

<b>Abgleich von Portalverzeichnissen über ldap.gv.at</b>	<b>Konvention</b>	
	<b>PorLdapSync 1.0.0</b>	
	<b>Empfehlung</b>	
Kurzbeschreibung	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.	
<b>Autor(en):</b>	<b>Rainer Hörbe Martin Spitzenberger, BKA</b>	<b>Projektteam / Arbeitsgruppe</b>
		<b>VD-Betrieb / AG I-Z</b>
<b>Beiträge von:</b>		

Version 1.0.0: **08.04.2009**

Fristablauf: **13.07.2009**

---

## Abgleich von Portalverzeichnissen über ldap.gv.at

Stamm- und Anwendungsportale benötigen zum Teil gemeinsame Daten, deren Kommunikation erleichtert und redundante Pflege eingespart werden soll. Durch einen Austausch der Daten via ldap.gv.at an dem alle (Sub-)Teilnehmer<sup>1</sup> teilnehmen können, soll der Abgleich gewährleistet werden. Für diese Daten müssen Verantwortlichkeit und Prozess der Wartung definiert sein.

### (1) Use Cases

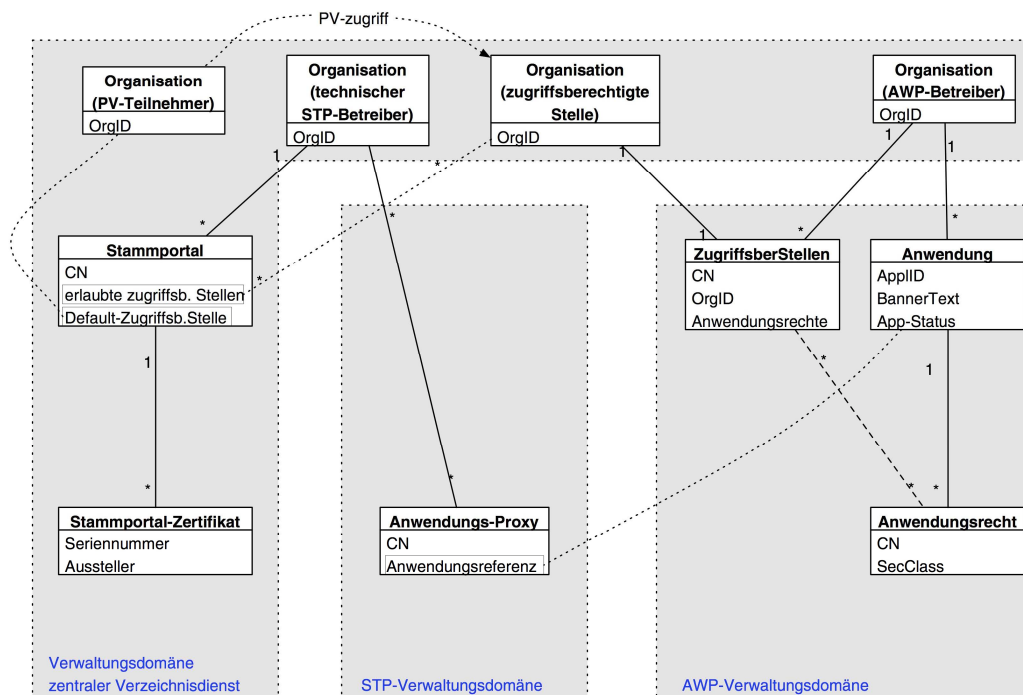
Folgende Anwendungsfälle werden durch die zentrale Bereitstellung von Daten unterstützt:

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

---

<sup>1</sup> Organisation die am Portalverbund teilnehmen, im Sinne von PVP 1.9  
PorLdapSync 1.0.0

## (2) 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 Delegationsknoten verantwortlich sind. Klassendiagramme sind in [LDAPPV] zu finden.

Im Bereich der zentralen Verwaltungsdomäne ist die erstmalige Einrichtung der Delegationsknoten von der laufenden Wartung der untergeordneten Objekte und Attribute zu unterscheiden. Erstere erfolgt durch eine Gruppe definierter Stellen (siehe (5)), letztere durch den jeweils verantwortlichen (Sub-)Teilnehmer selbst.

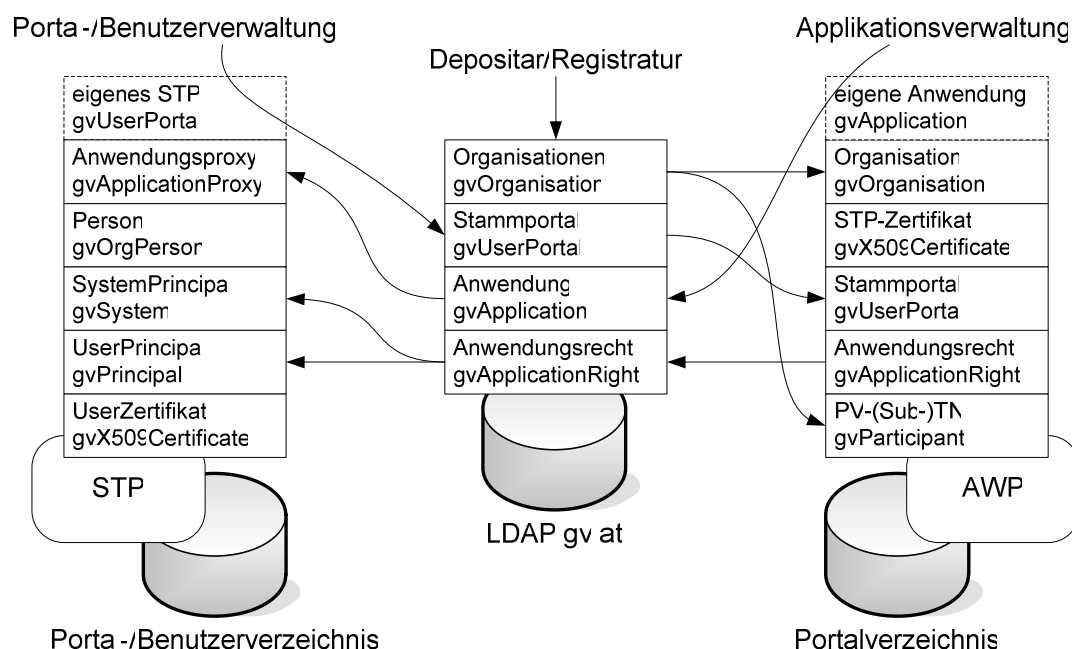
Stamm- und Anwendungsportale benötigen sowohl eigene als auch fremde Daten, die Zuständigkeit der Objekte ist wie folgt:

Art der Objekte	Objektklasse im LDAP	Verwaltungsdomäne
(Sub-)Teilnehmer	gvOrganisation	Zentraler Verzeichnisdienst
STP-Betreiber	gvOrganisation	Zentraler Verzeichnisdienst
AWP-Betreiber	gvOrganisation	Zentraler Verzeichnisdienst
STP	gvUserPortal, gvApplicationProxy, gvPortal	Lokales Verzeichnis / STP
Personen	gvOrgPerson	Lokales Verzeichnis / Personalverwaltung /
Benutzer	gvPrincipal	Lokales Verzeichnis / Benutzerverwaltung STP
Application User	gvUserPrincipal	Lokales Verzeichnis /

		Benutzerverwaltung STP
Benutzerzertifikate	gvX509PKC	Lokales Verzeichnis / Benutzerverwaltung STP
AWP	gvApplication, gvApplicationRight, gvParticipant, gvUserPortal	Lokales Verzeichnis / 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:

Lokales Verzeichnis	>> Upload von eigenen öffentlichen Daten >>	Zentraler Verzeichnisdienst
	<< Download fremder öffentlicher Daten <<	



### (3) Erforderliche Daten des zentralen Verzeichnisdienstes

Die zentrale Verwaltungsdomäne ist für die vollständige Befüllung von ldap.gv.at mit folgenden Daten, welche das erforderliche Minimum für den effizienten Betrieb des Portalverbundes darstellen, zuständig:

Objektklasse	weitere Attribute (neben den in ldap.gv.at Teil 1 und Teil 2 als MUSS definierten)	Datenbereich
Organisationen: gvOrganisation		Alle selbstständigen Organisationen der PV-(Sub-)Teilnehmer und Dienstleister, die im

		Geltungsbereich der Portalverbundvereinbarung ein Portal betreiben.
Stammportal: gvUserPortal		Alle extern zugänglichen Stammportale im Portalverbund (egal ob für Produktions- oder Testbetrieb)
Anwendung: gvApplication	URL: gvURL App-Status: gvApplicationStatus Eintrag-Status: gvStatus Url Mapping: gvURLMapping Anwendungsverantwortlicher: gvAppOwner technischer Kontakt: gvAppTechContact administrativer Kontakt: gvAppAdmin	Alle Anwendungen im Portalverbund
Rolle: gvApplicationRight	Sicherheitsklasse: gvSecClass Parametersyntax: gvRoleSyntax Eintrag-Status: gvStatus Beschreibung des Rechts: description	Alle Anwendungen im Portalverbund

Private Organisationen, die auf Grund anderer Vereinbarungen auf ein Portal zugreifen werden ausschließlich lokal geführt und nicht in ldap.gv.at repliziert. Diese Organisationen werden durch ein entsprechendes, vom Replikationsmechanismus erkennbares Attribut gekennzeichnet.

#### **(4) Erstbefüllung**

Die Befüllung des zentralen Verzeichnisdienstes mit den in 0 beschriebenen Daten wird durch den Auftraggeber des zentralen Verzeichnisdienstes veranlasst. Nach Anlage der entsprechenden Einträge erfolgt eine Verständigung der eingetragenen (Sub-)Teilnehmer. Die weitere Datenpflege erfolgt durch diese selbst gemäß den in (6) angeführten Varianten. Participants können die Datenpflege intern an Anwendungs- bzw. Portalverantwortliche delegieren.

#### **(5) Registrierungsprozess**

Für die Registrierung nach der Erstbefüllung hinzukommender (Sub-)Teilnehmer ist einerseits der Depositar laut §1 Abs 3 PVV zuständig, welcher den technischen Betreiber des zentralen Verzeichnisdienstes mit der Durchführung beauftragt. Andererseits sind folgende Stellen (im folgenden

Registraturstellen genannt) berechtigt, (Sub-)Teilnehmer in ldap.gv.at einzutragen und dafür mit Schreibzugriff auf Organisationsobjekte ausgestattet:

- Stadt Wien
- BMI
- BMF
- BKA

Der Prozess der Registratur ist wie folgt definiert:

- Ein Antrag auf Beitritt zur Portalverbundvereinbarung ist wie bisher an den Depositar zu richten, welcher die Daten nach Ablauf der Einspruchsfrist in ldap.gv.at einträgt und somit veröffentlicht.
- Ein Antrag auf Erfassung von Daten eines (Sub-)Teilnehmers kann bei einer der oben angeführten Registraturstellen eingehen.
- Die Registraturstelle prüft, ob der Antragsteller berechtigt ist die Daten einzubringen; es erfolgt eine formelle Prüfung auf Vollständigkeit (siehe Punkt 0).
- Die Registraturstelle legt einen Delegationsknoten mitsamt Administratorobjekt an und verständigt den Antragsteller.
- Nach Anlage des Eintrages erfolgt die weitere Datenpflege durch den Antragsteller gemäß (6).

## (6) Datenpflege

### (6.1) Replikation mit Senderkomponente

Das LFRZ stellt eine PVP/SOAP-Schnittstelle zur Verfügung, mit der Daten aus lokalen Verzeichnissen in ldap.gv.at geladen werden können. Es besteht die Möglichkeit durch Vergleich der Änderungsdaten von Objekten nur zuletzt geänderte Objekte zu übertragen und so die Datenmenge zu minimieren.

Der Download kann per PVP/SOAP oder alternativ auch per ldap(s) erfolgen, da dafür keine Authentifizierung erforderlich ist.

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

Die Pflege des eigenen Portals und eigener Anwendungen kann direkt in LDAP.gv.at erfolgen oder durch Replikation der entsprechenden in den lokalen Verzeichnissen anzulegenden Objekte durchgeführt werden.

---

### **(6.2) *Wartungsapplikation***

Für die Pflege der Objekte in ldap.gv.at wird eine Wartungsapplikation über Portalverbund bereitgestellt, welche die direkte Änderung der eigenen Organisationsdaten<sup>2</sup> in ldap.gv.at ohne Replikation aus einem lokalen Verzeichnis und ohne LDAP-Werkzeuge ermöglicht.

### **(6.3) *LDAP-Editor***

Neben der Weboberfläche kann, die entsprechenden Berechtigungen vorausgesetzt, auf ldap.gv.at auch direkt mittels Standard-LDAP-Editor schreibend zugegriffen werden. Auf diese Weise können alle eigenen Daten (einschließlich Applikationen) im zentralen Verzeichnis gepflegt werden.

## **(7) Referenzen**

- [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://www.ref.gv.at/KONVENTIONEN.1116.0.html>

---

<sup>2</sup> Die Applikation unterstützt auch die Pflege von Personendaten  
PorLdapSync 1.0.0