

<h1>Spezifikation LDAP-gv.at</h1>		Konvention
		LDAP-gv.at 2.5.1
		Ergebnis der Arbeitsgruppe
Kurzbeschreibung	Spezifikation des LDAP-Schemas für den zentralen Verzeichnisdienst der Verwaltung. LDAP-gv.at definiert die Objekte zur Darstellung von Personen, Dienstverhältnissen und Funktionen sowie der Aufbauorganisation in elektronischen Behördenverzeichnissen.	
Autor(en):	Harald Hahn (LFRZ)	Projektteam / Arbeitsgruppe
		AG Integration und Zugänge (AG-IZ) AG-Leitung: Ing. Dipl.-Ing.(FH) Hannes Wittmann, MSc (Mag. Wien) Stellvertretung: Dipl.-Ing. Dominik Klauser, BSc (BKA)
Beiträge von:	Harald Stradal (BM.I), Hildegard Freidl (STMK), Markus Frühwirth (HVB), Harald Hahn, Peter Pichler, Gerold Pesendorfer (LFRZ), Peter Reichstädter (BKA)	

Version 2.0.1: 01.02.2002	Fristablauf: 08.03.2002
Unterversion 2.1.0: 01.02.2002	Fristablauf: 26.06.2003
Unterversion 2.3.0: 21.02.2006	Fristablauf: 20.3.2006
Unterversion 2.4.0: 22.05.2009	Fristablauf: 13.7.2009
Unterversion 2.5.0: 28.03.2012	Fristablauf: 25.5.2012
Unterversion 2.5.1: 22.12.2017	Fristablauf: - (Länderangabe bei ablehnender Stellungnahme)

Inhalt

1	Dokumentstruktur	3
2	LDAP-Modell (allgemein).....	3
2.1	Abgrenzung	3
2.2	Directory Information Tree (DIT)	3
2.3	Abbildung der Aufbauorganisation.....	3
2.4	Klassen- und Attributbeschreibung	4
2.5	Allgemeine Attribute	5
2.6	Zugriffssteuerung	5
3	LDAP-Klassen.....	6
4	Referenzen	14
5	Historie	15

1 Dokumentstruktur

Dieses Dokument beschreibt das LDAP-Schema von ldap.gv.at und definiert die Objekte zur Darstellung von Personen, Aufbauorganisation, Kontakten, Adressbuch, etc. Das Schema wurde für die Implementierung des Portalverbundprotokolls um Objektklassen für Benutzerverwaltungs- und Berechtigungssysteme erweitert und im Dokument „LDAP-gv.at_PV 1.0.0“ separat veröffentlicht. Für das elektronische Behördenverzeichnis des Bundes wurde für die spezifischen Erweiterungen zum Standardschema ein zusätzliches Best Practice Dokument „BV Bund 1.0.0“ erstellt und unter www.ref.gv.at veröffentlicht.

2 LDAP-Modell (allgemein)

2.1 Abgrenzung

Im ldap.gv.at-Verzeichnis werden Objekte der österreichischen Verwaltung geführt. Mit **gvOrganisation** werden eigenständige Verwaltungseinheiten dargestellt, wie Gemeinden, Länder, Ministerien, Selbstverwaltungskörper etc. Ihre Geschäftseinteilung wird mit Objekten der Klasse **gvOrgUnit** abgebildet. Die Personeneinträge der Klasse **gvOrgPerson** sind Dienstverhältnisse also Mitarbeiter im weiteren Sinne, einschließlich Wartungspersonal von Dienstleistern oder freie Mitarbeiter. Einträge für Funktionen (**gvPersonFunction**) können bei Bedarf mehrfache Dienstzuordnungen abbilden.

2.2 Directory Information Tree (DIT)

- Der LDAP Verzeichnisdienst ist als verteilter Dienst mit gemeinsamen DIT-Wurzel-Objekt (Klasse Domain, **[RFC2251]**), welches den **DN** (Distinguished Name) dc=at führt, konzipiert.
- Unter dem Wurzel-Objekt sind die Domainobjekte mit dem DN dc=at“, „dc=local“ etc. angeordnet. Objekte unter dc=at können über LDAP.gv.at synchronisiert werden. Objekte unter dc=local bleiben im lokalen Verzeichnis.
- Unterhalb der Domain-Objekte sind die Wurzelknoten von Organisationen. Jede Personal führende Organisation, an die vom Anwendungsverantwortlichen Rechte delegiert werden, hat einen eigenen Eintrag der Klasse **gvOrganisation** für ihren Teilbaum.
- Parallel zur Hierarchie der Domain Components, die den Internet-Domänen folgen, soll die Org-ID (internes Verwaltungskennzeichen [VKZ]) als Alternative verwendet werden. Besonders in der Bundesverwaltung, wo Domänen oft kurzlebig sind, ist diese zusätzliche Adressierung sinnvoll.
- 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.

2.3 Abbildung der Aufbauorganisation

Die Aufbauorganisation entsprechend der Geschäftseinteilung, wird unterhalb des Container-Objekts mittels der Objektklasse **gvOrgUnits** abgebildet. Die Hierarchie im Objekt gvOrgUnit wird durch das Attribut **gvOuIdParent** definiert, womit der DN gleich bleibt, wenn sich die übergeordnete Hierarchie ändert.

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

2.4 Klassen- und Attributbeschreibung

In Kapitel 3 werden die einzelnen Objektklassen detailliert beschrieben. Die jeweiligen Attribute und Eigenschaften werden durch folgende Beschreibungskürzel definiert:

2.4.1 Kardinalität des Attributes

leer (default): optional

M: mandatory (Pflichtfeld)

2.4.2 Einzelwert/Liste

S: single-valued

L (default): multi-valued

Die LDAP RFCs definieren Attribute typischerweise als Listenattribute (z.B. cn, ou, dc,..). Es wird generell empfohlen bei der Befüllung darauf zu achten, dass die Verwendung von mehreren Werten problematisch sein kann (z.B. bei Bezeichnung (cn) einer gvOrgUnit).

2.4.3 Leere Attribute

Attribute ohne Werte entsprechen NULL und scheinen im LDAP nicht auf.

2.4.4 Type (Syntax, Matching)

- leer bedeutet das gleiche wie cis
- bin binary
- cis Directory String (UTF8),
Matching: Case Insensitive
- ces Directory String (UTF8),
Matching Case Exact String
- dn Distinguished Name
- ia5 IA5-String (auch ISO 646 oder US-ASCII bezeichnet)
- int Integer
- jpeg JPEG Bild
- tel Telephone Number
- uri PrintableString; Matching: Case Exact String

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

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

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

2.5 Allgemeine Attribute

2.5.1 Server-maintained 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

2.5.2 Custom Attribute

Die folgenden Felder MÜSSEN in Objekten der Klassen gvOrgPerson, gvPersonFunction und gvOrgUnit enthalten sein. Sie werden im Folgenden gesammelt dargestellt und in den einzelnen Objektklassen nicht mehr angeführt:

- **gvStatus:** Objekt im LDAP gültig, MUSS-Feld, cis(32), Werte: ‚active‘ oder ‚inactive‘.
- **gvSource:** MUSS-Feld für ID- und Zeitstempel des Benutzers, der die Änderung veranlasst hat. Dient zur Anzeige, nicht zur maschinellen Verarbeitung, da Benutzerkennungen nicht immer direkt lesbar sind (z.B. bei Portalbenutzern). Welche Benutzerkennung verwendet wird spezifiziert die verantwortliche Organisation (UID oder DN). Die Zeit wird sekundengenau eingetragen. ISO 8601 erlaubt Füllzeichen zur besseren Lesbarkeit: yyyy-mm-ddThh:mm:ss[Z]. Z steht für die Zeitzone UTC (optional), T trennt Datum und Zeit. Format: User-DN/Datum-Zeit; Zeitzone=UTC (gvGID=AT:B:0:123456,ou=people,gvOuID=AT:B:164,dc=at/2005-05-15T12:00:01 oder gvUID=mmustermann@bmi.gv.at/2005-08-18T12:00:02)
- **gvScope:** Zugriffsstufe, MUSS-Feld, cis(32). (Werte siehe 2.6).

Die folgenden Felder KÖNNEN in Objekten der Klassen gvOrgPerson, gvPersonFunction und gvOrgUnit enthalten sein und werden in den einzelnen Objektklassen nicht mehr angeführt:

- **gvAttributeScope:** Listenfeld für die Zugriffsstufen einzelner Attribute, cis(64). Bestehend aus einem Paar Attributname=Zugriffsstufe pro Value. (Werte siehe 2.6). Standardwert bei nicht angegebenem Attribut ist public. (gvBirthdate=local gvJpegPhoto=gv.at)
- **gvExtensionItem:** Optionale cis(65536) Liste. Kann verwendet werden, um spezifische Zusatzinformationen zu einzelnen Einträgen zu speichern, ohne dafür Schemaanpassungen vornehmen zu müssen. Jeder Eintrag SOLL mit einem Präfix ausgestattet werden, der den Zweck genau angibt. Soll nicht in den zentralen VD repliziert werden und darf im zentralen VD nicht öffentlich zugänglich sein.

2.6 Zugriffssteuerung

Zugriffsstufen auf Eintrags- und Attributebene sind auf folgenden Ebenen definiert:

- **private** - Daten die nicht publiziert jedoch z.B. für die Benutzerverwaltung benötigt werden

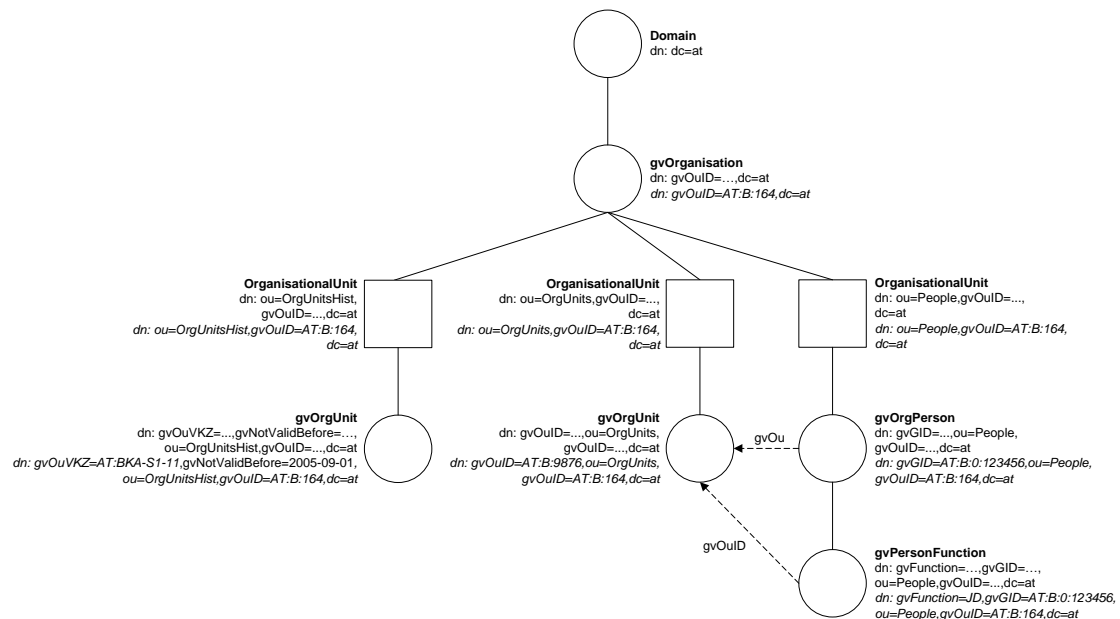
- **local** - die im internen Netz der Organisation publizierten Daten
- **gv.at** - die im Behörden-Intranet publizierten Daten als Sicht von ‚local‘
- **public** - die im Internet für anonyme Benutzer publizierten Daten als Sicht von ‚gv.at‘)

Die Zugriffsstufe auf Eintragungsebene wird über das Attribut gvScope gesetzt, um eine einfache Zugriffssteuerung und Filtermöglichkeit z.B. für die Replizierung von lokalen Verzeichnissen nach LDAP.gv.at oder für Web-Frontends realisieren zu können. Die Unterscheidung wird durch unterschiedliche Server-Adressen erreicht, die entweder unterschiedliche Server-Instanzen adressieren oder Authentifizierungs-Proxies für unterschiedlich berechnigte User am Server sind. Darüber hinaus erlaubt gvAttributeScope applikatorisch eine differenzierte Publikation von einzelnen Attributen wie Telefonnummern und E-Mail-Adressen.

Die Auswahl der Datenfelder für die Replizierung von einem lokalen Verzeichnis nach LDAH.gv.at, insbesondere jener, die personenbezogene Daten betreffen, obliegt dem Anwendungsverantwortlichen des lokalen Verzeichnisses nach Maßgabe der datenschutzrechtlich relevanten Bestimmungen.

3 LDAP-Klassen

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



- **Domain:** Abbildung der Domain-Struktur oberhalb von Organisationen, um Domänen wie .at, .local etc. abzubilden.
- Die Organisation, abgebildet durch die Klasse **gvOrganisation**, hat bei Bediensteten die Personalhoheit für die Person und ist daher für die Benutzerverwaltung rechtlich zuständig. Für eine natürliche Person können auch mehrere gvOrgPerson Einträge geführt werden, wenn diese mehrere (Dienst-, ...) Verträge mit einer oder unterschiedlichen Organisationen hat.

- Unterhalb einer Organisation existieren Container-Objekte **OrganizationalUnits** (people, orgUnits, orgUnitsHist) um für diese Objektklassen getrennte Namensräume zu schaffen.
- **gvOrgPerson**: Derzeit werden nur Bedienstete (Mitarbeiter) von Behörden berücksichtigt, die in einem oder mehreren Dienstverhältnissen stehen und deren Personendaten jeweils von der personalführenden Stelle gewartet werden¹. Die Zusammenführung mehrerer gvOrgPerson Einträge auf die gleiche natürliche Person erfolgt durch **gvbPK**. Für Mitarbeiter, die keine Bediensteten sind (Leiharbeitsverträge, Werksverträge, etc.) gilt das im übertragenen Sinn.
- Berechtigungen (gvRights) werden mittels der Auxiliary-Objektklasse **gvPrincipal** (siehe [LDAPPV]) an gvOrgPerson angehängt.
- Wenn ein Objekt gvOrgPerson (Person oder Dienstverhältnis) in einer Organisation unterschiedliche Funktionen mit unterschiedlichen Rechten hat, werden die Funktionen mit **gvPersonFunction** abgebildet und die Rechte mit gvPrincipal an gvPersonFunction angehängt. 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)
- Die Organisationseinheiten werden im Sinne des DIT flach abgebildet. Die Hierarchie der Aufbauorganisation wird über das Attribut gvOuIdParent implementiert.

gvOrganisation	Wurzelknoten für eine Organisation Abgeleitet von gvOrgUnit (die von gvOrgUnit abgeleiteten Attribute sind hier wegen der übersichtlicheren Darstellung nicht repliziert)	
(Achtung! nicht mit ‚z‘ geschrieben)		
dn: gvOuID=...,dc=at (dn: gvOuID=AT:B:164,dc=at)		
Attribut	Beschreibung (Beispiel)	Eigenschaft
dc	Domain der Organisation des Dateneigners. Der Wert MUSS unterhalb des übergeordneten Domain-Objekts eindeutig sein. (dc=at)	M, L, ia5
o	Kurzbezeichnung der Organisation (BMI)	M, S, cis(64)
Weitere Attribute siehe gvOrgUnit Die Beschreibung für gvLegalSuccessor gilt im analogen Sinn für Organisationen		

¹ Im Bundesbereich erfolgt dies etwa mittels PM/SAP.

organizationalUnit		Knoten zur Definition von Namensräumen unterhalb des Domain-Eintrags
dn: ou=...,gvOuID=...,dc=at (dn: ou=People,gvOuId=AT:B:164,dc=at)		
Attribut	Beschreibung (Beispiel)	Eigen-schaft
ou	Namespace (People, OrgUnits, OrgUnitsHist)	M, L, cis(64)

- Für das Anlegen historischer Organisationen und Organisationseinheiten wird ein Container mit dem Namespace ou=OrgUnitsHist gebildet. Objektklassen können **gvOrganisation** oder **gvOrgUnit** sein. Der DN dieser Objektklassen ist dann: gvOuVKZ=...,gvNotValidBefore=...,ou=OrgUnitsHist,gvOuID=...,dc=at

gvOrgPerson		Person in einem Vertragsverhältnis zu einer Organisation. Abgeleitet von InetOrgPerson.
dn: gvGID=...,ou=People,gvOuID=...,dc=at (dn: gvGID= AT:B:0:123456,ou=People,gvOuID=AT:B:164,dc=at)		
Attribut	Beschreibung (Beispiel)	Eigen-schaft
cn	Vorname Familienname (Martin Mustermann)	M, L, cis(64) ²
displayName	Einer der Werte aus cn [RFC2798] im Format „Familienname, Vorname“	S, cis(64)
sn	Familienname laut Stammzahlregister-Anfrage (Mustermann)	M, L, cis(64)
givenName	Vorname laut Stammzahlregister-Anfrage (Martin)	L, cis(64)
gvGID	Global eindeutiger Identifier bestehend aus: ‚AT:‘, einem Präfix, der die Systematik (z.B. VKZ der personalführenden Organisation, IT-System,...) im gesamten Verbund eindeutig bezeichnet, sowie einem innerhalb der Systematik unverwechselbar einer Person zuordenbarem nicht wiederverwendbarem Identifier. (z.B.: AT:BPK:ZP:j/NxdRQhp+tNyE9WhHdBSYuy3hA= AT:B:0:123456 PMSAP-Nr. im Bundesbereich, AT:L6:12345 im Länderbereich, AT:GGA-31001:1234 im Gemeindebereich)	M, S, ces(128)

² Die Beschränkung auf 64 Zeichen stammt nicht aus einem RFC, sondern ist durch eine Einschränkung in Softwareprodukten (z.B. Novell eDirectory) begründet.

gvBirthdate	Geburtsdatum im Format JJJJ-MM-TT	S, cis(10) ³
gvbPK	bPK der Person mit Bereichskürzel als Präfix oder bPK-PV ohne Präfix Syntax: gvBpkValue ::= [Präfix ":"] bPk Präfix ::= <Bereichskürzel lt. Bereichsabgrenzungsverordnung> bPk ::= bereichsspezifische Personenkennung für den mit dem Präfix bezeichneten Verwaltungsbereich <i>(PV:j/NxdRQhp+tNyE9WhHdBSYuy3hA=)</i>	S, ces(32)
gvOPK (deprecated)	(Rückführbares) Personenkennzeichen für den Bereich Organwalter [SZ-bPK] <i>(ZLscSj/dzLD6cD9m5XYFFA==)</i>	S, ces(128)
uid	Innerhalb der Domäne eindeutige Userkennung + Domain-Suffix im RFC 822-Format [RFC882] als Login-ID für Portale <i>(mmustermann@bmi.gv.at)</i>	L, cis(256)
gvOtherID	Andere Identifier mit Präfix <i>(PMSAP-LID:xmueller@bka.gv.at)</i>	L, ces(256)
gvSex	Geschlecht der Person <i>(male, female oder unknown)</i>	S, cis(7)
personalTitle	Akademischer Titel <i>(Mag. d. s. K.)</i>	L, cis(64)
gvIntTitle	Internationaler (nachgestellter) akademischer Titel <i>(LLM)</i>	S, cis(64)
title	Funktionsbezeichnung <i>(Abgeordneter z. NR., Bezirkshauptfrau)</i>	L, cis(64)
gvAmtstitel	Amtstitel <i>(Hofrat)</i>	S, cis(64)

³ 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.

telephoneNumber	<p>Liste von Telefonnummern im internationalen Format gem. ITU T-REC-E.123. Jeder Eintrag des LDAP-Listen-Attributes darf nur eine Telefonnummer enthalten. Landescode, Vorwahl und Anschluss müssen angegeben werden. Die Angabe der Nebenstelle ist optional.</p> <p>Beispiele: +43 1 33176, +43 680 333333333, +351 213 927860</p> <p>Abgesehen von einem führenden „+“ und Ziffern sollen nur Leerzeichen verwendet werden. (siehe E.123 Kap. 7.2 und Kap. 9). Leerzeichen sollen nur zwischen Landescode und Vorwahl sowie zwischen Vorwahl und Anschluss-Nummer verwendet werden. (E.123 Kap. 9.2).</p>	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>)	L, cis(128)
postOfficeBox	Postfach der Postanschrift (<i>Postfach 103</i>)	L, cis(40)
postalAddress	Postanschrift ohne Name Format: (max. 6 Zeilen á 40 Zeichen; die Zeilen sind durch \$ getrennt) ⁴ (<i>Hintere Salzamtstraße 1\$1030 Wien</i>)	L, cis(245)
postalCode	Postleitzahl der Postanschrift ohne Ländercode (<i>1082</i>)	L, cis(13)
l	Ort (<i>Wien</i>)	L, cis(64)
c	Land der Postadresse (2-stelliges Kürzel nach ISO 3166-1) (<i>AT</i>)	L, cis(2)
co	Land ausgeschrieben - in Deutsch	L, cis(64)
gvPhysicalAddress	Besuchs- und Lieferadresse Format wie postalAddress	S, cis(245)
roomNumber	Zimmernummer	L, cis(256)
mail	RFC 822 E-Mail Adresse im simple format (Nur Werte, deren Zugriffsstufe public ist) (<i>martin.mustermann@bmi.gv.at</i>)	L, cis(256)

⁴ Formatiert nach den Empfehlungen der österreichischen Post AG (siehe [ADR]).

jpegPhoto	Portrait in der Größe bis zu 120x160 Pixel in JPEG-Codierung. Die empfohlene Größe ist bis 5 kB	L, jpeg
gvOu	gvOuId (siehe gvOrgUnit.gvOuId) der Organisationseinheit(en), zu der die Person zugeteilt ist (kein dn) (gvOu=AT:L9:9876)	L, cis(32)
description	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.	L, cis(1024)

- Weitere optionale und im Arbeitskreis nicht besprochene Attribute sind in [RFC2798] definiert.

gvPersonFunction		Funktionen einer Person, um unterschiedliche Anwendungsrechte abzubilden
dn: gvFunction=...,gvGID=...,ou=People,gvOuID=...,dc=at (dn: gvFunction=JD,gvGID=AT:B:0:123456,ou=People,gvOuID=AT:B:164,dc=at)		
Attribut	Beschreibung (Beispiel)	Eigenschaft
gvFunction	Kurze Funktionsbezeichnung (JD)	M, S, cis(32)
description	Funktionsbezeichnung (Journaldienst)	L, cis(1024)
gvOuID	gvOuID der Organisationseinheit, zu der die Person in dieser Funktion zugeteilt ist. (gvOuId=AT:L9:9876)	M, S, cis(32)
gvSortkey	Zur Festlegung der Sortierreihenfolge von Funktionen	S, cis(64)

- Um die Zugehörigkeit zu *mehreren* Organisationen und die Zuteilung von Rechten abzubilden bestehen folgende Varianten:
 1. n gvOrgPerson, 1 Wert im Attribut gvOu: Pro Dienstverhältnis bzw. Org-ID existiert ein gvOrgPerson-Objekt. Damit können sich für eine Person mehrere gvOrgPerson-Objekte im Verzeichnis befinden, wobei gvOrgPerson um gvPrincipal erweitert wird und der Org-ID damit eine Liste von Rechten zugeordnet wird. gvOrgPerson.gvOu enthält einen einzigen Eintrag.
 2. 1 gvOrgPerson, n gvPersonFunction: Zu jeder Funktion ist im Attribut gvPersonFunction.gvOuId festgelegt, zu welcher Organisationseinheit diese zugeordnet ist. In gvOrgPerson.ou sind alle Organisationseinheiten angeführt, für die die Person tätig ist.

Die angeführten Varianten stehen implementierenden Stellen frei zur Auswahl. Um Redundanzen zu vermeiden SOLLTE ausschließlich eine der angeführten Möglichkeiten implementiert werden.

gvOrgUnit	1. Organisationseinheit 2. Organisation gvOrgUnit wird von OrganizationalUnit abgeleitet	
dn: gvOuID=..., ou=OrgUnits,gvOuID=...,dc=at (dn: gvOuID=AT:B:9876,ou=OrgUnits,gvOuID=AT:B:164,dc=at)		
Attribut	Beschreibung (Beispiel)	Eigen-schaft
gvOuID	Primärschlüssel für Organisationseinheit Syntax: gvOuID::= Landeskennung ":" ID ID::= "VKZ:" VKZ Org-Id VKZ... Verwaltungskennzeichen gem [VKZ] Org-Id... Org-Id gem [VKZ] Landeskennung...gem ISO 3166 - Alpha2 (AT:VKZ:GGA1234, AT:L9:9876)	M, S, cis(32)
gvOuVKZ	Organisationskennzeichen (OKZ) gemäß der Spezifikation [VKZ]. Das Organisationskennzeichen ist für die Verwendung auf Ausdrucken, als Suchbegriff bzw. zur Anzeige vorgesehen. Das OKZ enthält Semantik und ist nur für österreichische Organisationen definiert. Für Referenzen in elektronischen Datenbeständen soll dieses Kennzeichen NICHT verwendet werden, sondern ausschließlich die gvOuId. Das VKZ kann aufgrund von Namensänderungen angepasst werden müssen. (z.B. BMEIA statt BMAA für das Außenministerium) (z.B. GGA-12345)	M, S, cis(32)
ou	Kurzbezeichnung der Organisationseinheit (z.B. IV/2b)	M, L, cis(64)
gvOuIdParent	Übergeordnete OE; Wert: gvOuId der übergeordneten OEs (kein dn!)	S, cis(32)
cn	Bezeichnung der Organisationseinheit (ausgeschrieben) (Abt. ITMS/Ref. NIK - Referat nationale und internationale Koordination)	M, L, cis(64)
gvOuCn	Gesamtbezeichnung der Organisationseinheit (für die Anschrift ohne Adressteil). Wert kann mehrzeilig sein mit als Trennzeichen. (Bundesministerium für Inneres Sektion IV/Abt. ITMS/Ref. NIK)	M, S, cis(1024)
mail	RFC 822 [RFC882] E-Mail-Adresse (helpdesk@xyz.gv.at)	L, cis(256)
telephoneNumber	Tel-Nummer	L, tel(32)

facsimileTelephoneNumber	Fax-Nummer	L, tel(32)
street	(Postadresse, nicht Standortadresse)	L, cis(128)
postOfficeBox	Postfach der Postanschrift (<i>Postfach 103</i>)	L, cis(40)
l	Ort (<i>Wien</i>)	L, cis(64)
postalAddress	Wie gvOrgPerson	L, cis(245)
postalCode	Wie gvOrgPerson	L, cis(40)
c	Wie gvOrgPerson	L, cis(2)
co	Wie gvOrgPerson	L, cis(64)
gvPhysicalAddress	Wie gvOrgPerson	S, cis(245)
gvImageRef	Verwendung + Referenz auf Bilder im Format {Verwendung} URI Standardverwendungen sind Logo, Zugang und Zufahrt, die Liste kann erweitert werden; z.B.: {logo} <i>http://www.xyz.gv.at/logo1.jpg</i> {Zugang} <i>http://www.xyz.gv.at/zugang.jpg</i>	L, uri
gvWebAddress	URL der Homepage	S, uri
description	Wie gvOrgPerson ⁵	L, 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	S, cis(32)
gvSortkey	Zur Festlegung der Sortierreihenfolge in Listen von OEs der gleichen Ebene wird gvSortkey als erster und ou als zweiter Sortierschlüssel verwendet	S, cis(64)
gvNotValidBefore	nicht gültig vor - im Format JJJJ-MM-TT	S, cis(10)
gvNotValidAfter	nicht gültig nach - im Format JJJJ-MM-TT	S, cis(10) ⁶
gvOtherID	Zusätzliche(s) Kennzeichen zum Datenabgleich	L, ces(128)

- Das Attribut **gvLegalSuccessor** zeigt immer zum unmittelbaren Rechtsnachfolger. Dieser kann wiederum einen Rechtsnachfolger haben. Um den

⁵ Für die Beschreibung der Aufgaben einer Organisationseinheit soll das Attribut gvDescription aus dem Best Practice Dokument BV Bund 1.0.0 verwendet werden.

⁶ Wenn die Organisationseinheit besteht (aktiv ist), bleibt der Eintrag leer.

aktuellen Rechtsnachfolger einer Organisationseinheit oder einer Organisation zu finden, muss die Verkettung bis ans Ende aufgelöst werden.

- Weitere optionale Attribute sind in [RFC2256] definiert.

4 Referenzen

- [SZ-bPK] Hollosi, Arno/Hörbe, Rainer: Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK), <http://reference.e-government.gv.at/AG-II-BK-Stammzahl-bPK-Algorit.2229.0.html>, 2007
- [RFC882] Mockapetris, P.: RFC 882 – Domain Names - Concepts and Facilities, <http://www.ietf.org/rfc/rfc882.txt?number=882>, 1983
- [RFC2798] Smith, M.: RFC 2798 – Definition of the inetOrgPerson LDAP Object Class, <http://www.ietf.org/rfc/rfc2798.txt?number=2798>, 2000
- [RFC2251] Wahl, M. et. al.: RFC 2251 – Lightweight Directory Access Protocol (v3), <http://www.ietf.org/rfc/rfc2251.txt?number=2251>, 1997
- [RFC2256] Wahl, M.: RFC 2256 – A Summary of the X.500(96) User Schema for Use with LDAPv3, <http://www.ietf.org/rfc/rfc2256.txt?number=2256>, 1997
- [VKZ] Grandits, Franz: Kennzeichen für Organisationseinheiten von Gebietskörperschaften bzw. von Körperschaften öffentlichen Rechts (Verwaltungskennzeichen), http://reference.e-government.gv.at/Q-VV_Vewaltungskennzeichen_vkz.1070.0.html, 2007
- [VKZEB] Grandits, Franz: Ebenen-und Bereichskennungen für das Verwaltungskennzeichen, <http://reference.e-government.gv.at/VKZ-Bereichskennungen.673.0.html>, 2011
- [ADR] Post AG: "Richtig Adressieren" http://www.business.post.at/content/pdf/RichtigAdressieren_WWW1.pdf
- [SecC] Hörbe, Rainer: Spezifikation Sicherheitsklassen, SecClass 2.1.0 <http://www.ref.gv.at/KONVENTIONEN.1116.0.html>, 2007
- [LDAPPV] Hahn, Harald/Pichler, Peter/Hörbe, Rainer/Gombotz, Dietmar/Spitzenberger, Martin: Spezifikation LDAP-gv.at für Portalverbund, LDAP-gv.at_PV 1.0.0, <http://reference.e-government.gv.at/AG-IZ-LDAP-Dokumente-LDAP-gvat.2258.0.html>, 2009

5 Historie

Version	Datum	Kommentar
2.3.0	21.02.2006	Version 2.3.0 baut auf dem internen Entwurf LDAP-gv.at 2.2.9 auf und beinhaltet im Hinblick auf die Anforderungen der Standardportalsoftware Schemaänderungen, die auf offiziellem Wege abzustimmen sind.
Ersteller		
Martin Spitzenberger		<ul style="list-style-type: none">• Anpassung der DNs wegen Entfall von combined-DNs• Zusammenfassung der Attribute gvSource, gvScope und gvStatus im allgemeinen Teil• gvOrgPerson:<ul style="list-style-type: none">○ Anpassungen und Beschreibung von gvGID○ Aufnahme der Attribute gvOtherID, gvbPK und gvOPK○ Korrektur der Beschreibung des Feldes l○ Entfernung von gvRights und gvSecClass aus gvOrgPerson (zukünftig in gvPrincipal [LDAPPV])• gvPersonFunction:<ul style="list-style-type: none">○ Präzisierung der Verwendung○ Entfernung von gvRights und gvSecClass aus gvOrgPerson (zukünftig in gvPrincipal [LDAPPV])• gvOrgUnit:<ul style="list-style-type: none">○ Klarere Beschreibung von gvOuID○ Aufnahme bzw. Anpassung der Attribute gvOuVKZ, gvNotValidBefore, gvNotValidAfter sowie gvOtherID○ Korrektur der Beschreibung des Feldes l• OrganisationalUnit<ul style="list-style-type: none">○ ou=OrgUnitsHist ermöglicht Containerobjekt für historisierte Organisationseinheiten

Version	Datum	Kommentar
2.4.0	22.05.2009	<ul style="list-style-type: none">• DIT-Änderung: Löschung des DC „gv“.• Beschreibung von gvSource: „Änderung“ ersetzt „Transaktion“ zur besseren Verständlichkeit• Erläuterung gvOrgPerson (S. 6): Streichung von gvGID, da diese im verzeichnis eindeutig und somit für die Zusammenführung von Einträgen nicht geeignet ist.• Präzisierung der Beschreibung von gvOrgUnit.gvOuId
Ersteller		
Martin Spitzenberger		

- gvOrgPerson.gvGID:
 - Beschreibung „Global eindeutiger Identifier“
 - Anpassung Beispieltext für bPK
 - Anpassung ergänzende Beschreibung
- Neue Attribute, die sich aus den allgemeinen Anforderungen elektronischer Behördenverzeichnisse ergeben:
 - gvOrgPerson.gvIntTitle
 - gvPersonFunction.gvSortKey
- Ergänzung von gvAttributeScope
- Kennzeichnung von Single-Value Attributen, Default ist Multi-Value

Version	Datum	Kommentar
2.4.1	30.08.2010	<ul style="list-style-type: none"> • gvAttributeScope <ul style="list-style-type: none"> ○ in Listenfeld geändert ○ auf 64 Zeichen erweitert ○ Abgrenzung zu MUSS-Custom Attributen ○ Formatierung auf Fett korrigiert • gvOrgUnit.gvOtherID auf Listenfeld korrigiert • gvOrgPerson.gvOu: Im Beschreibungstext Org-ID durch Referenz auf gvOrgUnit.gvOuId ersetzt • Multivalue Attribute gem. RFCs korrigiert
Ersteller		
Martin Spitzenberger		

Version	Datum	Kommentar
2.4.1	03.06.2011	<ul style="list-style-type: none"> • gvExtensionItem bei den Objektklassen gvOrgPerson, gvOrgUnit und gvPersonFunction hinzugefügt • gvOrgPerson.gvIntTitle ist Single Valued • gvPersonFunction.description ist laut RFC ein Listfeld und cis(1024)
Ersteller		
Harald Hahn		

Version	Datum	Kommentar
2.4.1	30.11.2011	<ul style="list-style-type: none"> • gvExtensionItem als Custom Attribute definiert • gvbPk: Der Text widerspricht dem Beispiel (das „AT:“) • Die Präfix für die gvGid wurde genauer definiert • gvOuVKZ: Kein Landespräfix für gvOuVKZ • telephoneNumber: Formatvorgaben an ITU T-REC-E.123 angepasst.
Ersteller		
Peter Pichler		

Version	Datum	Kommentar
2.5.0	02.02.2012	<ul style="list-style-type: none"> • Hinweis zu RFC Listenattributen (single/multi value) • gvbPK: Bei der bPK aus der Personalverwaltung entfällt das Präfix. • Beschreibungstext Dokumentstruktur aktualisiert
Ersteller		
Harald Hahn / Gerold Pesendorfer		

Version	Datum	Kommentar
2.5.1	10.01.2017	<ul style="list-style-type: none"> • gvOrgPersonFunction – Änderung bei Abbildung der Zuordnung zu mehreren Organisationseinheiten (GP) • gvExtensionItem Änderung bei Replikation in zentralen VD (GP) • Nicht Wiederverwendbarkeit der gvGid eindeutiger beschrieben (PP / Sub-AG-PVP) • deprecated Kennzeichnung des Attributes gvOrgPerson.gvOPK (Sub-AG PVP) • Titelblatt angepasst
Ersteller		
Peter Pichler (LFRZ, Sub-AG-PVP)		