhofer Gesellschaft
FZ	Forschungszentrum
IETF	Internet Engineering Task Force
ISO	International Standards Organization
LDAP	Lightweight Directory Access Protocol
MPG	Max Planck Gesellschaft
NF	Name Form
ODS	Offenes Deutsches Schulnetz
RDN	Relative Distinguished Name
RFC	Request For Comments
SOC	Structural Object Class

Literatur

[1] Gietz, K.P., Schneider, R., Spanier, K., „X.500 für alle - Das DFN-Projekt AMBIX“, DFN Mitteilungen 24, November 1996

[2] Sauer, M., „Richtlinien für die Qualität von Einträgen im Teilbaum c=DE“, DS-Info 3, Tübingen Oktober 1999

[3] „The Directory: Overview of Concepts, Models, and Services“, ITU-T Recommendation X.500 — ISO/IEC 9594:1993-1

[4] „The Directory: Models“, ITU-T Recommendation X.501 — ISO/IEC 9594:1993-2

[5] „The Directory: Selected Attribute Types“, ITU-T Recommendation X.520 — ISO/IEC 9594:1993-6

[6] „The Directory: Selected Object Classes“, ITU-T Recommendation X.521 — ISO/IEC 9594:1993-7)

[7] Sollins, K., „A plan for Internet Directory Services“, RFC 1107, July 1989

[8] Hardcastle-Kille, S., et.al., „A strategic Plan for deploying an Internet X.500 Directory service“, RFC 1430, February 1993

[9] Postel, J., Anderson, C., „White pages meeting report“, RFC 1588, February 1994

[10] Jurg, P., Introduction to White Pages Services based on X.500, RFC 1684, August 1994

[11] The North American Directory Forum, „A naming scheme for c=US“, RFC 1255, September 1991

[12] Barker, P., Kille, S., Lenggenhager, T., „Naming and Structuring Guidelines for X.500 Directory Pilots, RFC 1617, May 1994

[13] Michaelson, G., Prior, M., „Naming Guidelines for the AARNet X.500 Directory Service“, RFC 1562, December 1993

[14] Wahl, M., Howes, T., Kille, S., „Lightweight Directory Access Protocol (v3)“, RFC 2251, December 1997

[15] Wahl, M., „A Summary of the X.500(96) User Schema for use with LDAPv3, RFC 2256, December 1997

[16] Grimstad, A., Huber, R., Sataluri, S., Wahl, M., “Naming Plan for Internet Directory-Enabled Applications“, RFC 2377, September 1998

[17] Hardcastle-Kille, S., „X.500 and Domains“, RFC 1279, November 1991

[18] Barker, P., Kille, S., „The COSINE and Internet X.500 Schema“, RFC 1274, November 1991

[19] Kille, S., Wahl, M., Grimstad, A., Huber, R., Sataluri, S., „Using Domains in LDAP/X.500 Distinguished Names“, RFC 2247, January 1998

[20] „Codes for the Representation of Names and Countries“, ISO 3166:1988

[21] Kuhn, M., Spanier, K., „Richtlinien zur Vergabe von Organisations-Namen im DFN Directory, DFN Text 5, Version 0.4, Dezember 1992

[22] Gietz, P., „Richtlinien für die Namensgebung von Organisationen im deutschen Teilbaum des Directory“, DS-Info 4, (work in progress)

[23] Gietz, P., „Thessaurus zu Alias-Kategorien für den automatischen Aufbau von Sichtweisen im deutschen Directory“, DS-Info TP 3.0, aktuelle Version unter:
`www.directory.dfn.de/ds-info/tp.html`
(work in progress)

[24] Wahl, M., „MIME Directory Profile for LDAP Schema“, draft-ietf-schema-ldap-01.txt, August 1998, (work in progress)

[25] Gietz, P., „OIDs und Definitionen von DFN Directory Services“, DS-Info TP 4.0, aktuelle Version unter:
`www.directory.dfn.de/ds-info/tp.html`
(work in progress)

Autor

Peter Gietz
DFN Directory Services
Zentrum für Datenverarbeitung der Universität Tübingen

E-Mail: `peter.gietz@directory.dfn.de`
DN: `cn=Peter Gietz, o=DFN Directory Services, c=DE`