

1
2
3

<h1>Spezifikation LDAP-gv.at</h1>		Konvention	
		LDAP-gv.at 2.2.9 2005-07-05	
Entwurf öffentlich			
Kurzbeschreibung:	Spezifikation des LDAP-Schemas für den Verzeichnisdienst der Verwaltung und den Portalverbund.		
Autor:	Rainer Hörbe Robert Wollendorfer DI Michael Liehmann	Projektteam / Arbeitsgruppe:	Arbeitsgruppe Verzeichnisdienste (Teil 1) Arbeitsgruppe Autorisierungssysteme (Teil 2)

4
5

Stelle:	vorgelegt am:	angenommen am:
IKT-Board		
Städtebund		
Gemeindebund		
Länder		

6
7
8
9
10
11
12

13	Inhalt	
14		
15		
16	1. Dokumentstruktur	3
17	2. LDAP-Modell (allgemein)	3
18	2.1 Abgrenzung	3
19	2.2 Directory Information Tree (DIT)	3
20	2.3 Abbildung der Aufbauorganisation	3
21	2.4 Klassen- und Attributbeschreibung	4
22	2.5 Allgemeine Attribute	5
23	2.6 Zugriffssteuerung	5
24	3. LDAP-Klassen TEIL 1.....	6
25		

26 1. Dokumentstruktur

27 Dieses Dokument ist in zwei Teile geteilt. Der erste Teil definiert die Objekte zur
 28 Darstellung von Personen, Aufbauorganisation, Kontakten, Adressbuch, etc.
 29 Der zweite Teil spezifiziert Objekte für Berechtigungssysteme.

30 2. LDAP-Modell (allgemein)

31 2.1 Abgrenzung

32 Im ldap.gv.at-Verzeichnis werden Objekte der österreichischen Verwaltung geführt.
 33 Mit **gvOrganisation** werden eigenständige Verwaltungseinheiten dargestellt, wie
 34 Gemeinden, Länder, Ministerien, Selbstverwaltungskörper etc.
 35 Ihre Geschäftseinteilung wird mit Objekten der Klasse **gvOrgUnit** abgebildet, und
 36 die Personeneinträge der Klasse **gvOrgPerson** sind Mitarbeiter im weiteren Sinn,
 37 also auch Wartungspersonal von Dienstleistern oder freie Mitarbeiter.
 38 Die weiteren Klassen dienen zur Definition von Benutzerrechten an Anwendungen,
 39 die über Organisationen verteilt sein können.

40 2.2 Directory Information Tree (DIT)

- 41 • Der LDAP Verzeichnisdienst ist als verteilter Dienst mit gemeinsamen DIT-Wurzel-
 42 Objekt (Klasse Domain, **Fehler! Verweisquelle konnte nicht gefunden**
 43 **werden.**), welches den **DN**(Distinguished Name) dc=at führt, konzipiert.
- 44 • Unter dem Wurzel-Objekt sind die Domainobjekte mit dem DN „dc=gv,dc=at“,
 45 „dc=or,dc=at“ etc. angeordnet.
- 46 • Unterhalb der Domain-Objekte sind die Wurzelknoten von Organisationen. Jede
 47 Personal führende Organisation, an die vom Anwendungsverantwortlichen Rechte
 48 delegiert werden, hat einen eigenen Eintrag der Klasse **gvOrganisation** für
 49 ihren Teilbaum.
- 50 • Parallel zur Hierarchie der Domain Components, die den Internet-Domänen
 51 folgen, soll die Org-ID (internes Verwaltungskennzeichen **Fehler!**
 52 **Verweisquelle konnte nicht gefunden werden.**) als Alternative verwendet
 53 werden. Besonders in der Bundesverwaltung, wo Domänen oft kurzlebig sind, ist
 54 diese zusätzliche Adressierung sinnvoll. Diese wird über combined DNs erreicht.
 - 55 ○ zb.: wenn die Domäne eines Ministeriums bmxzyz.gv.at ist, und der Org-ID
 56 AT:b:164, dann wäre der DN des obersten Knotens des Ministeriums:
 57 dc=bmxzyz + gvOuId=AT:b:164, dc=gv, dc=at
- 58 • Auf der Hierarchie-Ebene unterhalb der Organisationen sind Container-Objekte
 59 der Klasse OrganizationalUnit, die für die anderen Objektklassen getrennte
 60 Namesräume schaffen und für die ACLs vorgesehen sind.

61 2.3 Abbildung der Aufbauorganisation

62 Die Aufbauorganisation entsprechend der Geschäftseinteilung, wird unterhalb des
 63 Container-Objekts mittels der Objektklasse **gvOrgUnits** abgebildet. Sollen Benutzer
 64 nicht die gesamte Aufbauorganisation zu sehen bekommen, sind diese Teile über
 65 ACLs für die entsprechenden Benutzer zu sperren.

66

67 Andere Formen der Aufbau-Organisation, wie sie z.B. für Rechteverwaltungen und
 68 Workflow-Systeme benötigt werden, sind unterhalb des Containers **gvGroups** zu
 69 führen. In der Datenwartungsanwendung kann es sinnvoll sein, einen Teil der
 70 korrespondierenden Objekte unter **gvOrgUnit** und **gvGroup** so zu führen, dass für
 71 den Benutzer der Anschein entsteht, dass es jeweils nur einen Eintrag gibt. Damit
 72 lassen sich Schattenhierarchien aufbauen, die teilweise mit der Geschäftseinteilung
 73 übereinstimmen.

74 Die Hierarchie im Objekt gvOrgUnit durch das Attribut **gvOuidParent** definiert,
 75 womit der DN gleich bleibt, wenn sich die übergeordnete Hierarchie ändert.

76 Attribute vom Typ ‚dn‘, die somit Pointer auf Einträge enthalten, SOLLEN die
 77 Organisation über das Attribut ‚gvOuid‘ adressieren, nicht über ‚dc‘.

78

79 2.4 Klassen- und Attributbeschreibung

80 In Kapitel 3 und Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**
 81 werden die einzelnen Objektklassen detailliert beschrieben. Die jeweiligen Attribute
 82 und Eigenschaften werden durch folgenden Beschreibungskürzel definiert:

83 2.4.1. Kardinalität des Attributes

84 **leer** (default): optional

85 **M**: mandatory (Pflichtfeld)

86 2.4.2. Einzelwert/Liste

87 **leer** (default): single-valued

88 **L**: multi-valued

89 2.4.3. Type (Syntax, Matching)

- 90 • leer bedeutet das gleiche wie cis
- 91 • bin binary
- 92 • cis Directory String (UTF8),
93 Matching: Case Insensitive
- 94 • ces Directory String (UTF8),
95 Matching Case Exact String
- 96 • dn Distinguished Name
- 97 • ia5 IA5-String (auch ISO 646 oder US-ASCII bezeichnet)
- 98 • int Integer
- 99 • jpeg JPEG Bild
- 100 • tel Telephone Number
- 101 • uri PrintableString; Matching: Case Exact String

102 Wenn ein numerischer Wert in Klammern angegeben wird, die das die max. Länge,
 103 z.B. cis(64) für einen directoryString mit bis zu 64 Zeichen. Die Länge kann kürzer
 104 sein als sie durch RFCs normiert ist.

105 Im Hinblick auf eine mögliche EU-weite Kommunikation werden Attributnamen und
106 Listenwerte in englischer Sprache definiert.

107 Alle Attribute, die nicht in einem RFC definiert sind, haben den Präfix 'gv'.
108

109 2.5 Allgemeine Attribute

110 ○ Für Erstellung und Modifikation sind pro Objektklasse **Fehler! Verweisquelle**
111 **konnte nicht gefunden werden.** server-maintained Attribute zu führen.

112 • **createTimestamp**: Zeitpunkt der Erstellung des Eintrags

113 • **modifyTimestamp**: Zeitpunkt der letzten Modifikation
114

115 2.6 Zugriffssteuerung

116 ○ Zugriffsstufen auf Eintrags- und Attributebene sind auf drei Ebenen definiert:

117 ○ **local** - die im internen Netz der Organisation publizierten Daten

118 ○ **intra** - die im Behörden-Intranet publizierten Daten als Teilmenge von
119 ‚local‘

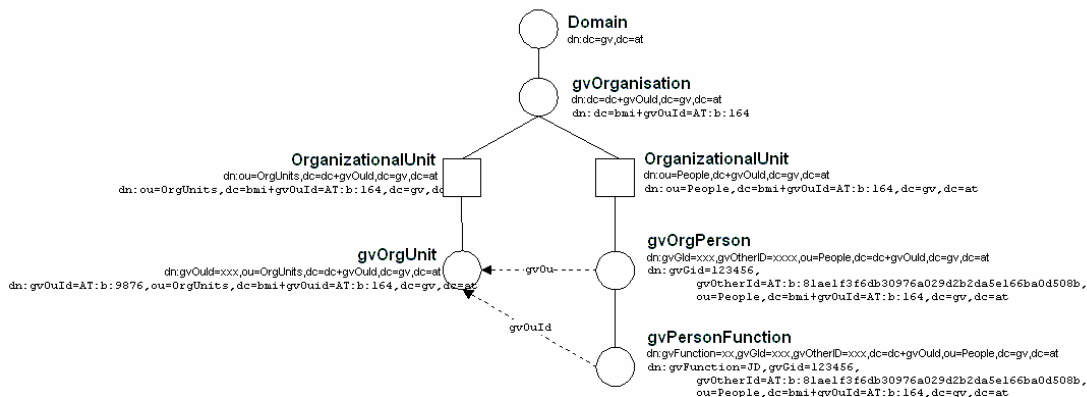
120 ○ **public** - die im Internet für anonyme Benutzer publizierten Daten als
121 Teilmenge von ‚intra‘)

122 Die Zugriffsstufe auf Eintragungsebene wird über das Attribut **gvScope** gesetzt,
123 um eine einfache Zugriffssteuerung realisieren zu können.

124 Darüber hinaus gehend wird im Schema keine Zugriffsteuerung
125 berücksichtigt, um eine differenzierte Publikation von Attributen wie
126 Telefonnummern und E-Mail-Adressen zu erreichen. Die entsprechenden
127 Strukturen sind intern zu realisieren und für den Client nicht sichtbar. Die
128 Unterscheidung wird durch unterschiedliche Server-Adressen erreicht, die
129 entweder unterschiedliche Server-Instanzen adressieren oder
130 Authentifizierungs-Proxies für unterschiedlich berechnigte User am Server
131 sind.

3. LDAP-Klassen TEIL 1

Im folgenden Schema wird dargestellt, wie Objekte in Abhängigkeit von ihren Klassen im DIT (Directory Information Tree) positioniert werden müssen:



- 137
- 138
- 139 • **Domain:** Abbildung der Domain-Struktur oberhalb von Organisationen, um die
- 140 Interent.Domänen wie gv.at, or.at etc. abzubilden.
- 141
- 142 • Die Organisation, abgebildet durch die Klasse **gvOrganisation**, hat bei
- 143 Bediensteten die Personalhoheit für die Person und ist daher für die
- 144 Benutzerverwaltung rechtlich zuständig. Eine natürliche Person kann auch als
- 145 gvOrgPerson Einträge in mehreren Domains existieren, wenn sie (Dienst-, ..)
- Verträge mit verschiedenen Organisationen hat.
- 146 • Unterhalb einer Organisation sind Container-Objekte
- 147 **OrganizationalUnits** (zb: people, orgUnits, ..) um für diese Objektklassen
- 148 getrennte Namensräume zu schaffen.
- 149 • **gvOrgPerson:** Derzeit werden nur Bedienstete (Mitarbeiter) von Behörden
- 150 berücksichtigt, deren Personendaten jeweils von der Personal führenden Stelle
- 151 gewartet werden. Dies wird in nächster Zukunft über das PM/SAP durchgeführt
- 152 werden.
- 153 Die Zusammenführung mehrerer gvOrgPerson Einträge auf die gleiche natürliche
- 154 Person erfolgt durch globale Identifier **gvGid** und **gvbPK**. Da in SAP eine Person
- 155 mehrmals in einer Organisation vorkommen kann, muss eine eindeutige
- 156 Rferenzierung über dieses Tupel erfolgen.
- 157 Für Mitarbeiter, die keine Bediensteten sind (Leiharbeitsverträge, Werksverträge,
- 158 etc.) gilt das im übertragenen Sinn.
- 159 • Wenn eine Person in einer Organisation unterschiedliche Funktionen mit
- 160 unterschiedlichen Rechten hat, werden die Rechte zusätzlich an Funktionen der
- 161 Person mittels der Objektklasse **gvPersonFunction** vergeben.
- 162 • Die Differenzierung der Rechte nach Funktionen kann zum Beispiel für folgende
- 163 Situationen genutzt werden:
 - 164 ○ Entwickler und Administratoren (Entwicklungs- vs. Testuser)
 - 165 ○ Vertretungsrechte

- 166 ○ Tätigkeit für verschiedene Organisationseinheiten
- 167 ○ Sonderdienste (z.B. hat ein Wachbeamter für die Zeit, in der er
- 168 Journaldienst verrichtet, erweitere Berechtigungen)
- 169 • Personen können mehreren Organisationseinheiten zugeordnet werden. In
- 170 diesem Fall MÜSSEN die Zuordnungen von gvPersonFunction gleichzeitig in
- 171 gvOrgPerson eingetragen werden, und zwar als Attributliste in gvOu.
- 172 • Die Organisationseinheiten werden im Sinne des DIT flach abgebildet. Die
- 173 Hierarchie der Aufbauorganisation wird über das Attribut gvOuIdParent
- 174 implementiert.
- 175

gvOrganisation (Achtung! nicht mit ,z' geschrieben)	Wurzelknoten für eine Organisation Abgeleitet von gvOrgUnit (die von gvOrgUnit abgeleiteten Attribute sind hier wegen der übersichtlicheren Darstellung nicht repliziert)	
dn: dc=... (dn: dc=bmi+gvOuID=AT:b:164, dc=gv, dc=at)		
Attribut	Beschreibung (Beispiel)	Eigen schaft
dc	Domain der Organisation des Dateneigners. Der Wert MUSS unterhalb des übergeordneten Domain-Objekts eindeutig sein (dc=bmi, dc=gv, dc=at)	M, ia5
O	Bundesministerium f. Inneres	M, cis(64)
Weitere Attribute siehe gvOrgUnit Die Beschreibung für gvLegalSuccessor gilt im analogen Sinn für Organisationen		

176

177

gvOrgPerson	Person in einem Vertragsverhältnis zu einer Organisation. Abgeleitet von InetOrgPerson.	
dn: gvGID=..., ou=People, dc=... (dn: gvGID=234523, gvOtherID=AT:B:0:123456, ou=People, dc=bmi+gvOuID=AT:B:164, dc=gv, dc=at)		
Attribut	Beschreibung (Beispiel)	Eigenschaft
cn	Vorname Familienname (Martin Mustermann)	M, L, cis(64)
displayName	Einer der Werte aus cn (RFC 2798[xx]) im Format „Familienname, Vorname“	cis(64)
sn	Familienname laut Stammzahlregister-Anfrage (Mustermann)	M, cis(64)
givenName	Vorname laut Stammzahlregister-Anfrage (Martin)	cis(64)
gvGID	Global Identifier: im Bund die Personalnummer aus SAP	M ces(128)
gvBirthdate	Geburtsdatum im Format JJJJ-MM-TT	cis(10) ¹
gvbPK	bPK des Benutzers für den Bereich Personalverwaltung (AT:B:0:123456)	M, ces(32)
gvOPK	bPK des Organwalters der Person (01afdfkl6d2e0976a0292232dcfep06bk9d220b)	ces(128)
UID	Innerhalb der Domäne eindeutige Userkennung + Domain-Suffix im RFC 822[xx]-Format als Login-ID für Portale (mmustermann@bmi.gv.at)	cis(256)
gvSex	Geschlecht der Person (male, female oder unknown)	cis(7)
personalTitle	Akademischer Titel (Mag. d. s. K.)	cis(64)
title	Funktionsbezeichnung (Abgeordneter z. NR., Bezirkshauptfrau, ..)	cis(64)
gvAmtstitel	Amtstitel (Hofrat)	cis(64)

¹ Wenn bei einem Geburtsdatum der Tag nicht bekannt ist, wird er auf 0 gesetzt. Analoges gilt für den Monat. Um formalen Datumsprüfungen zu entgehen, wird das Attribut als String typisiert.

Spec LDAP gv.at

telephoneNumber	Tel-Nummer(n) wie in RFC 2252 [xx] § 6.30 Format: +LL VVVV AAAAAA NNNN L: Landescode; V: Vorwahl; A: Anschluss-Nummer; N: Nebenstelle außer der Nebenstelle sind alle Teile verpflichtend	L, tel(32)
mobile	Format wie telephoneNumber	L, tel(32)
facsimileTelephone Number	Fax-Nummer Format wie telephoneNumber	L, tel(32)
street	Straße der Postanschrift (<i>Rathausstr. 1</i>)	cis(128)
postOfficeBox	Postfach der Postanschrift (Postfach 103)	cis(40)
postalAddress	Postanschrift ohne Name Format: (max. 6 Zeilen á 40 Zeichen; die Zeilen sind durch \$ getrennt) Formatiert nach den Empfehlungen der österreichischen Post AG [7] (<i>Hintere Salzamtstraße 1\$1030 Wien</i>)	cis(245)
postalCode	Postleitzahl der Postanschrift ohne Ländercode (<i>1082</i>)	cis(13)
l	Ort (<i>Wien</i>)	cis(64)
c	Land der Postadresse (2-stelliges Kürzel nach ISO 3166-1) (<i>AT</i>)	cis(2)
co friendlyCountryName	Land ausgeschrieben - in Deutsch	cis(64)
gvPhysicalAddress	Besuchs- und Lieferadresse Format wie postalAddress	cis(245)
roomNumber	Zimmernummer	cis(256)
mail	RFC 822 E-Mail Adresse im simple format (Nur Werte, deren Zugriffsstufe public ist) (<i>martin.mustermann@bmi.gv.at</i>)	cis(256)
jpegPhoto	Portrait in der Größe bis zu 120x160 Pixel in JPEG- Codierung. Die empfohlene Größe ist bis 5 kB	L, jpeg
gvOuID	gvOuID (Org-ID) der Organisationseinheit(en), zu der die Person zugeteilt ist (kein dn) (<i>gvOuID= AT:19:9876</i>)	cis(32)

gvRights	<p>Liste der dem Benutzer gewährten Rechte pro Anwendung im Stammportal einschließlich der dazugehörigen Parameter. Wird auch zum Aufbau von Menüs verwendet. Das Format ist:</p> <pre>app-dn \$ role(role-param [, role-param]..); role(role-param)..</pre> <p>Die Schreibweise [Delimiter Token].. bedeutet, dass Token mehrfach wiederholt werden kann, wenn es durch Delimiter getrennt ist.</p> <pre>gvAppId=ZMR, ou=Applications,dc=bmi+gvOuid=AT:b:164, dc=gv, dc=at \$ zmr-behoerdenanfrage(GKZ=10101, GKZ=10103); zmr-fremdenbehoerdenanfrage(GKZ=10100)</pre>	L, ces(2048)
gvSecClass	<p>Maximale Sicherheitsstufe, für die eine Person administrativ eingestuft ist, z.B.: durch Identifikation und Schulung. Dieser Wert wird vom Portal zusammen mit anderen Parametern (z.B. Qualität der Authentifizierung) verwendet, um die Sicherheitsklasse einer Transaktion zu bestimmen. Siehe [4]</p> <p>Werte: 0 bis 3</p>	int(1)
description	<p>Frei verwendbares Feld. Einträge länger als 1024 Zeichen sind als Liste von Strings <= 1024 Zeichen abzuspeichern. Die Trennung erfolgt beim letzten Whitespace vor der maximalen Stringlänge.</p>	cis(1024)
gvStatus	<p>Objekt im LDAP gültig (<i>active</i> oder <i>inactive</i>)</p>	M, cis(32)
gvSource	<p>ID- und Zeitstempel des Benutzers, der die Transaktion veranlasst hat. Die Zeit wird sekundengenau eingetragen. ISO 8601 erlaubt Füllzeichen zur besseren Lesbarkeit:</p> <pre>yyyy-mm-ddThh:mm:ssZ</pre> <p>Z steht für die Zeitzone UTC, T trennt Datum und Zeit.</p> <p>Format: User-DN/Datum-Zeit; Zeitzone=UTC (<i>gvGID=AT:b:0:81ae1f3f6db30976a029d2b2da5e166ba0d508b, ou=people, gvOuid=AT:b:164, dc=gv,dc=at/2003-05-15T12:00:01</i>)</p>	M, cis(256)
gvScope	<p>Zugriffsstufe (<i>public, gv.at, local, intra</i>)</p>	M, cis(32)

179

180

181

182

183

- Der Inhalt des Attributs **gvGID** ist der Präfix ‚AT:B:0:‘ und im Bund die aus SAP gelieferte Personenkennzahl der Person.
- Weitere optionale und im Arbeitskreis nicht besprochene Attribute sind in **Fehler! Verweisquelle konnte nicht gefunden werden.** definiert.

- 184
- 185
- 186
- 187
- 188
- Die Werte in den Attributen *gvStatus* und *gvSex* werden im Klartext (nicht abgekürzt) gespeichert
 - UserIDs sind nach der Löschung für die Dauer von 3 Jahren nicht mehr neu zu vergeben.

gvPersonFunction		Funktionen einer Person, um unterschiedliche Anwendungsrechte abzubilden
dn: gvFunction=..., gvGID=..., ou=People, dc=... (dn: gvFunction=JD,gvGID=AT:b:0:123456, ou=People,dc=bmi+gvOuID=AT:b:164,dc=gv,dc=at)		
Attribut	Beschreibung (Beispiel)	Eigenschaft
gvFunction	Kurze Funktionsbezeichnung (JD)	M,cis(32)
Description	Funktionsbezeichnung (<i>Journaldienst</i>)	cn(64)
gvOuID	gvOuID der Organisationseinheit, zu der die Person in dieser Funktion zugeteilt ist. Der Wert muss auch in gvOu in gvOrPerson enthalten sein. (<i>gvOuId=AT :I9 :9876</i>)	cis(32)
gvRights	Wie gvOrgPerson	L, dn
gvStatus	Wie gvOrgPerson	M
gvSource	Wie gvOrgPerson	M
gvScope	Wie gvOrgPerson	M

- 189
- 190
- 191
- 192
- 193
- Das Portal kann intern für Anwendungen, die innerhalb einer Session Rechte nicht nach Funktionen differenzieren können, UserID und Funktion auf eine applikationsspezifische UserID abbilden.

gvOrgUnit		1. Organisationseinheit 2. Organisation gvOrgUnit wird von OrganizationalUnit abgeleitet
dn : gvOuID=..., ou=OrgUnits,dc=... (dn: gvOuId=AT: b:9876, ou=OrgUnits,dc=bmi+gvOuId=AT:b:164,dc=gv,dc=at)		
Attribut	Beschreibung (Beispiel)	Eigenschaft
gvOuID	Eindeutige numerische Organisationbezeichnung, internes Verwaltungskennzeichen (AT + Org-ID) (<i>AT:I9:9876</i>)	M, cis(32)
gvOuVKZ	Eindeutige alphanumerische Organisationbezeichnung, internes Verwaltungskennzeichen (AT + VKZ) (<i>AT:BMI-S1-3</i>)	M, cis(64)

Spec LDAP gv.at

ou	Vewaltungskennzeichen Kurzbezeichnung der Organisationseinheit <i>(IV/2-e)</i>	M, cis(64)
gvOuidParent	Übergeordnete OE; Wert: gvOuid der übergeordneten OEs (kein dn!)	cis(32)
cn	Kurzbezeichnung der Organisationseinheit (ausgeschrieben) <i>(Abt. ITMS/Ref. NIK - Referat nationale und internationale Koordination)</i>	M, L, cis(64)
gvOuCn	Gesamtbezeichnung der Organisationseinheit (für die Anschrift ohne Adressteil) <i>(Bundesministerium für Inneres Sektion IV/Abt. ITMS/Ref. NIK)</i>	M, cis(1024)
mail	RFC 822 E-Mail Adresse <i>(helpdesk@xyz.gv.at)</i>	cis(256)
telephoneNumber	Tel-Nummer	L, tel(32)
facsimileTelephone Number	Fax-Nummer	L, tel(32)
street	(Postadresse, nicht Standortadresse)	cis(128)
postOfficeBox	Postfach der Postanschrift (Postfach 103)	cis(40)
l	Ort <i>Wien</i>	cis(64)
postalAddress	Wie gvOrgPerson	cis(245)
postalCode	Wie gvOrgPerson	cis(40)
c	Wie gvOrgPerson	cis(2)
co friendlyCountryName	Wie gvOrgPerson	cis(64)
gvPhysicalAddress	Wie gvOrgPerson	cis(245)
gvImageRef	Verwendung + Referenz auf Bilder im Format {Verwendung} URI Standardverwendungen sind Logo, Zugang und Zufahrt, die Liste kann erweitert werden; z.B.: <i>{logo} http://www.xyz.gv.at/logo1.jpg {Zugang}http://www.xyz.gv.at/zugang.jpg</i>	L, uri
gvWebAddress	URL der Homepage	uri
description	Frei verwendbares Feld	cis(1024)

gvLegalSuccessor	gvOuid der Organisation oder OE, die die unmittelbare Rechtsnachfolge antrat. Wenn die Organisation ohne Rechtsnachfolge aufgelöst wurde, ist der Wert „none“. Besteht die OE noch (gvStatus = active), ist dieses Attribut leer	cis(32)
gvSortkey	Zur Festlegung der Sortierreihenfolge in Listen von OEs der gleichen Ebene wird gvSortkey als erster und ou als zweiter Sortierschlüssel verwendet	cis(64)
gvNotValidBefore	nicht gültig vor - im Format JJJJ-MM-TT	M, cis(10)
gvNotValidAfter	nicht gültig nach - im Format JJJJ-MM-TT	cis(10) ²
gvStatus	Wie gvOrgPerson	M
gvSource	Wie gvOrgPerson	M
gvScope	Wie gvOrgPerson	M
gvOtherID	Zusätzliche(s) Kennzeichen zum Datenabgleich	ces(128)
...	Weitere optionale Attribute sind im RFC 2256 [5] definiert	

194

195

196

197

198

- Das Attribut *gvLegalSuccessor* zeigt immer zum unmittelbaren Rechtsnachfolger. Dieser kann wiederum einen Rechtsnachfolger haben. Um den aktuellen Rechtsnachfolger einer Organisationseinheit oder einer Organisation zu finden, muss die Verkettung bis ans Ende aufgelöst werden.

² Wenn die Organisationseinheit besteht (aktiv ist), bleibt der Eintrag leer.

199

OrganizationalUnit		OID: 2.5.6.5 Knoten zur Definition von Namensräumen unterhalb des Domain-Eintrags
dn : ou=..., dc=... (dn: ou=People, dc=bmi+gvOuid=AT:b:164,dc=gv,dc=at)		
Attribut	Beschreibung (Beispiel)	Eigen-schaft
ou	Namespace (People)	M, cis(64)

200