

Datum:	2006-04-21	Version:	V1.0
Verfasser:	Rainer Hörbe		
Projekt:	Ldap.gv.at	Themen:	<b>Abgleich von Portalverzeichnissen über ldap.gv.at</b>

## Inhalt

<b>1 ZWECK</b>		<b>1</b>
<b>2 GRUNDKONZEPT</b>	FEHLER! TEXTMARKE NICHT DEFINIERT.	
<b>3 ZENTRALE VERWALTUNGSDOMÄNE</b>		<b>3</b>
3.1 Datenstruktur der zentralen Verwaltungsdomäne		3
<b>4 REGISTRATUR</b>		<b>5</b>
<b>5 ABGLEICH DER DATEN ZWISCHEN LOKALEM UND ZENTRALEM VERZEICHNIS</b>		<b>5</b>
<b>6 WEITERE VORGANGSWEISE</b>		<b>6</b>
<b>7 REFERENZEN</b>		<b>6</b>

## 1 Zweck

Stamm- und Anwendungsportal benötigen zum Teil gemeinsame Daten, deren redundante Pflege eingespart werden soll. Durch einen Austausch der Daten via ldap.gv.at soll der Abgleich gewährleistet werden. Für diese Daten müssen Verantwortlichkeit und Prozess der Wartung definiert sein.

## 2 Use Cases

Folgende Anwendungsfälle werden durch die zentrale Bereitstellung von Daten unterstützt:

- Einrichtung von Stamm- and Anwendungsportalen (Zertifikat)
- Einrichtung von Anwendungen an Stammportalen (Anwendungsparameter, Rechte)
- Berechtigung von zugriffsberechtigten Stellen am Anwendungsportal
- Anwendungsinformationen für Anwendungsentwickler (WSDL, Anwendungs-Homepage)
- Publikation von Anwendungen laut PVV
- Antrag zur Nutzung von Anwendungen (Kontaktinformationen)
- Benachrichtigung über die Verfügbarkeit von anwendungen

### 3 Zuständigkeit für die Datenverwaltung in Portalen

Die durch das Datenmodell LDAP-gv.at definierten Objekte sind in Verwaltungsdomänen eingeteilt, die definieren, welche Organisationen und Anwendungsbereiche für die Pflege der Daten verantwortlich sind. Klassendiagramme sind in [ldap-gv.at dm2] zu finden.

Stamm- und Anwendungsportale benötigen sowohl eigene als auch fremde Daten, die Zuständigkeit der Objekte ist wie folgt:

<i>Art der Objekte</i>	<i>Objektklasse im LDAP</i>	<i>Verwaltungsdomäne</i>
eigene/nachgeordnete zugriffsberechtigte Stelle	gvOrganisation	Zentral / Ldap.gv.at
eigener STP-Betreiber	gvOrganisation	Zentral / Ldap.gv.at
eigener AWP-Betreiber	gvOrganisation	Zentral / Ldap.gv.at
eigenes STP	gvUserPortal, gvApplicationProxy, gvPortal	Lokal / STP
eigene Personen	gvOrgPerson	Lokal / Personalverwaltung
eigene Benutzer	gvPrincipal	Lokal / Benutzerverwaltung/Portal
eigene Application User	gvUserPrincipal	Lokal / Benutzerverwaltung
eigene Benutzerzertifikate	gvX509PKC	Lokal / Benutzerverwaltung
Eigenes AWP	gvApplication, gvApplicationRight, gvParticipant, gvPortal	Lokal / AWP

Portale benötigen eine lokale Instanz sämtlicher Verzeichnisdaten um eine gute Betriebssicherheit zu erreichen. Dazu werden die Daten zwischen lokaler und zentraler Instanz repliziert. Der Datenaustausch zwischen Portalen sieht demnach so aus:

<i>Lokale Verzeichnisinstanz</i>	<i>Zentrales ldap.gv.at</i>
>> Upload von eigenen öffentlichen Daten >>	
<< Download fremder öffentlicher Daten <<	

## 4 Zentrale Verwaltungsdomäne

Für die konsistente Identifikation von Organisationen ist es notwendig folgende rechtlich eigenständigen Organisationen in einem definierten Prozess vollständig zu erfassen:

- Gebietskörperschaften (Bund, Länder, Gemeinden)
- andere Portalverbundteilnehmer (HVSV, ..)
- Dienstleister die Portale betreiben (BRZG, Kommunalnet, ..)

Dadurch werden VKZ und OrgID definiert und sich darauf aufbauende Datenstrukturen verlässlich.

### 4.1 Datenstruktur der zentralen Verwaltungsdomäne

Die zentrale Verwaltungsdomäne ist für die vollständige Befüllung von ldap.gv.at mit folgenden Daten:

Objektklasse: Organisationen (gvOrganisation)

erforderliche Attribute: OrgID (gvOuID), VKZ (gvOuVKZ), Bezeichnung (cn)

Datenbereich: Alle selbstständigen Organisationen der PV-Teilnehmer, zugriffsberechtigten Stellen und Dienstleister, die ein Portal betreiben, soweit sie in den Geltungsbereich der Portalverbundvereinbarung fallen.

Private Organisationen, die auf Grund anderer Vereinbarungen auf ein Portal zugreifen, werden lokal geführt und nicht in ldap.gv.at repliziert. Diese Organisationen sollten unter einem separaten Knoten (dc=local, dc=at) geführt werden.

Objektklasse: Stammportal (gvUserPortal)

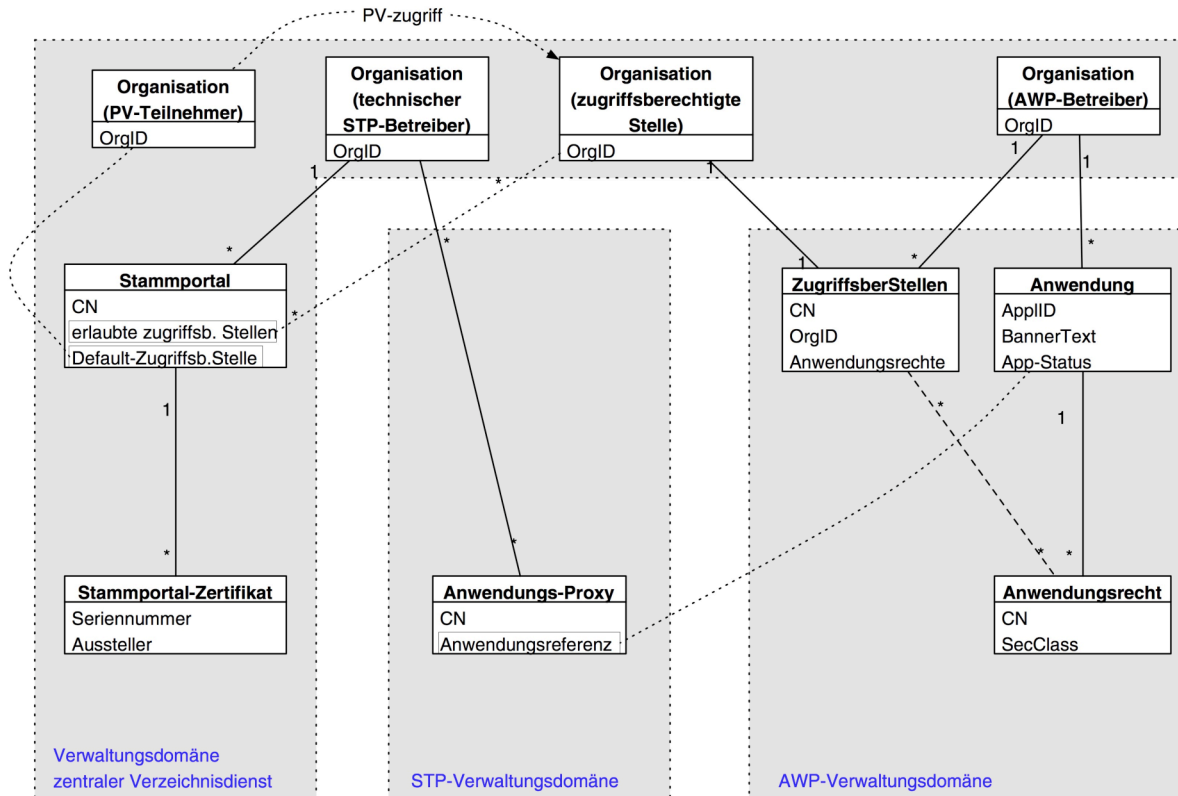
erforderliche Attribute: CN (cn), erlaubte zugriffsberechtigte Stellen (gvParticipant), Default-zugriffsb. Stelle (gvDefaultParticipant)

Datenbereich: Alle extern zugänglichen Stammportale im Portalverbund (egal ob für Produktions- oder Testbetrieb)

Objektklasse: Stammportalzertifikat (gvCertificate)

erforderliche Attribute: Seriennummer (x509SerialNumber), Issuer (x509IssuerDnsName)

Datenbereich: Alle Zertifikate von Stammportalen im Portalverbund



## 5 Registratur

Für die zentrale Verwaltungsdomäne ist als Registraturstelle das BKA (CIO) zuständig, welches das LFRZ mit der technischen Durchführung beauftragt. Der Prozess der Registratur ist wie folgt definiert:

- Antrag auf Erfassung/Änderung geht beim BKA ein, vorzugsweise als signierte E-Mail.
- Prüfung, ob Antragsteller berechtigt ist die Daten einzubringen, formelle Prüfung auf Vollständigkeit (VKZ, Mussfelder)
- Weiterleitung an das LFRZ (per signierter E-Mail)
- LFRZ führt Änderung durch und bestätigt an Antragsteller. Wenn eine zu vergebende OrgID nicht im Antrag enthalten ist, wird sie vom LFRZ im Bereich AT:BLFRZ: automatisch vergeben.

Das LFRZ stellt Vorlagen der Datenstruktur zur Verfügung. Seitens des LFRZ werden die entstehenden Kosten aus der Betriebsführung von ldap.gv.at getragen.

*Anmerkung: Im Zuge der Eintragung wird es immer wieder Unklarheiten im Bezug auf die Vergabe von VKZ kommen, da diese derzeit unterspezifiziert sind. Zur Vereinfachung der Abwicklung wäre es auch sinnvoll, wenn in diesem Prozess im Zweifelsfall gleich das VKZ festgelegt wird. -> TO DO der Q-PV*

## 6 Abgleich der Daten zwischen lokalem und zentralem Verzeichnis

Der Datenabgleich zwischen zentraler und lokaler Instanz ist bezogen auf die jeweilige Verwaltungsdomäne immer unidirektional. Upload und Download sollen wie folgt konfiguriert werden:

Organisationen, Stammportale, STP-Zertifikate	Download
Eigene Anwendungen und deren Rechte	Upload
Fremde Anwendungen und deren Rechte	Download
Eigene ApplicationProxies	Bleiben lokal

Das LFRZ wird eine PVP/SOAP-Schnittstelle zur Verfügung stellen, mit der die Daten ins Verzeichnis ldap.gv.at hochgeladen werden können. Der Download kann per PVP/SOAP oder alternative auch per ldap:// erfolgen, da dafür keine Authentifizierung erforderlich ist.

## 7 Weitere Vorgangsweise

Erstbefüllung:

- Bund aus PM/SAP (Dazu sollte es nicht notwendig sein eine datenschutzrechtliche Genehmigung jeder Organisation einzuholen, da keine personenbezogenen Daten enthalten sind.)  
Bundesorganisationen, die nicht im PMSAP geführt werden (z.B. Statistik) werden auf Antrag eingetragen.
- Länder: aus dem Amtskalender (oder durch die jeweilige LAD)
- Gemeinden: aus help.gv.at
- andere Organisationen: auf Antrag

## 8 Referenzen

[ldap-gv.at dm2]

Hahn, Pichler, Hörbe:

Datenmodell des Verzeichnisdienstes LDAP-gv.at TEIL 2

LdapGvAt\_Teil2, V1.2

<https://w4.wien.gv.at/> -> ldap -> schema