

**Gelöscht:** Spezifikation des LDAP-Schemas für den Portalverbund. Das Schema wurde mit dem LDAP-Schema der Arbeitsgruppe Verzeichnisdienste (IKT-Board) abgestimmt, dessen Anwendungen weiter gefasst sind.¶

**Gelöscht:** behördenübergreifende Autorisierungssysteme

Spezifikation LDAP-gv.at		Konvention	
		LDAP-gv.at 2.1.0 <u>27.06.2003</u>	
		Entwurf öffentlich	
Kurzbeschreibung:	<p><u>Spezifikation des LDAP-Schemas für Verzeichnisdienst der Verwaltung und Portalverbund.</u></p> <p><u>Die Erweiterungen der Version 2.1 dienen hauptsächlich der Einrichtung eines Verzeichnisdienstes als Basisdienst des e-Governments.</u></p>		
Autor:	Rainer Hörbe (Stabsstelle IKT)	Projektteam / Arbeitsgruppe:	Arbeitsgruppe <u>Verzeichnisdienste</u> (Teil 1) Arbeitsgruppe Autorisierungssysteme (Teil 2)

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

## Dokument

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

## Begriffsbestimmung

Siehe Dokument [1]

# LDAP-Modell (allgemein)

## Abgrenzung

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

## Directory Information Tree (DIT)

- Das Wurzel-Objekt (Klasse Domain) hat den DN dc=at. Darunter sind die Domainobjekte „dc=gv,dc=at“, „dc=or,dc=at“ etc. angeordnet.
- Unterhalb der Domain-Objekte sind die Wurzelknoten von Organisationen mit dem DN: dc nach RFC 2247. Jede Personal führende Organisation, an die vom Anwendungsverantwortlichen Rechte delegiert werden, hat einen eigenen Eintrag der Klasse Organization für ihren Teilbaum.
- Parallel zur Hierarchie der Domain Components, die den Internet-Domänen folgen, soll die Org-ID (internes Verwaltungskennzeichen) als Alternative verwendet werden. Besonders in der Bundesverwaltung, wo Domänen oft kurzlebig sind, ist diese zusätzliche Adressierung sinnvoll. Diese wird über combined DN's erreicht. Z.B. wenn die Domäne eines Ministeriums bmxyz.gv.at ist, und der Org-ID ATb:4711, dann wäre der DN des obersten Knotens des Ministeriums:  
dc=bmxyz + gvOuId=AT:b:4711, dc=gv, dc=at
- Der LDAP Verzeichnisdienst ist als verteilter Dienst mit gemeinsamen DIT-Root (dc=at) konzipiert.

**Gelöscht:** Über den ersten Teil wurde in der Arbeitsgruppe ein Konsens erzielt, der zweite Teil wurde vom BRZ nicht angenommen.¶  
Der erste Teil des Schemas enthält die für die Authentisierung, der zweite Teil die für Autorisierung und Navigation relevanten Daten.

**Gelöscht: Einführung¶**  
Zweck dieses Schemas ist die Definition einer externen LDAP-Sicht auf Daten von Benutzerverwaltungssystemen, welche die Kooperation von Web-Portalen mit delegierter Benutzerverwaltung, einheitlicher Menüführung, Single Sign-On und Revision nach dem Datenschutzgesetz ermöglicht. Die Quelle dieser Daten kann eine interne LDAP-Struktur oder ein RDBMS sein. Das Verzeichnis ist zwar nicht zur Verwaltung der Einträge gedacht oder optimiert, sondern für die Präsentation der für ein Portal relevanten Informationen (Benutzer, Applikationen, Rechte). Allerdings soll das derzeitige Konzept zukünftigen Applikationen den schreibenden Zugriff auf die Daten ermöglichen. Die Verbindung zwischen interner Benutzerverwaltung und LDAP sollte synchron sein.¶  
In diesem Schema sind interne Objekte und Attribute des Portals nicht berücksichtigt, wie etwa Daten zur Login-Verwaltung, Authentifikation über X.509-Zertifikate oder Trust-Beziehungen zu Fremdportalen.¶  
Die hier betrachtete Benutzerdomäne ist beispielhaft wie folgt strukturiert.¶

... [1]

**Gelöscht:** Organisation ... [2]

**Gelöscht:** Schema

**Gelöscht:** DIT-Root

**Gelöscht:**

**Gelöscht:** (abgeleitet aus Organization), mit

**Gelöscht:** dn

**Gelöscht:** gv.at oder .

- Auf der Hierarchie-Ebene unterhalb der Organisationen sind Container-Objekte der Klasse OrganizationalUnit, die für die anderen Objektklassen getrennte Namesräume schaffen und für die ACLs vorgesehen sind.

Gelöscht: zweiten

## Abbildung der Aufbauorganisation

Die Aufbauorganisation entsprechend der Geschäftseinteilung wird unterhalb des container-Objekts ou=orgUnits abgebildet. Sollen Benutzer nicht die gesamte Aufbauorganisation zu sehen bekommen, sind diese Teile über ACLs für die entsprechenden Benutzer zu sperren.

Andere Formen der Aufbau-Organisation, wie sie z.B. für Rechteverwaltungen und Workflow-Systeme benötigt werden, sind unterhalb des Containers ou=groups zu führen. In der Datenwartungsanwendung kann es sinnvoll sein, einen Teil der korrespondierenden Objekte unter ou=orgUnits und ou=Groups so zu führen, dass für den Benutzer der Anschein entsteht, dass es jeweils nur einen Eintrag gibt. Damit lassen sich Schattenhierarchien aufbauen, die teilweise mit der Geschäftseinteilung übereinstimmen.

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

Attribute vom Typ dn, (die also Pointer auf Einträge enthalten), SOLLEN die Organisation über das Attribut gvOuid adressieren, nicht über dc.

## Klassen- und Attributbeschreibung

In der Spalte Eigenschaften eines Attributes bedeutet:

M bedeutet mandatoy (= required); Default ist optional (= allowed).

L bedeutet multi-valued, leer (Default) bedeutet single-valued

Typen:

- bin binary
- cis Directory String (UTF8), Case Insensitive Match (Default)
- ces Directory String (UTF8), Case exact Match
- dn Distinguished Name
- int Integer
- tel Telephone Number
- uri URI (RFC 2396)

Gelöscht: String

Gelöscht: String

Formatiert: Nummerierung und Aufzählungszeichen

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

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

**Gelöscht:** Es wurden noch keine  
OID Werte beantragt.

**Gelöscht:** neuen

## **Allgemeine Attribute**

- Für Erstellung und Modifikation sind pro Objektklasse RFC2251 server-maintained Attribute zu führen.
  - createTimestamp: Zeitpunkt der Erstellung des Eintrags
  - modifyTimestamp: Zeitpunkt der letzten Modifikation

## **Zugriffssteuerung**

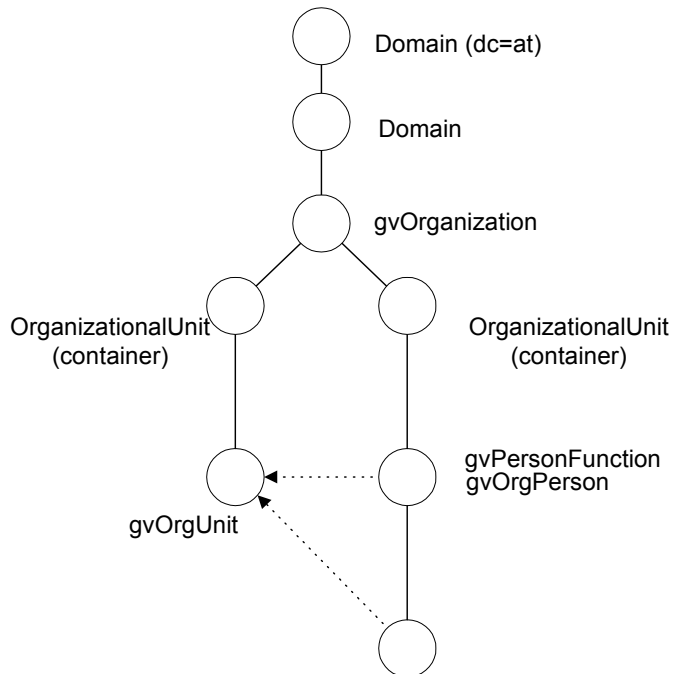
- Zugriffsstufen auf Eintrags- und Attributebene sind auf drei Ebenen definiert:
  - „local“ (die im internen Netz der Organisation publizierten Daten)
  - „gv.at“ (die im Behörden-Intranet publizierten Daten als Teilmenge von „local“)
  - „public“: (die im Internet für anonyme Benutzer publizierten Daten als Teilmenge von „gv.at“)

Die Zugriffsstufe auf Eintragebene wird über das Attribut gvScope gesetzt, um eine einfache Zugriffssteuerung realisieren zu können.

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

# LDAP-Klassen TEIL 1

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



- Domain: Abbildung der Domain-Struktur oberhalb von Organisationen, um die Interent.Domänen wie gv.at, or.at etc. abzubilden.
  - Die Organisation, (abgebildet durch die Klasse gvOrganization), hat bei Bediensteten die Personalhoheit für die Person und ist daher für die Benutzerverwaltung rechtlich zuständig. Eine natürliche Person kann auch als gvOrgPerson Einträge in mehreren Domains existieren, wenn sie (Dienst-, ..) Verträge mit verschiedenen Organisationen hat.
  - Unterhalb einer Organisation sind Container-Objekte (ou=people, ou=orgUnits, ..) um für diese Objektklassen getrennte Namesräume zu schaffen.
  - gvOrgPerson: Derzeit werden nur Bedienstete (Mitarbeiter) von Behörden berücksichtigt, deren Personendaten jeweils von der Personal führenden Stelle gewartet werden. Die Zusammenführung mehrerer gvOrgPerson Einträge auf die gleiche natürliche Person erfolgt durch einen Global Identifier. Innerhalb einer Organisation DARF eine Person nur in einem gvOrgPerson-Objekt abgebildet werden.

**Gelöscht:** die durch die Domain definiert

Für Mitarbeiter, die keine Bediensteten sind (Leiharbeitsverträge, Werksverträge, etc.) gilt das im übertragenen Sinn.

- Wenn eine Person in einer Organisation unterschiedliche Funktionen mit unterschiedlichen Rechten hat, werden die Rechte zusätzlich an Funktionen der Person (gvPersonFunction) vergeben.
  - Die Differenzierung der Rechte nach Funktionen kann zum Beispiel für folgende Situationen genutzt werden:
    - Entwickler und Administratoren (Entwicklungs- vs. Testuser)
    - Vertretungsrechte
    - Tätigkeit für verschiedene Organisationseinheiten
    - Sonderdienste (z.B. hat ein Wachbeamter für die Zeit, in der er Journaldienst verrichtet, erweiterte Berechtigungen)
  - Personen können mehreren Organisationseinheiten zugeordnet werden. In diesem Fall MÜSSEN die Zuordnungen von gvPersonFunction gleichzeitig in gvOrgPerson eingetragen werden, und zwar als Attributliste in gvOu.
  - Die Organisationseinheiten werden im Sinne des DIT flach abgebildet. Die Hierarchie der Aufbauorganisation wird über das Attribut gvOuIdParent implementiert.

<b><u>gvOrganisation</u></b>	<u>Wurzelknoten für eine Organisation</u> <u>Abgeleitet von gvOrgUnit</u> <u>(die von gvOrgUnit abgeleiteten Attribute sind hier wegen der übersichtlicheren Darstellung nicht repliziert)</u>	
<u>dn: dc=...</u> <u>(dn: dc=bmi+gvOuId=AT:b:4711, dc=gv, dc=at)</u>		
<b>Attribut</b>	<b>Beschreibung (Beispiel)</b>	<b>Eigenschaft</b>
dc	Domain der Organisation des Dateneigners. <u>Der Wert MUSS unterhalb des übergeordneten Domain-Objekts eindeutig sein</u> <i>(dc=bmi, dc=gv, dc=at)</i>	M
o	Bundesministerium f. Inneres	M
Weitere Attribute siehe gvOrgUnit Die Beschreibung für gvLegalSuccessor gilt im analogen Sinn für Organisationen		

<b>gvOrgPerson</b> 1.2.40.0.10.2.1.0.1	Person in einem Vertragsverhältnis zu einer Organisation. Abgeleitet von InetOrgPerson.	
dn: gvGid=..., ou=People, dc=... (dn: gvGid= <u>AT:b:0:81ae1f3f6db30976a029d2b2da5e166ba0d508b</u> , ou=People, dc=bmi+gvOuid= <u>AT:b:4711</u> , dc=gv, dc=at)		
<b>Attribut</b>	<b>Beschreibung (Beispiel)</b>	<b>Eigen-schaft</b>
cn	Vorname Nachname ( <i>Rainer Hörbe</i> )	M, <u>L</u>
<u>displayName</u>	<u>Einer der Werte aus cn (RFC 2798)</u> im Format „Nachname, Vorname“	
sn	Nachname laut ZMR-Anfrage ( <i>Hörbe</i> )	M
givenName	Vorname laut ZMR-Anfrage ( <i>Rainer</i> )	
gvGid	Global Identifier: <u>siehe nachstehende Erläuterung</u> <u>Wenn der Präfix im Format „Owner:System:“ fehlt, ist der Präfix B:0: anzunehmen.</u> ( <u>AT:B:0:81ae1f3f6db30976a029d2b2da5e166ba0d508b</u> )	M
<u>gvOtherId</u>	<u>Zusätzliche(s) Kennzeichen zum Datenabgleich und vorläufige Kennzeichen vor der Eintragung der VPK.</u> <u>Format: siehe Erläuterung im Anschluss</u> ( <u>Beispiel mit einer Sozialvers-Nr und einer Active Directory –SID</u> <u>AT:B:SV:3575240761</u> <u>AT:B:bmi.intra.gv.at-SID:0105000000000051500000</u> <u>093A2A24358A021ADBEB0C508E040000</u> )	<u>L</u>
uid	Innerhalb der Domäne eindeutige Userkennung + Domain-Suffix im RFC822-Format als Login-ID für Portale ( <i>rhoerbe@bmi.gv.at</i> )	
gvSex	Geschlecht der Person ( <i>male, female oder unknown</i> )	
personalTitle	Akademischer Titel ( <i>Mag. d. s. K.</i> )	
title	Funktionsbezeichnung ( <i>Abgeordneter z. NR., Bezirkshauptfrau, ..</i> )	
gvAmtstitel	Amtstitel ( <i>Hofrat</i> )	
telephoneNumber	Tel-Nummer(n) <u>wie in RFC 2252 § 6.30</u> <u>Format: +LL VVVV AAAAAA NNNN</u> <u>L: Landescode; V: Vorwahl; A: Anschluss-Nummer;</u> <u>N: Nebenstelle</u> <u>außer der Nebenstelle sind alle Teile verpflichtend</u>	L, tel
<u>mobile</u>	<u>Format wie telephoneNumber</u>	<u>L</u>
facsimileTelephone	Fax-Nummer	L, tel

Gelöscht: AT471131026100

Gelöscht: AT +  
“Verfahrenskennung”  
(AT471124086133)

Number	<u>Format wie telephoneNumber</u>	
street	Straße oder Postfach <u>der Postanschrift</u> ( <i>Rathausstr. 1</i> )	
postalAddress	Postanschrift ohne Name Format: <u>(max. 6 Zeilen á 40 Zeichen; die Zeilen sind durch \$ getrennt)</u> Formatiert nach den Empfehlungen der österreichischen Post AG [7] <i>Beispiel: Hintere Salzamtstraße 1\$1030 Wien</i>	
postalCode	Postleitzahl <u>der Postanschrift</u> ( <i>1082</i> ) <i>ohne Ländercode</i>	
city	Ort <u>der Postanschrift</u> ( <i>Wien</i> )	
<u>c</u>	<u>Land der Postadresse (2-stelliges Kürzel nach ISO 3166-1)</u> <u>(AT)</u>	
<u>co</u> <u>friendlyCountryName</u>	<u>Land ausgeschrieben (in Deutsch)</u>	
<u>gvPhysicalAddress</u>	<u>Besuchs- und Lieferadresse</u> Format wie postalAddress	
<u>roomNumber</u>	<u>Zimmernummer</u>	
mail	RFC822 E-Mail Adresse <u>im simple format (Nur Werte, deren Zugriffsstufe public ist)</u> ( <i>rainer.hoerbe@bmi.gv.at</i> )	
jpegPhoto	Portrait in der Größe bis zu 120x160 Pixel in JPEG-Codierung. Die empfohlene Größe ist bis 5 kB	<u>L</u>
gvOu	gvOuid (Org-ID) der Organisationseinheit(en), zu der die Person zugeteilt ist ( <u>kein dn</u> ) ( <i>gvOuid=AT:19:987q</i> )	<u>L</u>
gvRights	Liste der dem Benutzer gewährten Rechte ( <i>dn von gvApplicationRights</i> )	L, dn
<u>gvSecClass</u>	<u>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]</u> <u>Werte: 0 bis 3</u>	
<u>description</u>	<u>Frei verwendbares Feld</u>	
gvStatus	Objekt im LDAP gültig ( <i>active</i> oder <i>inactive</i> )	M
gvSource	<u>ID- und Zeitstempel des Benutzers, der die Transaktion veranlasst hat. Die Zeit wird sekundengenau eingetragen. ISO 8601 erlaubt Füllzeichen zur besseren Lesbarkeit:</u>	M

Gelöscht: , dn

Gelöscht: MA14, ou=OrgUnits, dc=magwien, dc=gv, dc=at

	<p><u>yyyy-mm-ddThh:mm:ssZ</u></p> <p><u>Z steht für die Zeitzone UTC, T trennt Datum und Zeit.</u></p> <p><u>Format: User-DN/Datum-Zeit; Zeitzone=UTC</u>  <u>(gvGid=AT:b:0:81ae1f3f6db30976a029d2b2da5e166ba0d508b,</u>  <u>ou=people, gvOuld=AT:b:4711,</u>  <u>dc=gv,dc=at/2003-05-15T12:00:01)</u></p>	
gvScope	Zugriffsstufe (public, gv.at, local)	M

- Gelöscht:** GID/OrgDomain
- Gelöscht:** AT543219876543/bmf.gv.at/2001-02-01
- Gelöscht:** 19:22:01

- Der Inhalt des Attributs gvGid ist der Präfix ‚AT:B:0:‘ und die aus der ZMR-Zahl über Einwegverschlüsselung abgeleitete VPK (verfahrensspezifische Personenkenung PERSONAL[2]). Als Übergangsregelung können auch andere Identifier aus gvOtherId verwendet werden.
- gvOtherId: Liste von Personenkennzeichen im Format Owner:System:Id, wobei Owner die Organisation ist, die das System verwaltet. System ist das Kennzeichensystem und Id ist der innerhalb des Systems eindeutige Schlüssel. Owner ist identisch mit dem Owner der Org-ID im Dokument Verwaltungskennzeichen [3]. System wird vom jeweiligen Owner verwaltet.
- Weitere optionale und im Arbeitskreis nicht besprochene Attribute sind im [RFC 2798](#) definiert
- 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.

**Gelöscht:** Verfahrenskennung. Die Ableitungsfunktion wird im Projekt Bürgerkarte definiert.

<b>gvPersonFunction</b>		Funktionen einer Person, um unterschiedliche Anwendungsrechte abzubilden
<p>dn: gvFunction=..., gvGid=..., ou=People, dc=...</p> <p>(dn: gvFunction=JD,gvGid=AT:b:0:81ae1f3f6db30976a029d2b2da5e166ba0d508b,ou=People,dc=bmi+gvOuld=AT:b:4711,dc=gv,dc=at)</p>		
Attribut	Beschreibung (Beispiel)	Eigen schaft
gvFunction	Kurze Funktionsbezeichnung (JD)	M
description	Funktionsbezeichnung (Journaldienst)	
gvOul <u>d</u>	<u>gvOuld der</u> Organisationseinheit, zu der die Person in dieser Funktion zugeteilt ist. <u>Der Wert muss auch in gvOu in gvOrPerson</u> enthalten sein. (gvOuld=AT:19:9876)	dn
gvRights	Wie gvOrgPerson	L, dn
gvStatus	Wie gvOrgPerson	M

- Gelöscht:** AT471131026100
- Gelöscht:** Pointer auf die
- Gelöscht:** L,
- Gelöscht:** Das Attribut erlaubt mehrfache Werte, in diesem Objekt darf jedoch nur ein
- Gelöscht:** MA14
- Gelöscht:** , ou=OrgUnits, , dc=gv, dc=at

gvSource	Wie gvOrgPerson	M
gvScope	Wie gvOrgPerson	M

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

<b>gvOrgUnit</b> <u>1.2.40.0.10.2.1.0.2</u>	<u>1. Organisationseinheit</u> <u>2. Organisation</u> <u>gvOrgUnit wird von OrganizationalUnit abgeleitet</u>		
dn : gvOuld=..., ou=OrgUnits,dc=... (dn: gvOuld= <u>AT:b:9876</u> , ou=OrgUnits,dc=bmi+gvOuld= <u>AT:b:4711</u> ,dc=gv,dc=at)			
<b>Attribut</b>	<b>Beschreibung (Beispiel)</b>	<b>Eigen schaft</b>	<b>OID</b>
gvOuld	<u>internes Verwaltungskennzeichen (AT + Org-ID)</u> <i>(AT:19:9876)</i>	M	
ou	<u>Vewaltungskennzeichen</u> Kurzbezeichnung der Organisationseinheit <i>(IV/2-e)</i>	M	
<u>gvOuldParent</u>	<u>Übergeordnete OE; Wert: gvOuld der übergeordneten OEs (kein dn!)</u>		
cn	Bezeichnung der Organisationseinheit (ausgeschrieben) <i>(Abt. ITMS/Ref. NIK Referat nationale und internationale Koordination)</i>	M, L	
mail	RFC822 E-Mail Adresse <i>(helplessdesk@xyz.gv.at)</i>		
telephoneNumber	Tel-Nummer	L, tel	
facsimileTelephone Number	Fax-Nummer	L, tel	
street	(Postadresse, nicht Standortadresse)		
city	Ort <i>(Wien)</i>		
postalAddress	Wie gvOrgPerson		
postalCode	Wie gvOrgPerson		
<u>c</u>	<u>Wie gvOrgPerson</u>		

Gelöscht: B28

Gelöscht: 1.3.18.0.2.4.705

<u>co</u> <u>friendlyCountryName</u>	<u>Wie gvOrgPerson</u>		
gvPhysicalAddress	Wie gvOrgPerson		
<u>gvImageRef</u>	<u>Verwendung + Referenz auf Bilder im Format</u> <u>{Verwendung} URI</u> <u>Standardverwendungen sind Logo, Zugang</u> <u>und Zufahrt, die Liste kann erweitert werden;</u> <u>z.B.:</u> <u>{logo} http://www.xyz.gv.at/logo1.jpg</u> <u>{Zugang}http://www.xyz.gv.at/zugang.jpg</u>	<u>L</u>	
gvWebAddress	URL der Homepage		
<u>description</u>	<u>Frei verwendbares Feld</u>		
<u>gvLegalSuccessor</u>	<u>gvOuid der Organisation oder OE, die die</u> <u>unmittelbare Rechtsnachfolge antrat.</u> <u>Wenn die Organisation ohne Rechtsnachfolge</u> <u>aufgelöst wurde, ist der Wert „none“.</u> <u>Besteht die OE noch (gvStatus = active), ist</u> <u>dieses Attribut leer</u>		
gvStatus	Wie gvOrgPerson	M	<a href="#">1.2.40.0.1</a> <a href="#">0.2.1.1.15</a>
gvSource	Wie gvOrgPerson	M	<a href="#">1.2.40.0.1</a> <a href="#">0.2.1.1.17</a>
gvScope	Zugriffsstufen ( <i>public, gv.at, local</i> )	M	<a href="#">1.2.40.0.1</a> <a href="#">0.2.1.1.19</a>
...	Weitere optionale Attribute sind im RFC 2256 definiert		

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

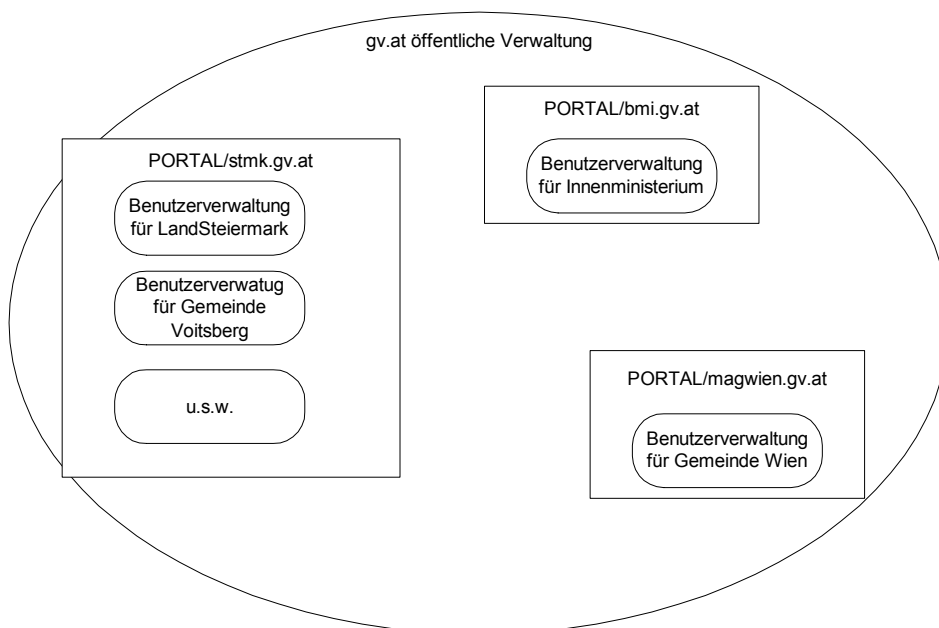
<b>OrganizationalUnit</b>	OID: 2.5.6.5 Knoten zur Definition von Namensräumen unterhalb des Domain-Eintrags		
dn : ou=..., dc=... (dn: ou=People, dc=bmi+ <a href="#">gvOuid=AT:b:4711</a> ,dc=gv,dc=at)			
<b>Attribut</b>	<b>Beschreibung (Beispiel)</b>	<b>Eigenschaft</b>	<b>OID</b>
ou	Namespace ( <i>People</i> )	M	

## LDAP-Klassen TEIL 2

### Einführung

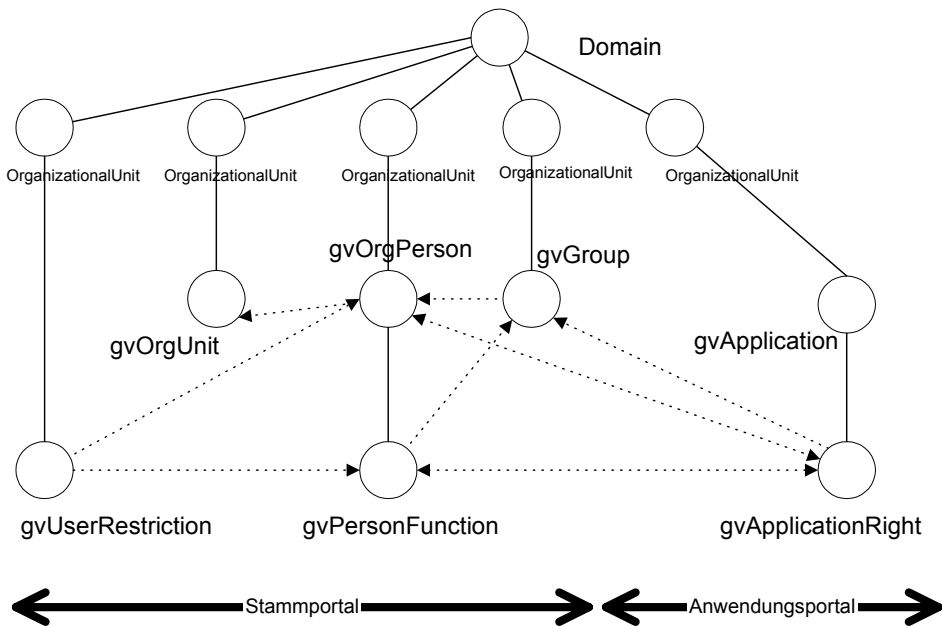
Zweck dieses Schemas ist die Definition einer externen LDAP-Sicht auf Daten von Benutzerverwaltungssystemen, welche die Kooperation von Web-Portalen mit delegierter Benutzerverwaltung, einheitlicher Menüführung, Single Sign-On und Revision nach dem Datenschutzgesetz ermöglicht. Die Quelle dieser Daten kann eine interne LDAP-Struktur oder ein RDBMS sein. Das Verzeichnis ist zwar nicht zur Verwaltung der Einträge gedacht oder optimiert, sondern für die Präsentation der für ein Portal relevanten Informationen (Benutzer, Anwendungen, Rechte). Allerdings soll das derzeitige Konzept zukünftigen Anwendungen den schreibenden Zugriff auf die Daten ermöglichen. Die Verbindung zwischen interner Benutzerverwaltung und LDAP sollte synchron sein.

Die hier betrachtete Benutzerdomäne ist beispielhaft wie folgt strukturiert.



Jede Organisation hat nur im lokalen (eigenen) Directory-Teil schreibenden Zugriff. Änderungen des Schemas für neue Anwendungen sind nur notwendig, wenn Anwendungen neue Anforderungen haben, die eine Ergänzung des globalen Modells benötigen.

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



- Gruppen können wiederum Gruppen enthalten. Die Auflösung der Rechte funktioniert so, dass die Verweise so lange aufgelöst werden, bis nur mehr Objekte der Klassen gvOrgPerson oder gvPersonFunction vorhanden sind.

## Delegation

Die Datenstruktur ist so flexibel gestaltet, dass verschiedenen Objekten Anwendungsrechte gewährt werden können (siehe Attribute „member“ in gvApplicationRight, und gvRights in gvOrgPerson).

Allerdings SOLLTE folgender Ablauf eingehalten werden:

1. Die zugriffsberechtigte Stelle gibt dem Anwendungsverantwortlichen ein Objekt gvGroup bekannt.
2. Dieses Objekt gvGroup wird vom Anwendungsverantwortlichen berechtigt, indem sein dn in uniqueMember für jedes zutreffende gvApplicationRight eingetragen wird.
3. Der Benutzeradministrator delegiert die Anwendungsrechte, indem er andere Gruppen, Benutzer oder Organisationseinheiten in die Gruppe einträgt. Damit stimmt dieser Ablauf auch mit den rechtlichen und organisatorischen Zuständigkeiten überein.
4. Mit dieser Berechtigung kann ein Anwender-Administrator, der Delegationsrechte für ein Gruppenobjekt besitzt, Rechte weitergeben, ohne selbst implizit Rechte an der Anwendung zu besitzen.
5. Aus technischen Gründen werden im LDAP-Schema Back-Pointer bei den Benutzern (gvOrgPerson) geführt, die sämtliche Anwendungsrechte der Person beinhalten. Dadurch wird die Suche in einer verteilten Umgebung wesentlich vereinfacht. Prinzipiell kommt für die Erzeugung der Back-Pointer sowohl ein Push- als auch Pull-Prinzip in Frage. Damit die Daten weitgehend synchron sind und die Netzwerklast gering gehalten wird, ist das Push-Prinzip vorzuziehen. Aus diesem Grund ist noch ein Protokoll zu definieren, mit dem Erteilung und Entzug von Rechten vom Anwendungsbetreiber dem Benutzer-Verwalter mitgeteilt wird.

<b>gvApplication</b>	Anwendung		
dn: gvApplId=..., ou=Applications, dc=... (dn: gvApplId=ZMR, ou=Applications, dc=bmi+gvOuid=AT:b:4711, dc=gv, dc=at)			
Attribut	Beschreibung (Beispiel)	Eigen-schaft	OID
gvApplId	Eindeutig Anwendungskennung (ZMR)	M	
cn	Name der Anwendung (Zentrales Melderegister)	M, <u>L</u>	
gvURL	Anwendungsadresse <u>im Stammportal</u> ( <a href="https://portal.ooe.gv.at/bmi.gv.at/eka">https://portal.ooe.gv.at/bmi.gv.at/eka</a> )		
<u>gvPortalTargetPrefix</u>	<u>Zieladresse am Anwendungsportal (für Reverse Proxy)</u> ( <a href="https://portal.bmi.gv.at/bmi.gv.at/eka">https://portal.bmi.gv.at/bmi.gv.at/eka</a> )		
description	Anwendungsbeschreibung		
gvSecClass	0 bis 3 (Default – wird durch <a href="#">gvApplicationRight</a> übersteuert)	M	
<u>gvSessionTimeout</u>	<u>Timeout in Sekunden für interaktive Benutzer-Sessions; Wird vom Stammportal im Portalverbund ausgewertet</u>	<u>int</u>	
gvBanner	Nachricht für den Benutzer, wird angezeigt, wenn die Anwendung "inactive" ist und der Benutzer über das Menü verzweigt.		
gvAppOwner	Anwendungsverantwortlicher	dn	
gvAppTechContact	technischer Kontakt	dn	
gvAppAdmin	administrativer Kontakt	dn	
gvStatus	Wie gvOrgPerson	M	<a href="#">1.2.40.0.1.0.2.1.1.15</a>
gvSource	Wie gvOrgPerson	M	<a href="#">1.2.40.0.1.0.2.1.1.17</a>
gvScope	Wie gvOrgPerson	M	<a href="#">1.2.40.0.1.0.2.1.1.19</a>

<b>gvApplicationRight</b>	Rechte und deren Parameter für Objekte der Klassen gvPerson, gvGroup, gvPersonFunction		
dn: cn=..., gvApplId=..., ou=Applications, dc=... (cn=ZMR-Anfrage, gvApplId=ZMR, dc=bmi+gvOuld=AT:b:4711, dc=gv, dc=at)			
Attribut	Beschreibung (Beispiel)	Eigen-schaft	OID
gvApplId	Wie in gvApplication	M	
cn	Bezeichnung der Berechtigung	M, L	
<u>unique</u> Member	Berechtigte Objekte wie gvGroup, gvOrgPerson, <u>gvPersonFunction</u> , gvOrgUnit, cn=gruppe13, gvApplId=wibis, ou=Applications, dc=magwien+gvOuld=AT:19:1508, dc=gv, dc=at	L, dn	2.5.4.31
gvSecClass	0 bis 3		
description			
gvStatus	Wie gvOrgPerson	M	<a href="#">1.2.40.0.1.0.2.1.1.15</a>
gvSource	Wie gvOrgPerson	M	<a href="#">1.2.40.0.1.0.2.1.1.17</a>
gvScope	Wie gvOrgPerson	M	<a href="#">1.2.40.0.1.0.2.1.1.19</a>

<b>gvGroup</b>	Liste von Benutzern und anderen Gruppen, die Organisationsstrukturen oder Funktionen abbilden		
dn: cn=..., ou=Groups, dc=... (cn=gruppe13, ou=Groups dc=magwien+gvOuld=AT:19:1508, dc=gv, dc=at)			
Attribut	Beschreibung (Beispiel)	Eigen-schaft	OID
cn	Name dieser Gruppe	M, <u>L</u>	
<u>unique</u> Member	Liste von Objekten der Klassen gvOrgPerson, gvPersonFunction, <u>gvOrgUnit</u> und gvGroup (cn=gruppe13, ou=Groups, dc=magwien+gvOuld=AT:19:1508, dc=gv, dc=at gvGid=AT81ae1f3f6db30976a029d2b2da5e166ba0d508b, ou=People, dc=magwien+gvOuld=AT:19:1508, dc=gv, dc=at)	L, dn	
gvStatus	Wie gvOrgPerson	M	<a href="#">1.2.40.0.1.0.2.1.1.15</a>
gvSource	Wie gvOrgPerson	M	<a href="#">1.2.40.0.1.0.2.1.1.17</a>

Gelöscht: M,

Gelöscht: AT543219876543

gvScope	Wie gvOrgPerson	M	<a href="#">1.2.40.0.1</a> <a href="#">0.2.1.1.19</a>
---------	-----------------	---	--

<b>gvUserRestriction</b>	Restriktionen eines Benutzers		
dn: gvApplId=... + cn=..., ou=Restrictions, dc=... (gvApplId=ZMR + cn=restr21576,ou=Restrictions,dc=bmi+gvOuid=AT:b:4711,dc=gv,dc=at)			
Attribut	Beschreibung (Beispiel)	Eigen-schaft	OID
cn	Bezeichnung der Restriktion oder lfd Nr.	M, L	
gvApplId	Wie in gvApplication	M	
gvRights	dn des betroffenen gvApplicationRight	M, L, dn	
<a href="#">unique</a> Member	dn von gvOrgPerson, gvPersonFunction, <a href="#">gvOrgUnit</a> oder gvGroup cn=gruppe13, ou=gvGroup <del>dc=magwien+gvOuid=AT:19:1508,dc=gv,dc=at</del>	L, dn	2.5.4.31
description	Platz für Vermerk des Rechtheverwalters zur Restriktion		
gvRegionalRestriction	Liste von anwendungsspezifischen Regionsbezeichnungen, für die eine Berechtigung besteht. <b>Regionsbezeichnungen für Anwendungen des BMI sind:</b>  - Organisationseinheiten, GemeindeKZ, Bundesländer (B, K, N, O, S, St, T, V, W, X=Ausland), <b>Formate:</b> DST=A23/bmi.gv.at GKZ=10234 BL=W	L	
gvStatus	Wie gvOrgPerson	M	<a href="#">1.2.40.0.1</a> <a href="#">0.2.1.1.15</a>
gvSource	Wie gvOrgPerson	M	<a href="#">1.2.40.0.1</a> <a href="#">0.2.1.1.17</a>
gvScope	Zugriffsstufen (public, gv.at, local)	M	<a href="#">1.2.40.0.1</a> <a href="#">0.2.1.1.19</a>

Gelöscht: dc=magwien

- Die Bezeichnung *Restriktion* wurde für dieses Objekt gewählt, weil viele Anwendungen keine Einschränkungen dieser Art kennen, andere aber grundsätzlich keine Zugriffe erlauben außer den in gvUserRestrictions angeführten Bereichen. Aus der Sicht des Benutzers ist es eigentlich eine Berechtigung und keine Einschränkung.
- Für weitere Restriktionen werden zusätzliche Attribute und Werteschlüssel definiert.

## LDAP-Schema in formaler Syntax

### Attribute

Match: = bedeutet EQUALITY, sub SUBSTRING, cim CaseInsensitiveMatch, dnm DistinguishedNameMatch, cem CaseExactMatch, int IntegerMatch

<u>OID</u>	<u>Name</u>	<u>Syntax</u>	<u>Match</u>
<a href="#">1.3.18.0.2.4.705</a>	<a href="#">city</a>	<a href="#">Directory String</a>	<a href="#">= cim, sub cim</a>
<a href="#">1.2.40.0.10.2.1.1.11</a>	<a href="#">gvAmtstitel</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.23</a>	<a href="#">gvAppAdmin</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.25</a>	<a href="#">gvAppId</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.27</a>	<a href="#">gvAppOwner</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.29</a>	<a href="#">gvAppTechContact</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.31</a>	<a href="#">gvBanner</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.33</a>	<a href="#">gvFunction</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.1</a>	<a href="#">gvGid</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.35</a>	<a href="#">gvImageRef</a>	<a href="#">Directory String</a>	<a href="#">= cem</a>
<a href="#">1.2.40.0.10.2.1.1.37</a>	<a href="#">gvOtherId</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.5</a>	<a href="#">gvOu</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.3</a>	<a href="#">gvOuid</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.39</a>	<a href="#">gvOuidParent</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.41</a>	<a href="#">gvOulist</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.9</a>	<a href="#">gvPhysicalAddress</a>	<a href="#">Directory String</a>	<a href="#">= cim; sub cim</a>
<a href="#">1.2.40.0.10.2.1.1.21</a>	<a href="#">gvRights</a>	<a href="#">DN</a>	<a href="#">= dnm</a>
<a href="#">1.2.40.0.10.2.1.1.19</a>	<a href="#">gvScope</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.43</a>	<a href="#">gvSecClass</a>	<a href="#">Integer{1}</a>	<a href="#">= int</a>
<a href="#">1.2.40.0.10.2.1.1.45</a>	<a href="#">gvSessionTimeout</a>	<a href="#">Integer{5}</a>	<a href="#">= int</a>
<a href="#">1.2.40.0.10.2.1.1.13</a>	<a href="#">gvSex</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.17</a>	<a href="#">gvSource</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.15</a>	<a href="#">gvStatus</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>
<a href="#">1.2.40.0.10.2.1.1.47</a>	<a href="#">gvTargetPrefix</a>	<a href="#">Directory String</a>	<a href="#">= cem</a>
<a href="#">1.2.40.0.10.2.1.1.49</a>	<a href="#">gvUrl</a>	<a href="#">Directory String</a>	<a href="#">= cem</a>
<a href="#">1.2.40.0.10.2.1.1.51</a>	<a href="#">gvWebAddress</a>	<a href="#">Directory String</a>	<a href="#">= cem</a>
<a href="#">1.2.40.0.10.2.1.1.53</a>	<a href="#">gvLegalSuccessor</a>	<a href="#">Directory String</a>	<a href="#">= cim</a>

## Objektklassen

gvApplication <a href="#">1.2.40.0.10.2.1.0.3</a>	SUP top STRUCTURAL MUST ( gvSecClass \$ cn \$ gvApplId \$ gvStatus \$ gvSource \$ gvScope ) MAY ( gvUrl \$ <a href="#">gvTargetPrefix</a> \$ gvAppAdmin \$ gvBanner \$ description \$ gvAppTechContact \$ gvAppOwner )
gvApplicationRight <a href="#">1.2.40.0.10.2.1.0.4</a>	SUP top STRUCTURAL MUST ( gvApplId \$ gvScope \$ cn \$ gvSource \$ gvStatus ) MAY ( uniqueMember \$ gvSecClass \$ description )
gvGroup <a href="#">1.2.40.0.10.2.1.0.5</a>	SUP top STRUCTURAL MUST ( gvScope \$ cn \$ uniqueMember \$ gvSource \$ gvStatus )
gvUserRestriction <a href="#">1.2.40.0.10.2.1.0.6</a>	SUP top STRUCTURAL MUST ( cn \$ gvApplId \$ gvStatus \$ gvSource \$ gvRights \$ gvScope ) MAY ( uniqueMember \$ gvRegionalRestriction \$ description )
<a href="#">gvOrganisation</a> <a href="#">1.2.40.0.10.2.1.0.7</a>	SUP gvOrgUnit STRUCTURAL MUST ( dc \$ o )
gvOrgPerson 1.2.40.0.10.2.1.0.1	SUP inetOrgPerson STRUCTURAL MUST ( gvGid \$ gvScope \$ gvSource \$ gvStatus ) MAY ( gvOtherId \$ gvSex \$ gvRights \$ gvAmtstitel \$ gvOu \$ gvSecClass \$ gvPhysicalAddress )
gvOrgUnit <a href="#">1.2.40.0.10.2.1.0.2</a>	SUP organizationalUnit STRUCTURAL MUST ( gvOuId \$ gvScope \$ cn \$ gvSource \$ gvStatus ) MAY ( gvOuIdParent \$ city \$ gvImageRef )
gvPersonFunction <a href="#">1.2.40.0.10.2.1.0.8</a>	SUP top STRUCTURAL MUST ( gvScope \$ gvSource \$ gvFunction \$ gvStatus ) MAY ( gvRights \$ gvOuId \$ description )

## Beispielbaum

```
dc=at
  dc=gv
    dc=bmi + gvOuid=AT:b:4711
      ou=Applications
        gvApplId=ZMR
          cn=ZMR-Query
            cn=Meldebehörde
      ou=Groups
        cn=Firmenbuchabfrage
      ou=OrgUnits
        gvOuid=AT:b:98761
        gvOuid=AT:b:98777
      ou=People
        gvGid=B:8:81ae1f3f6db30976a029d2b2da5e166ba0d508b
        gvGid=B:8:f3f608bdb30976a029d2b81ae12da5e166ba0d5
          gvFunction=Referatsleiter EDVZ
          gvFunction=Betriebsrat
      ou=Restrictions
        gvApplId=ZMR+cn=restr21576
    ...
  dc=magwien + gvOuid=AT:l9:1508
    ou=Applications
    ou=Groups
    ou=OrgUnits
    ou=People
      gvGid=B:8:6a029d2b81ae12da5e3097a0d5166bf3f608bdb
```

## Referenzen

- [1] AG Autorisierungsverfahren: Begriffsdefinitionen Portalverbund:  
[http://reference.e-government.gv.at PV-Begriffe.doc](http://reference.e-government.gv.at/PV-Begriffe.doc)
- [2] AGV §13 (4a) Zum Zweck der eindeutigen Identifikation von Verfahrensbeteiligten im elektronischen Verkehr mit der Behörde darf diese die ZMR-Zahl ... als Ausgangsbasis für eine verwaltungsbereichsspezifisch unterschiedliche, abgeleitete und verschlüsselte Personenkennzeichnung verwenden.
- [3] Grandits, Franz: Verwaltungskennzeichen:  
[http://reference.e-government.gv.at. Dokument VKZ 1.1.0 \(Entwurf vom 15.5.2003\)](http://reference.e-government.gv.at/Dokument/VKZ_1.1.0_(Entwurf_vom_15.5.2003))
- [4] Hörbe, Rainer: Sicherheitsklassen im Portalverbundsystem.  
[http://reference.e-government.gv.at SecClass 1.0.0](http://reference.e-government.gv.at/SecClass_1.0.0)
- [5] RFC 2256: A Summary of the X.500(96) User Schema for Use with LDAPv3
- [6] RFC 1798: Definition of the inetOrgPerson LDAP Object Class
- [7] [Post AG, "Richtig Adressieren"](http://www.business.post.at/content/pdf/RichtigAdressieren_WWW1.pdf)  
[http://www.business.post.at/content/pdf/RichtigAdressieren\\_WWW1.pdf](http://www.business.post.at/content/pdf/RichtigAdressieren_WWW1.pdf)

## **Zusammenfassung der Änderungen seit Version 2.0.2**

(Detaillierte Änderungen sind im Dokument Struktur „LDAP-gvat2\_1-aend“  
beschrieben.

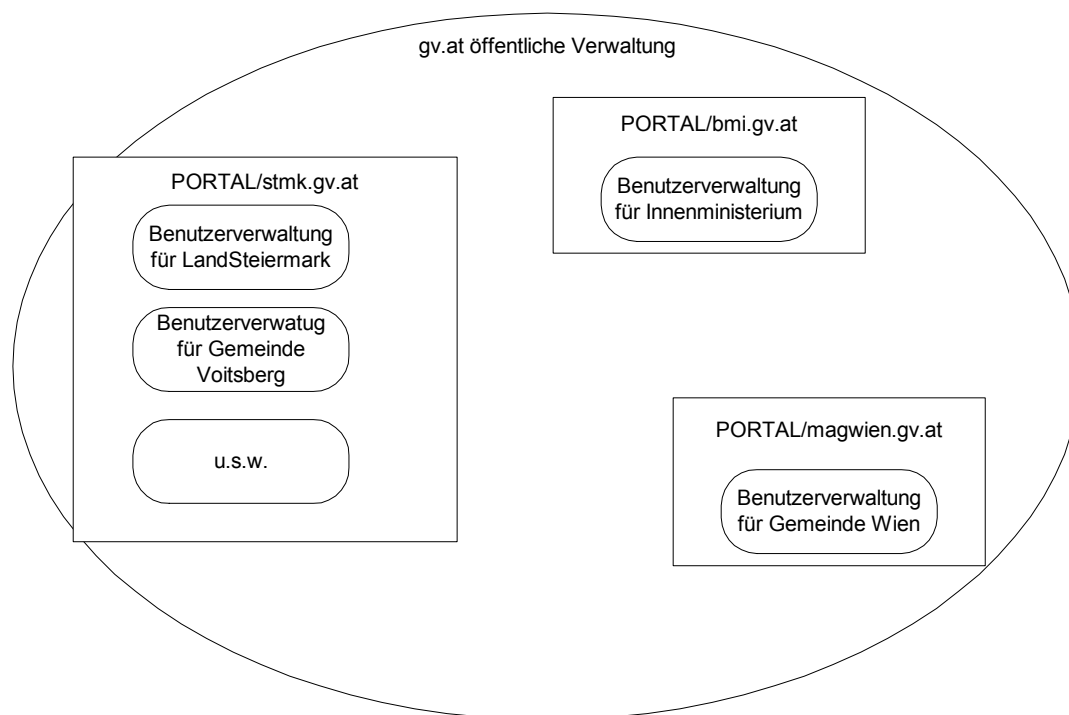
1. Geänderte Einleitung, da das Verzeichnis nicht nur für Berechtigungssysteme,  
sondern auch als Basisdienst des e-Government verwendet wird.
2. Geänderte Darstellung der Aufbauorganisation (siehe Seite 2)
3. Verwendung der Org-ID (des internen, numerischen Verwaltungskennzeichens)  
für die Bildung des DN's von Organisationen und Organisationseinheiten. (Siehe  
Seite 2: Directory Information Tree)
4. Zusätzlich zur gvGid können auch andere eindeutige Kennzeichen in gvOtherId  
geführt werden, um die Synchronisation mit Anwendungen, die keine gvGid  
kennen, zu erleichtern.
5. Zusätzliche Attribute bei gvOrgPerson (gvOtherID, Besuchsadresse, Mobiltelefon,  
Zimmernummer, Land, gvSecClass)
6. Zusätzliche Attribute bei gvOrgunit (Besuchsadresse, Land, Webadresse, Bilder  
für Logo und Zufahrtsplan)
7. Exaktere Definition von Attributwerten (z.B. postalAddress).
8. Vereinheitlichung der Begriffe mit den Dokumenten des Portalverbundsystems.
9. Klärung der Zugriffssteuerung auf der Ebene der Attributwerte (Seite 4), z.B.  
welche E-Mailadressen oder Telefonnummern öffentlich angezeigt werden.
10. Organisationen werden durch Einträge der Klasse gvOrganization abgebildet  
(bisher organization).
11. Das Attribut gvLegalSuccessor wird dafür verwendet, Rechtsnachfolger für  
Organisationen und Organisationseinheiten festzulegen.

## Einführung

Zweck dieses Schemas ist die Definition einer externen LDAP-Sicht auf Daten von Benutzerverwaltungssystemen, welche die Kooperation von Web-Portalen mit delegierter Benutzerverwaltung, einheitlicher Menüführung, Single Sign-On und Revision nach dem Datenschutzgesetz ermöglicht. Die Quelle dieser Daten kann eine interne LDAP-Struktur oder ein RDBMS sein. Das Verzeichnis ist zwar nicht zur Verwaltung der Einträge gedacht oder optimiert, sondern für die Präsentation der für ein Portal relevanten Informationen (Benutzer, Applikationen, Rechte). Allerdings soll das derzeitige Konzept zukünftigen Applikationen den schreibenden Zugriff auf die Daten ermöglichen. Die Verbindung zwischen interner Benutzerverwaltung und LDAP sollte synchron sein.

In diesem Schema sind interne Objekte und Attribute des Portals nicht berücksichtigt, wie etwa Daten zur Login-Verwaltung, Authentifikation über X.509-Zertifikate oder Trust-Beziehungen zu Fremdportalen.

Die hier betrachtete Benutzerdomäne ist beispielhaft wie folgt strukturiert.



Organisation	Organisation der öffentlichen Verwaltung, welche für in ihrer Ressourcenverwaltung sowie der internen Organisation eigenständig ist (z.B. Ministerium, Land, Gemeinde)
Applikation	IT-System, welches die Erledigung einer speziellen Aufgabe der öffentlichen Verwaltung unterstützt (z.B. Wohnbauförderung)
Personal führende Organisation	Organisation, welche in ihrem Bereich Personalentscheidungen trifft und Personal verwaltet. Wird sich in den meisten Fällen mit 1. decken
Organisationseinheit	Organisatorische Einheit innerhalb einer Organisation, welche die Aufgabenteilung zu den einzelnen Bediensteten eigenständig vornimmt

Bediensteter	Person, welche Aufgaben der öffentlichen Verwaltung im organisatorischen Kontext einer Organisation oder einer Organisationseinheit durchführt.
Funktion	Arbeitskontext einer Person, der mit spezifischen Berechtigungen verbunden ist. Z.B. Wachbeamter (Funktion A) hat Journaldienst (Funktion B mit erweiterten Berechtigungen)
Directorybetreiber	Betreiber eines Verzeichnisdienstes für eine oder mehrere personalführende Organisationen und/oder einen oder mehrere Anwendungseigner
Anwendungseigner	auftraggebende Organisation laut Datenschutzgesetz
Anwendungsverwalter	Verwaltet Anwendungsrechte einer bestimmten Anwendung und gibt diese an eine Organisation oder eine Organisationseinheit bzw. direkt an einzelnen Bedienstete weiter
Benutzerverwalter	Verwaltet Daten von Bediensteten und Organisationseinheiten innerhalb einer Organisation
Anwendungsrechte	Rechte innerhalb einer Anwendung. Dieses Recht bildet eine spezielle Teilaufgabe innerhalb einer Anwendung ab
Rechteverwalter	Vergibt Anwendungsrechte einer Organisationseinheit an konkrete Bedienstete