

Revisionsabfrage im Portalverbund		Konvention	
		PVP-AuditQuery 1.0.0	
		Empfehlung	
Kurzbeschreibung:	In diesem Dokument wird die Schnittstelle spezifiziert, die laut Portalverbundvereinbarung §4(8) pro Stammportal umzusetzen ist. Diese Schnittstelle ist so gestaltet, dass sie auch für die interne Revision eines Stammportals verwendet werden kann.		
Autor:	Rainer Hörbe (Q-PV)	Projektteam / Arbeitsgruppe:	Arbeitsgruppe Q-PV
Beiträge von:	Wolfgang Kremser (BMI) Peter Pfläging (Wien) Harald Stradal (BMI)		

Inhaltsverzeichnis

1. DATENMODELL	3
2. REFERENZEN.....	3
3. UMSETZUNG	4
3.1. AUSGABEFORMAT	4
3.2. BEREITSTELLUNG DER REVISIONSABFRAGE	4
3.3. ABFRAGE FÜR ENDBENUTZER	5
3.3.1. Request	5
3.3.2. Response	6
3.4. ZUGRIFF ÜBER SOAP	7
3.5. BERECHTIGUNGSPRÜFUNG	9
3.6. GUI-SCHNITTSTELLE FÜR REVISIONSBERECH.....	9
4. ANHANG	9
4.1. ERGEBNIS DER BEISPIEL-URLS	9
4.2. AUSGABEBEISPIEL	11

1 Datenmodell

Laut PVV sind in der Revisionsabfrage den Anwendungsverantwortlichen für alle Benutzer, die auf deren jeweiligen Anwendungen Zugriff haben, folgende Attribute auszugeben:

- o Familienname
- o Vorname
- o UserID
- o Global Identifizier
- o Organisationseinheit des Benutzers (Schlüssel)
- o Organisationseinheit des Benutzers (Bezeichnung)
- o Zugriffsrechte

2 Referenzen

Die externen Referenzen sind in der aktuellen PVP-Spezifikation (www.ref.gv.at) angegeben.

3 Umsetzung

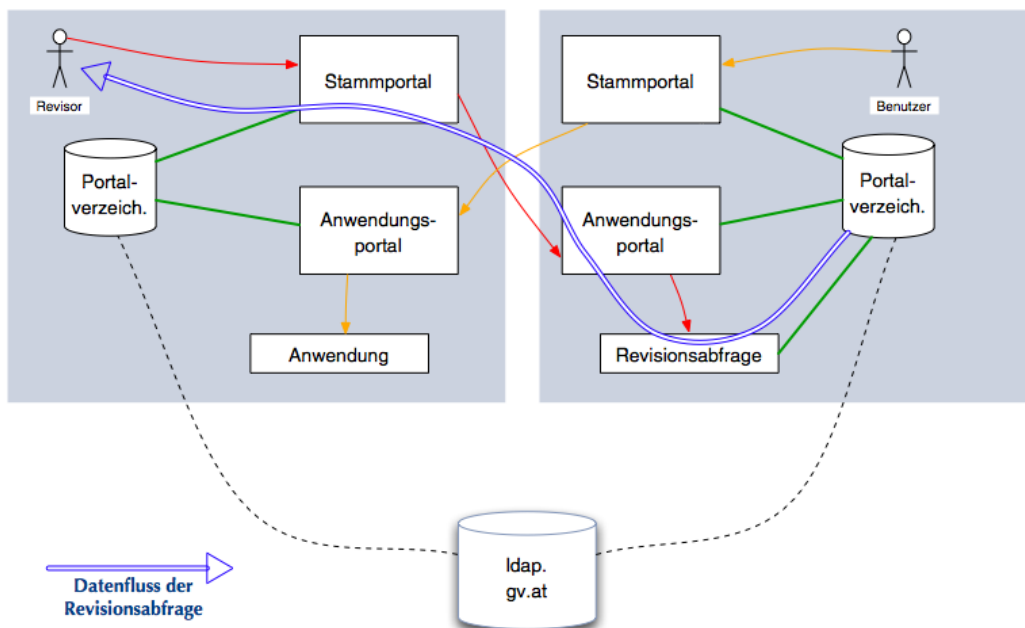
3.1 Ausgabeformat

Die Revisionsabfrage wird für die Abfrageberechtigten in zwei Formen bereitgestellt:

1. Von Endbenutzern direkt verarbeitbar. Dazu wird als das Flat-File Format CSV verwendet, das von diversen Editoren und Office-Werkzeugen importiert werden kann, die Zugriffe erfolgen nach dem REST-Modell.
2. Für Entwickler als Programmschnittstelle, wo der Zugriff über SOAP erfolgt und die Daten im XML-Format ausgegeben werden.

3.2 Bereitstellung der Revisionsabfrage

Die Funktion wird als Anwendung an den Anwendungsportalen der Stammportalbetreiber implementiert. Den Revisionsberechtigten der Anwendungsverantwortlichen sind die notwendigen Zugriffsrechte einzurichten, damit alle Berechtigungen der betreffenden Anwendung gelesen werden können.



Organisationen mit Stamm- aber ohne eigenes Anwendungsportal können die Funktionalität des Anwendungsportals auch in der Revisionsabfrage implementieren. Dazu ist im Wesentlichen nur das Zertifikatsmanagement erforderlich.

3.3 Abfrage für Endbenutzer

3.3.1 Request

Revisionsabfragen werden als HTTP GET-Requests am Portal abgesetzt. Dabei müssen bzw. können die Selektionsparameter als Teile des Pfades im URL angegeben werden:

1. das Verwaltungskennzeichen der zugriffsberechtigten Stelle,
2. Globale ApplikationsID der Anwendung in ldap.gv.at (gvglobapplid) und
3. der CN des Anwendungsrechts.

Verwaltungskennzeichen und Globale ApplikationsID sind verpflichtend. Der CN des Anwendungsrechts ist optional und dient der weiteren Einschränkung der Abfrage.

Jeder Selektionsparameter kann den Wert ‚all‘ für sämtliche Werte oder eine konkrete Ausprägung haben. Ist der Pfad leer muss eine Liste der für den Benutzer verfügbaren Werte angezeigt werden, d.h. die Schnittmenge der erlaubten und verfügbaren Werte.

Der Pfad hat damit folgenden Aufbau:

Query-URL := Application-root-URL / Org-path / Appl-path
[/ Right-path]

Application-root-URL := URL

Org-path := all | VKZ

VKZ := all | +CHAR

Appl-path := all | +CHAR

Right-path := all | +CHAR

Beispiele:

- a) https://awp.land.gv.at/at.gv.land.auditqry/
- b) https://awp.land.gv.at/at.gv.land.auditqry/all/
- c) https://awp.land.gv.at/at.gv.land.auditqry/all/all/
- d) https://awp.land.gv.at/at.gv.land.auditqry/all/all/all/
- e) https://awp.land.gv.at/at.gv.land.auditqry/gga-10101/all/all/
- f) https://awp.land.gv.at/at.gv.land.auditqry/all/at.gv.bmi.zmr/all/

(Ergebnisse der Anfragen im Anhang)

3.3.2 Response

Der Response ist im CSV-Format aufgebaut und mit dem MIME-Type text/csv entsprechend RFC 4180 auszugeben, die Zeichencodierung ist ISO-8859-15, das Format ist in EBNF-Schreibweise wie folgt aufgebaut:

```
Response := Kopfzeile *Datenzeile
Kopfzeile := "Name,UserID,Global Identifier,VKZ,ou,Organisationseinheit,Anwendung,Rechte" CR LF
Datenzeile := UserPortal "\", " Personenid Organisationszuordnung Anwendungsrechte
Personenid := Common-Name "\", " UserID "\", " Global-Id "\", "
Organisationszuordnung := "VKZ "\", " Organisationseinheit "\", "
Anwendungsrechte := Anwendung "\", " Rechte
```

Alle finalen Elemente der Datenzeile sind Strings im Format +CHAR

Es wird eine Zeile pro Permutation aus Benutzer, Organisationseinheit und Anwendung ausgegeben.

Rechteparameter sind im Format von gvRights laut der Spezifikation von LDAP-gv.at auszugeben.

Quoting laut RFC4180 ist anzuwenden wo erforderlich, sonst optional.

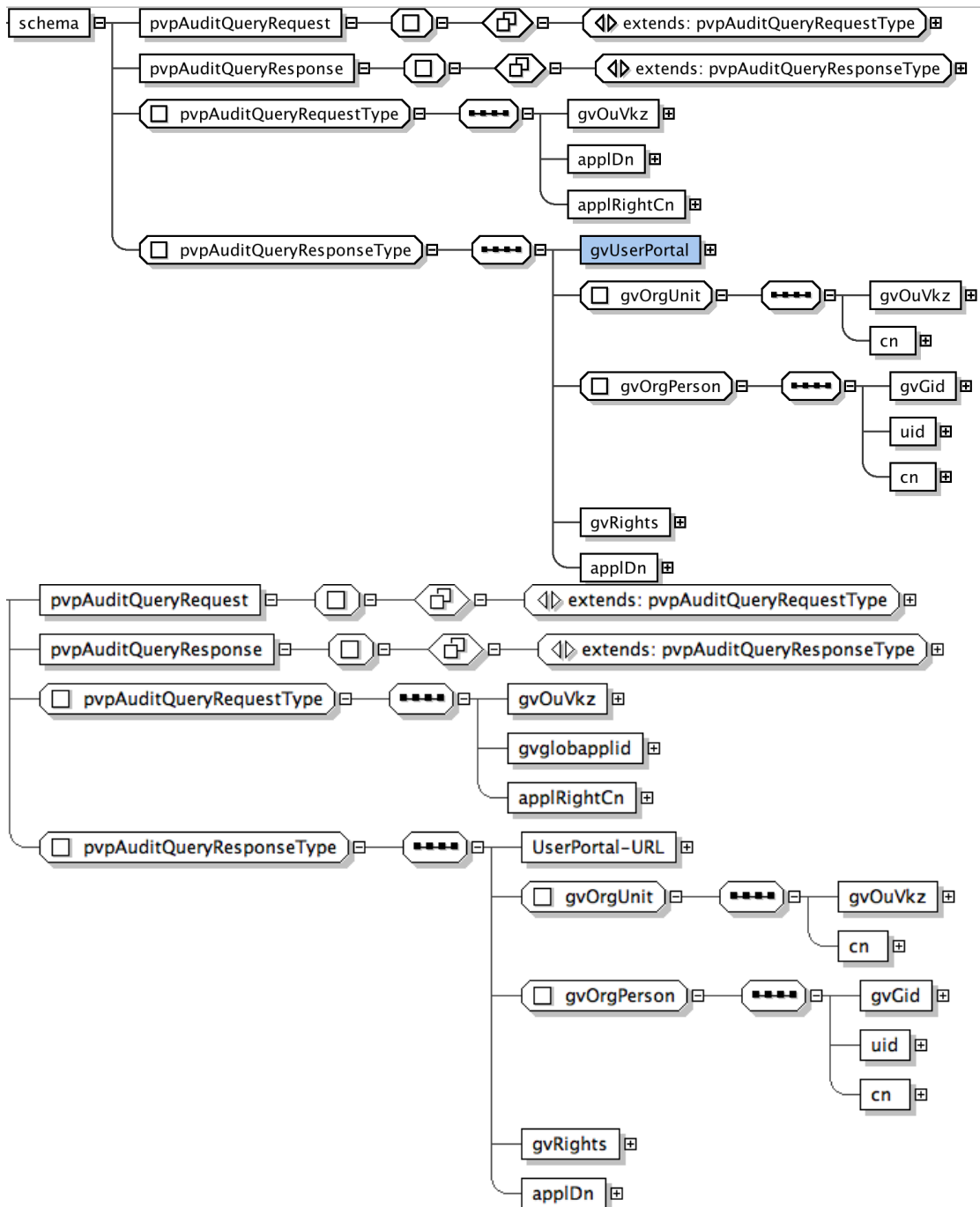
Zuordnung der Elemente zum Datenmodell LDAP-gv.at

<i>Revisionsabfrage</i>	<i>LDAP-gv.at</i>
UserPortal	URL des Stammportal
Common-Name	gvOrgPerson.cn
UserID	gvOrgPerson.uid
Global-Id	gvOrgPerson.gvGid
VKZ	VKZ der Organisation
Organisationseinheit	gvOrgUnit.cn
Anwendung	gvPrincipal.gvRights (Teilstring vor dem "\$" in verkürzter Schreibweise, nur Werte, durch "/" getrennt)
Rechte	gvPrincipal.gvRights (Teilstring nach dem "\$")

3.4 Zugriff über SOAP

Request und Response entsprechen in Funktion und Inhalt der Abfrage für Endbenutzer (->3.3). Das XML-Schema für SOAP Request und Response ist im Anhang (pvp-auditquery1.xsd) definiert.

Grafische Darstellung:



Im Request kann jeder Parameter den Wert "*" als Platzhalter für beliebige Werte enthalten.

3.5 Berechtigungsprüfung

Die Revisionsabfrage ist eine Anwendung am Anwendungsportal des Stammportalbetreibers, oder wird selbst als Anwendungsportal betrieben¹. Berechtigte Anwendungsverantwortlichen werden Rechte eingeräumt, damit diese Revisionsabfragen durchführen können.

Das Rechteschema dafür ist z.B. wie folgt definiert:

```
Anwendung "AuditQuery"
Recht "Revisionsabfrage(Anwendungsverantwortliche=<orgid>)"
```

3.6 GUI-Schnittstelle für Revisionsberechtigte

Im einfachsten Fall werden die Abfragen den Revisoren als Links zur Verfügung gestellt und können als Bookmarks gespeichert werden. Bei Bedarf kann eine Anwendung entwickelt werden, welche die Request-Parameter formulargesteuert aufbaut und absendet.

4 Anhang

4.1 Ergebnis der Beispiel-URLs

- a) <https://awp.land.gv.at/at.gv.landat.gv.land/auditquery/>
- b) Liste der zugriffsberechtigten Stellen, jeweils mit link auf die Anwendungen der zugriffsberechtigten Stelle.
- c) <https://awp.land.gv.at/at.gv.land/auditgry/all/>
- d) Liste der Anwendungen aller zugriffsberechtigten Stellen, jeweils mit link auf die Liste der Rechte der jeweiligen Anwendung.
- e) <https://awp.land.gv.at/at.gv.land/auditgry/all/all/>
- f) Liste der Rechte aller Anwendungen aller zugriffsberechtigten Stellen, jeweils mit link auf die Liste der Benutzer der jeweiligen Berechtigung.
- g) <https://awp.land.gv.at/at.gv.land/auditgry/all/all/all/>
- h) Liste aller berechtigten Benutzer.
- i) <https://awp.land.gv.at/at.gv.land/auditgry/gga-10101/all/all/>
- j) Liste aller berechtigten Benutzer der Gemeinde mit dem GKZ 10101.

¹ D.h., dass die Funktionalität des AWP in die Anwendung integriert ist.

- k) [https://awp.land.gv.at/at.gv.land/auditqry/all/gvaplid=zmr,ou=application,gvuid=at%3ab%3a112,dc=gv,dc=at /all/](https://awp.land.gv.at/at.gv.land/auditqry/all/gvaplid=zmr,ou=application,gvuid=at%3ab%3a112,dc=gv,dc=at/all/)
- l) Liste aller berechtigten Benutzer für das ZMR

