Spezifikation LDAP-gv.at für Portalverbund		**Konvention** **LDAP-gv.at_PV 1.6.2** **Ergebnis der Arbeitsgruppe**
Kurzbeschreibung	Spezifikation eines Datenmodells für Portalverzeichnisse. Dieses Dokument stellt eine Erweiterung zum Schema LDAP-gv.at dar.	
Autor(en):	Harald Hahn (LFRZ) Rainer Hörbe (Wien)	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:	Dietmar Gombotz, Peter Pichler, Peter Reif, Martin Spitzenberger	

Version 1.6.0 : ***31.1.2014*** *Abgelehnt von:*	*Fristablauf:* ***TT.MM.JJJJ*** (Länderangabe bei ablehnender Stellungnahme)
Unter-Version 1.6.1: ***20.04.2015***	*Fristablauf:* ***TT.MM.JJJJ*** (Länderangabe bei ablehnender Stellungnahme)
Unter-Version 1.6.2: **21.12.2017**	*Fristablauf:* ***TT.MM.JJJJ*** (Länderangabe bei ablehnender Stellungnahme)

(1) Inhaltsverzeichnis

(2) Einführung

Zweck dieses Datenmodells ist die Definition einer externen Sicht auf Daten von Portalen im Portalverbund. Die Quelle dieser Daten kann eine interne LDAP-Struktur oder ein RDBMS sein.

LDAP-gv.at-PV ist eine Erweiterung des LDAP.gv.at Schema und enthält jene Erweiterungen, die für den Portalverbund und den Betrieb von PVP Portalen benötigt werden.

(3) Anwendungsfälle

Diese Definition erweitert das LDAP-gv.at Schema um jene Datenelemente, die für den Betrieb von PVP Portalen notwendig sind. Die verschiedenen Profile mithilfe derer Stammportale / Identity Provider (STP/IdP) auf geschützte Ressourcen zugreifen können, sind in den PVP2 Spezifikationen festgelegt.

Anwendungsfälle AWP

Akteur	***Operation***
Stammportal	Fordert eine geschützte Ressource mittels PVP-R-Profil an
Stammportal	Schickt einen SAML Response mit Authentifizierungsinformationen über den angemeldeten Benutzer.

Anwendungsfälle STP

Akteur	***Operation***
User/Systemprincipal	Geschützte Ressource anfordern
User/Systemprincipal	Login/Logout (UserId/Passwort) durchführen
User/Systemprincipal	Login (HW-Zertifikat) durchführen
User Principal	Login (Kerberos) durchführen
User Principal	Passwort ändern
User Principal	Anwendungsliste anfordern
Revisor	Revisionsprotokoll anfordern

Anwendungsfälle Benutzer- und Rechteverwaltung

Akteur	***Operation***
Benutzer-Administrator	Rechte und Rechteparameter verwalten (aus der Sicht des Portals ist nur das Attribut gvPrincipal.gvRights relevant)
Benutzer-Administrator	Zertifikat importieren und zuordnen
Benutzer-Administrator	Zertifikat sperren
Benutzer-Administrator	Principal für Benutzer bzw. System einrichten (UserID, Startpasswort)
Benutzer-Administrator	Passwortsperre rücksetzen, neues Initial-Passwort vergeben
Benutzer-Administrator	Principal sperren/entsperren

Anwendungsfälle Portalverwaltung (AWP)

Akteur	***Operation***
AWP-Administrator	Neue Anwendung erstellen
AWP-Administrator	Anwendungsattribute ändern
AWP-Administrator	Anwendung vorübergehend sperren
AWP-Administrator	STP-Benutzer informieren (Banner-Msg)
AWP-Administrator	Anwendung stilllegen
AWP-Administrator	Anwendungsrechte administrieren
AWP-Administrator	Zugriffsberechtigte Stelle erstellen, Rechte verwalten
AWP-Administrator	Portal-Konfiguration ändern
AWP-Administrator	Zertifikat importieren und zuordnen
AWP-Administrator	Zertifikat sperren

Client-Zertifikate, die zur Authentifizierung am Portal verwendet werden, müssen registriert werden, um vom Client verwendet werden zu können.

Der Prozess der Registratur besteht darin, dass Attribute aus dem Zertifikat extrahiert und in das Verzeichnis importiert werden. Für die Registratur sind verschiedene Schnittstellen möglich: einzeln mit manueller Prüfung durch einen Benutzeradministrator, im Batch für mehrere User oder als Selbstregistratur für Inhaber von Zertifikaten mit Personenbindung.

Anwendungsfälle Portalverwaltung (STP)

Akteur	***Operation***
STP-Administrator	Neue Anwendung am Stammportal einrichten
STP-Administrator	Anwendung verwalten/entfernen
STP-Administrator	Stammportal definieren
STP-Administrator	Zuordnung zugriffsberechtigter Stellen zu Stammportal verwalten

(4) Struktur

(4.1) Verwaltungsdomänen

Der Verzeichnisdienst ldap.gv.at besteht aus einem zentralen und verschiedenen lokalen Verzeichnissen, die ein einheitliches Grundschema und optional lokale Erweiterungen haben. Das Verzeichnis ist in Verwaltungsdomänen unterteilt, die regeln, welche Organisationen und Anwendungsbereiche bestimmte Objekte pflegen.

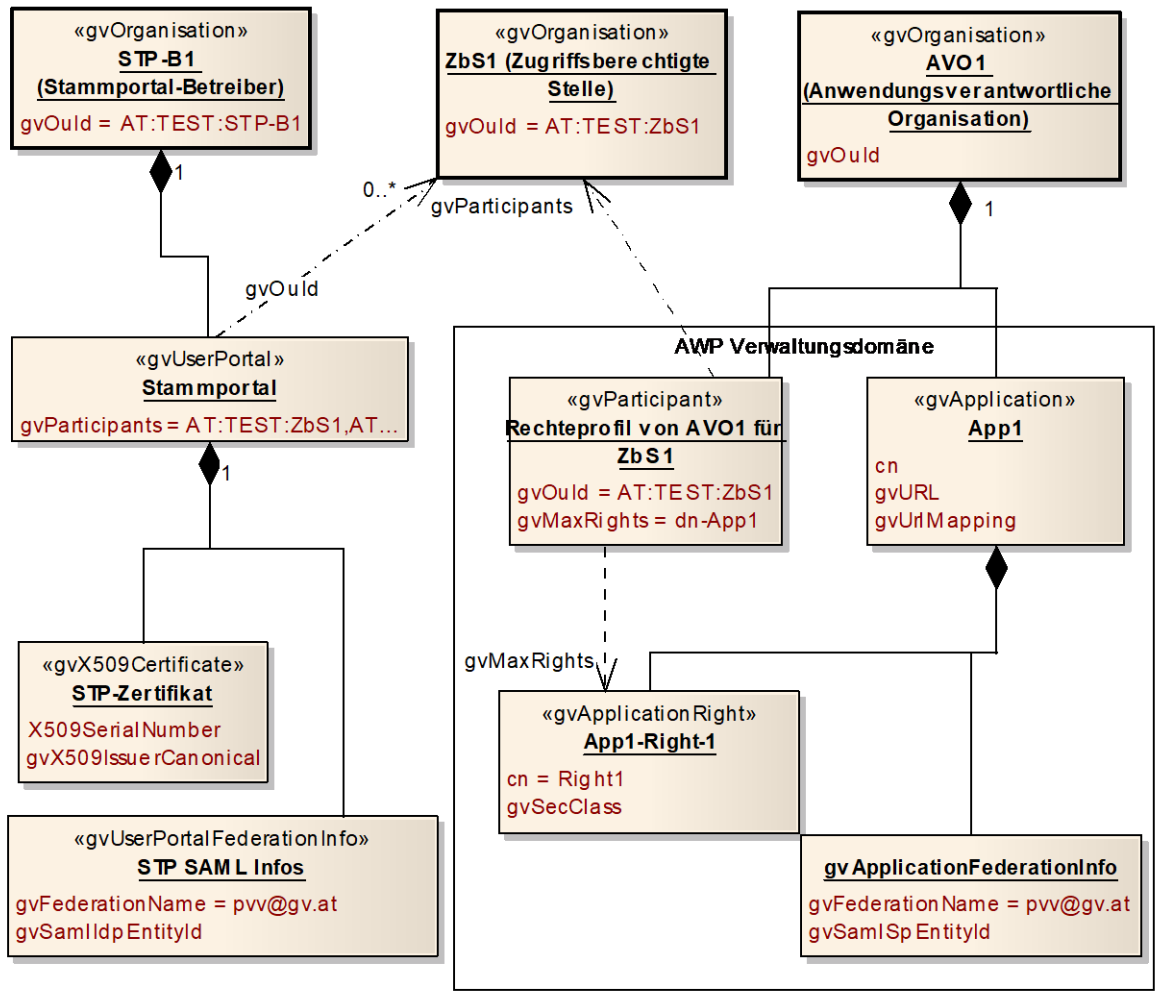
Lokale Verzeichnisse werden in der Regel sämtliche benötigten Daten lokal speichern, wobei die Daten fremder Verwaltungsdomänen über einen Replikationsmechanismus vom zentralen Verzeichnisdienst heruntergeladen werden können.

Verwaltungsdomänen sind:

- zentraler Verzeichnisdienst: führt die Liste der eigenständigen Organisationen von Bund, Ländern, Gemeinden, Städten, Selbstverwaltungskörpern etc.
- Stammportal: Objekte, die vom Stammportalbetreiber verwaltet werden. Die Benutzerverwaltung ist nicht Teil der Stammportalverwaltung.
- Anwendungsportal: definiert Anwendungen, deren Rechte, und die Delegation an zugriffsberechtigte Stellen.
- Personal: über Dienstverhältnisse werden Personen Organisationen zugeordnet.
- Konten- und Rechte: Benutzer- und Systemkonten enthalten Authentifizierungsinformationen und Berechtigungen

(4.2) Datenmodell aus Sicht eines Anwendungsportals

Folgendes UML Objektdiagramm gibt einen Überblick über die im Rahmen der Abarbeitung eines Zugriffs am Anwendungsportal benötigten LDAP Objekte:



AWP-Verwaltungsdomäne (benötigte Daten, für deren Wartung die anwendungsverantwortliche Organisation selbst zuständig ist)

Einrichten einer Anwendung

Wird eine Anwendung in ein Anwendungsportal integriert, muss sie mithilfe eines gvApplication Objektes beschrieben werden. Neben für den Portalbetrieb technisch notwendigen Angaben (z.B. Weiterleitungsregeln für den Reverse-Proxy Betrieb) werden Namen und Bezeichnungen festgelegt. Alle möglichen Rechte der Anwendung müssen mithilfe eines gvApplicationRight Objektes beschrieben werden. (Für die PVP-2-S-Profil Unterstützung gibt es ein zusätzliches neues Kindobjekt von gvApplication, gvApplicationFederationInfo – mehr dazu siehe (4.4) "PVP-2 – Unterstützung Multi-Federation / Unterstützte PVP Versionen und Profile").

Rechteprofile für zugriffsberechtigte Stellen einrichten

Für jede fremde Organisation, der Zugriff auf eigene Anwendungen eingeräumt werden soll, muss mithilfe eines gvParticipant Objektes ein Rechteprofil zugeordnet werden. Über Einträge des Attributes gvMaxRights muss (lt. PVV §5 Abs. 1) zu einer Organisation festgelegt werden, welche Rechte zugreifenden Personen aus der jeweiligen Organisation maximal gewährt werden.

Zentrale Verwaltungsdomäne (benötigte LDAP Daten, die von außen bezogen werden)

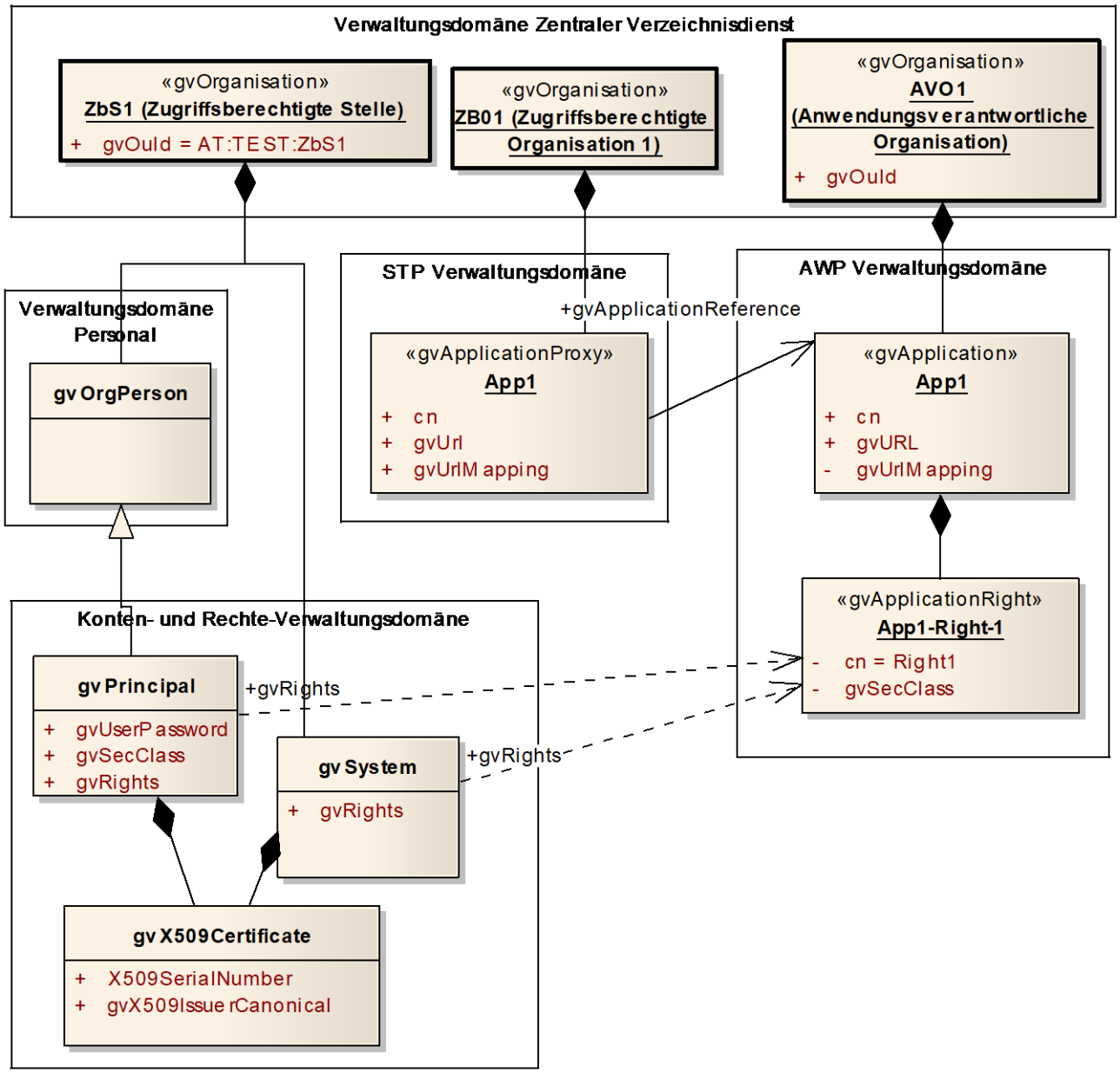
Identifikation des zugreifenden Portals

Bei einem Zugriff über das Reverse Proxy Profil muss das Zertifikat des zugreifenden Stammportals überprüft werden. Über Seriennummer und Zertifikats-Aussteller wird ein gvX509Certificate Objekt gefunden und so das zugreifende Stammportal festgestellt. Bei Zugriffen über SAML (S-Profil) erfolgt die Identifikation des zugreifenden Portals über die sogenannte Entity-ID (über die SAML Metadaten festgelegte, innerhalb einer Federation eindeutige ID für einen SAML Infrastruktur)

Prüfung der Zuständigkeit des zugreifenden Portals für die anfragende zugriffsberechtigte Stelle

Nicht jede zugriffsberechtigte Stelle betreibt ein eigenes Stammportal. Kleine Organisationen haben Verträge mit Dienstleistern, die den Stammportalbetrieb für sie erledigen. Zu einem Stammportal ist über das Listenattribut gvParticipants festgelegt, für welche zugriffsberechtigten Stellen berechtigterweise zugegriffen werden darf.

(4.3) Datenmodell aus Sicht eines Stammportals



Zentrale Verwaltungsdomäne

Basisdaten von Organisationen können verbundweit über das zentrale ldap.gv.at Verzeichnis ausgetauscht werden.

AWP Verwaltungsdomäne

Die Grunddaten für Anwendungen müssen von der anwendungsverantwortlichen Organisation bereitgestellt werden.

STP Verwaltungsdomäne

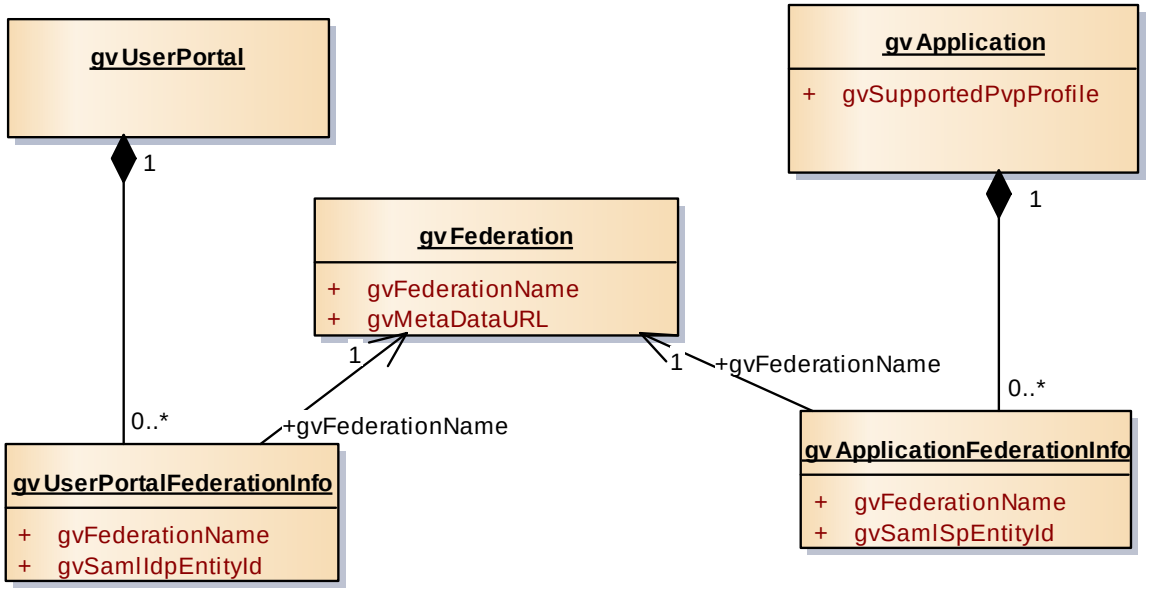
Zu den vom Anwendungsverantwortlichen gelieferten Informationen (gvApplication, gvApplicationRight) werden mithilfe von gvApplicationProxy Objekten stammportalspezifische Festlegungen für die jeweilige Anwendung getroffen.

Verwaltungsdomäne Personal / Konten- und Rechteverwaltungsdomäne

Userdaten werden typischerweise über Prozesse der Personalverwaltung gewartet. Über die Auxilliary-Klasse gvPrincipal kann ein gvOrgUser Objekt um portalspezifische Attribute (Portal-Passwort, Sicherheitsklasse, Rechte,…) erweitert werden.

(4.4) PVP-2 – Unterstützung Multi-Federation / Unterstütze PVP Versionen und Profile

Ldap.gv.at-PV erlaubt seit der Version 1.6 die Abbildung von Federations und die Festlegung unterstützter PVP Versionen und Profile. Diese Erweiterung ist für die Unterstützung von PVP 2.x erforderlich



Festlegung unterstützter PVP Versionen und Profile

Betroffene Attribute: gvUserPortal.gvSupportedPvpProfile, gvApplication.gvSupportedPvpProfile
Zu Stammportalen (gvUserPortal) und gvApplication Objekten kann mit dem Listenattribute gvSupportedPvpProfile angegeben werden, welche PVP-Profile in welchen Versionen unterstützt werden.

Definition Federation

Unter einer Federation versteht man eine Summe von Identity-Providern (Stammportalen) und Service-Providern (geschützte Anwendung), die sich gegenseitig vertrauen.
Ein Beispiel für eine Federation ist der Portalverbund der österreichischen Behörden. Ein anderes Beispiel ist die Infrastruktur einer Organisation, die als eine Federation gesehen werden kann. (Z.B. LFRZ-Federation für die IdPs und SPs der Land-, forst- und wasserwirtschaftliches Rechenzentrum GmbH)

Verwendete Federations müssen mit einem Eintrag des Typs gvFederation beschrieben werden.

Zuordnen von gvUserPortal und gvApplications zu Federations

Zu einer als SAML Service-Provider angebotenen gvApplication muss mithilfe von gvApplicationFederationInfo Objekten angegeben werden, in welchen Federations das Service angeboten wird und mit welcher Entity-Id der SP in den Metadaten der jeweiligen Federation bezeichnet wird.
Zu einem Stammportal, das als SAML IdP auftritt muss mit einer Instanz der Klasse gvUserPortalFederationInfo angegeben werden, in welchen Federations das Portal als IdP agiert und mit welcher Entity-ID der IdP in den Metadaten der jeweiligen Federation geführt wird.

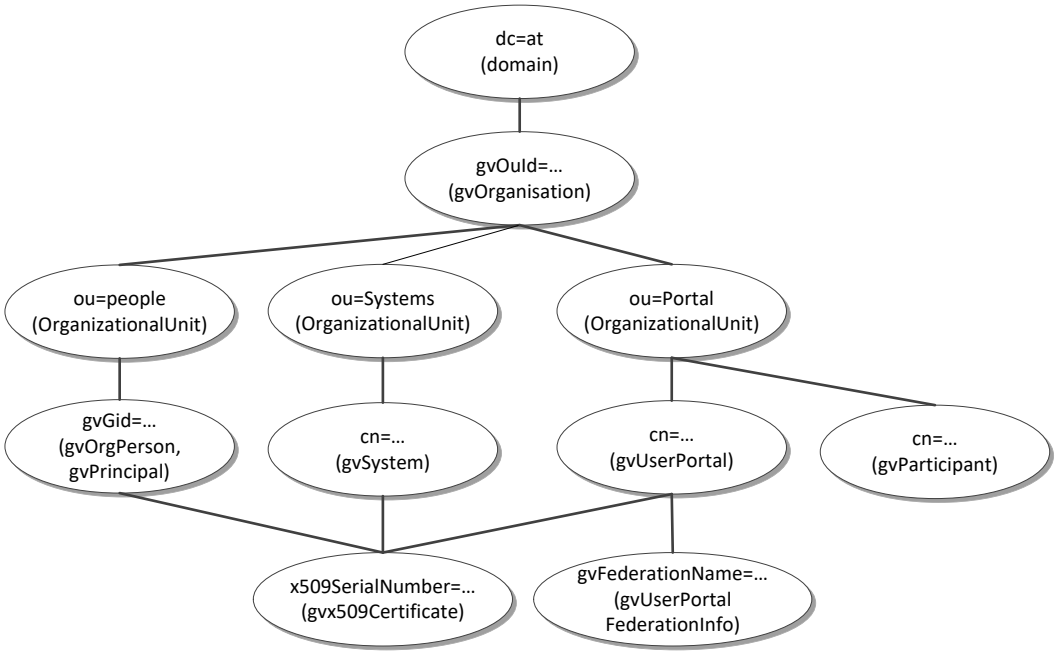
(4.5) Directory Information Tree (DIT)

Mit der Struktur des DIT wird die Vergabe von Zugriffsberechtigungen und Delegationspunkten für die physische Verteilung (Referrals) unterstützt. Die verschiedenen Informationen werden immer innerhalb jener gvOrganisation verwaltet, die für die Verwaltung zuständig ist.

Folgende Diagramme stellen dar, wie die Objekte in Abhängigkeit von ihren Klassen im DIT positioniert werden.

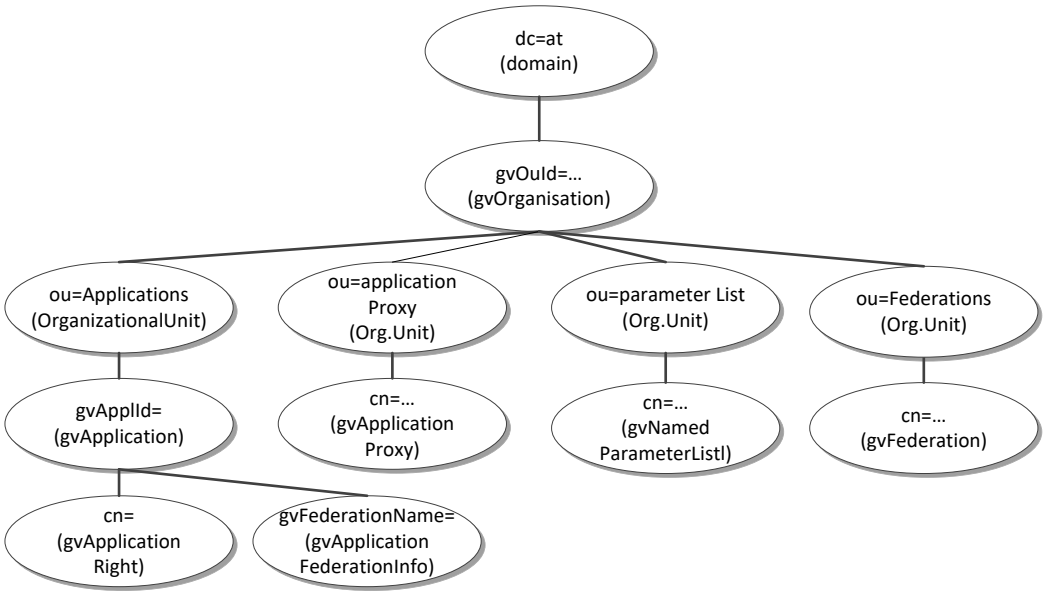
Benutzer, Portale und zugriffsberechtigte Stellen

Folgendes Diagramm zeigt, wo im LDAP Baum Informationen über Benutzer (Personen - gvOrgPerson, Systembenutzer – gvSystem), Stammportale (gvUserPortal, gvx509Certificate, gvUserPortalFederationInfo) und Rechteprofile für zugriffsberechtigte Stellen (gvParticipant) positioniert sind:



Anwendungen, Rechte, Parameterlisten und Federations

Folgendes Diagramm zeigt, wo die Anwendungsdefinition der Anwendungsverantwortlichen (gvApplication, gvApplicationRight, gvApplicationFederationInfo, gvNamedParameterList), anwendungsspezifische Informationen eines Stammportals (gvApplicationProxy) bzw. die Beschreibung einer Federation (gvFederation) zu finden sind:



(5) LDAP Klassen

LDAP-gv.at_PV setzt eine Implementierung des Schemas LDAP-gv.at für Organisationsverzeichnisse voraus. Die Klassen gvOrganisation und gvOrgPerson sind hier zum besseren Verständnis angeführt, verweisen jedoch auf die Spezifikation LDAP-gv.at.

Für alle Klassen gelten außerdem die folgenden allgemeinen Attribute aus LDAP-gv.at:

- createTimestamp,
- modifyTimestamp,
- gvStatus,
- gvSource,
- gvScope,
- gvExtensionItem

gvApplication	Anwendung, wie sie im Anwendungsportal definiert ist.	
dn: gvApplId=...,ou=Applications, .. *(dn: gvApplId=ZMR,ou=Applications,gvOuId=AT:B:999,dc=at)*		
Attribut	**Beschreibung (Beispiel)**	**Eigen-schaft**
gvApplId	Anwendungskennung – bestehend aus druckbaren ASCII Zeichen exclusive BACKSLASH (\) und SPACE ( ). Eine Anwendung wird eindeutig über den DN referenziert, wie z.B. in gvApplicationReference. *(MAW, MAW@org.gv.at, AT.GV.ORG.MAW2-P)*	M, ia5(64)
cn	Name der Anwendung *(Musteranwendung)*	M, L, cis(64)
gvURL	Startadresse der Anwendung im Anwendungsportal (=Zieladresse des Stammportals) *(https://myportal.gv.at/at.gv.myorg.app1/start/)*	S, ces
gvURLMapping	Wenn auf die tatsächliche Anwendung über das R-Profil zugegriffen wird, definiert gvURLMapping die Weiterleitungsregeln für den Reverse-Proxy. Aufbau von gvUrlMapping Einträgen siehe Beschreibung unterhalb der Tabelle */at.gv.myorg.app1/|https://10.0.0.1/at.gv.myorg.app1/|check*	L, ces(1024)

gvSupported PvpProfile	PVP Versionen und Profile mit denen das Service angeboten wird. **Syntax:** gvspp ::= PvpVersion „_" RorS_Profile PvpVersion::= "1.8" | "1.9" | "2.1" RorS_Profil ::= "R"|"S" **Beispiele:** 1.8_R 1.9_R 2.1_R 2.1_S	L, cis(1024)
gvApplicationGroups	Für die Gruppierung von zusammengehörigen Anwendungen. (zur Erleichterung von Dokumentation und statistischen Auswertungen)	L, cis
description	Anwendungsbeschreibung	L, cis(1024)
gvBanner	Textnachricht, die Benutzern im Stammportal-Menü zusätzlich zum Namen und Logo der Anwendung angezeigt wird. Kann z.B. verwendet werden um auf Wartungsfenster oder ähnliche betriebsrelevante Sachverhalte hinzuweisen.	cis(1024)
gvApplicationDocumentationURL	URL unter der die Anwendungsdokumentation zu finden ist.	cis
gvAppOwner	Anwendungsverantwortlicher (URL)	cis
gvAppTechContact	technischer Kontakt (URL)	cis
gvAppAdmin	administrativer Kontakt (URL)	cis
jpegPhoto	Applikationslogo. Empfohlene max. Größe: 20 x 60 Pixel.	L, JPEG
gvMaxConcurrent Requests	Maximale Anzahl gleichzeitiger Anfragen für diese Applikation. Ein Anwendungsportal soll Anfragen sofort zurückweisen, wenn dieser Wert überschritten wird. 0… Anzahl gleichzeitiger Anfragen soll nicht limitiert werden. Diese Konfigurationsmöglichkeit hat den Zweck, andere vom selben Anwendungsportal angebotene Anwendungen, trotz Überlastung einer Anwendung, verfügbar zu halten.	int
gvApplicationStatus	Status der Verfügbarkeit: on-line, off-line; off-line bedeutet, dass die Anwendung vorübergehend außer Betrieb ist, gvStatus muss daher active sein. Wenn das Attribut fehlt oder leer ist, ist das als on-line zu interpretieren.	cis[8]

gvDecommissionDate	Stilllegungsdatum. Wenn das Datum gesetzt ist, muss gvStatus inactive sein. Der Eintrag ist frühestens 3 Jahre nach der Stilllegung zu löschen.	Generalized Time
gvMaxSecClassAllow	Gibt an, ob Portale, die das Attribut gvMaxSecClass gesetz haben, zugreifen dürfen: false… default, kein Zugriff von Portalen mit gvMaxSecClass true… Zugriff von Portalen mit gvMaxSecClass erlaubt	Bool

gvURLMapping
Jeder Eintrag enthält eine Abbildungsregel von Quell- auf Zieladressen, und Attribute, die den Adressbereich genauer beschreiben. (Berechtigungsprüfung erforderlich, PVP-SOAP oder PVP-http,...). Die Syntax ist:

gvUrlMapping::= SourceURL „|" TargetURL „|" Check-Option [„|" Root-Cookie-Option] [„|" Protocol-Option]

Erläuterung:

- SourceURL… absolute bzw. serverrelative (führendes Slash) URL
- TargetURL….absolute URL
- Check-Option::= „check" | „nocheck" | "optional"

Mit "check" wird festgelegt, dass der URL-Bereich der Zugriffsprüfung des Portals unterliegt. Nur authentifizierte und autorisierte Benutzende dürfen zugreifen.

"nocheck" bedeutet, dass für Ressourcen in diesem Adressbereich keine Zugriffsprüfung durchgeführt wird. Es handelt sich um einen öffentlich verfügbaren Teil der Anwendung.

Mit "optional" wird festgelegt, dass auch ohne Anmeldung bzw. spezielle Berechtigung auf den URL-Bereich zugegriffen werden kann. Rechte werden nur dann gemeldet, wenn diese explizit zugeordnet wurden. Wird authentifiziert ohne explizite Rechte zugegriffen, werden PVP-Header mitgeschickt aber keine Rechte. Nicht authentifizierte Zugriffe werden ohne PVP-Header zum Zielserver weitergeleitet.

- Root-Cookie-Option::= „root"

Wird die Root-Cookie-Option („|root") angegeben, so wird der Pfad von Set-Cookie Kommandos der Zielanwendung von Root-Cookies auf den Pfad der SourceURL geändert. Root-Cookies sind Cookies mit dem Pfad „/". Wird die Option weggelassen, so wird das URL-Mapping nicht für das Ändern des Pfades von Root-Cookies verwendet. (Anm: Verwendet eine Anwendung Root-Cookies als Session-Cookie, kann es vorkommen, dass die parallele Benutzung zweier Anwendungen über dasselbe Stammportal nicht möglich ist, da die Anwendungen denselben Cookie-Namen für das Session-Cookie verwenden. Mithilfe der Root-Cookie-Option kann dieses Problem gelöst werden)

- Protocol-Option::= "pvphttp" | "pvpsoap"

Das Trennzeichen ist das Zeichen "Vertical Bar". Mithilfe dieser Option kann festgelegt werden, ob die PVP-Header als http-Header oder als SOAP-Header an den Zielserver weitergegeben werden sollen.

Wird die Option weggelassen so wird folgende Regel angewendet, um zu bestimmen, welches Protokoll verwendet werden soll:

- Um das Protokoll zu bestimmen, wird das URL-Mapping mit der längsten passenden Source-URL verwendet, bei dem eine Protocol-Option angegeben ist. (Analog zu „Suchen von gvURLMapping Einträgen mithilfe der SourceURL")
- Gibt es kein passendes URL-Mapping mit Protocol-Option so ist für alle Anfragen, deren Pfad mit „/soap" beginnt, PVP-SOAP zu verwenden - anderenfalls PVP-http.

Suchen von gvURLMapping Einträgen mithilfe der SourceURL

Um für eine URL aus der Anfrage des Clients den passenden gvUrlMapping Eintrag zu finden, wird wie folgt vorgegangen:

1. Es wird eine Liste mit gvURLMapping Einträgen zusammengestellt, deren SourceURL linksbündig mit der URL aus der Client Anfrage übereinstimmt. Wenn mithilfe der absoluten URL keine passenden gvUrlMapping Einträge gefunden werden, wird nach Einträgen gesucht, deren Source URL linksbündig mit der serverrelativen URL übereinstimmt.
2. Aus der in Schritt 1 erstellten Liste wird das gvURLMapping mit der längsten SourceURL ausgewählt.

Suchen von gvURLMapping Einträgen mithilfe der TargetURL

Um eine URL aus der Zielserver Antwort (z.B. Ziel URL eines Redirects) für den Client zu übersetzen, wird wie folgt vorgegangen:

Es wird eine Liste aus gvURLMapping Einträgen zusammengestellt, deren TargetURL linksbündig mit der URL aus der Server Antwort übereinstimmt. Aus dieser Liste wird das gvURLMapping mit der längsten TargetURL ausgewählt.

gvApplication FederationInfo	gvApplicationFederationInfo Mit Elementen dieses Types wird für eine gvApplication festgelegt, in welchen Federations die Anwendung angeboten wird.

dn: gvFederationName=..,ou=Federations,..
(dn: gvFederationName*=PVV@gv.at,ou=Federations, gvouid=AT:B:112,dc=at)*

Attribut	**Beschreibung (Beispiel)**	**Eigen-schaft**
gvFederationName	*Referenziert jene gvFederation in der die Anwendung angeboten werden soll*	M, cis(1024)
gvSamlSpEntityId	SP-Entity-ID (Eindeutige Kennung) der Anwendung in den Metadaten der durch gvFederationName bezeichneten Federation	L, cis(1024)

gvApplicationProxy	Anwendungsspezifische Informationen für Stammportale. Das Objekt ist ein Stellvertreter für den Eintrag der Anwendung im Anwendungsportal

dn: cn=...,ou=ApplicationProxy,..
(dn: cn=zmr@bmi.gv.at,ou=ApplicationProxy,gvOuId=AT:B:999,dc=at)

Attribut	**Beschreibung (Beispiel)**	**Eigen-schaft**
cn	Eindeutige Bezeichnung in der Form: Application-ID "@" Domainname *(app1@myorg.gv.at)*	M, L, cis(64)
gvApplicationReference	dn der zugehörigen gvApplication Instanz in kanonisierter Schreibweise *(gvApplId=app1@myorg.gv.at,ou=Applications,gvOuId=AT:B:999,dc=at)*	dn
gvURL	URI, Anwendungsadresse im Stammportal. Wird vom Stammportal als Zieladresse für den der Anwendung zugeordneten Menülink verwendet. Die URI kann absolut oder relativ angegeben werden. *(https://myportal.gv.at/at.gv.myorg.app1/start /at.gv.myorg.app1/start)*	uri
gvURLMapping	Informationen für URL Mapping im Stammportal. Analog zu gvApplication.gvUrlMapping /at.gv.myorg.app1/|https://myawp.gv.at/at.gv.myorg.app1/|check*)*	L, ces(1024)
gvOpenWindow	Steuert, ob eine Anwendung in einem neuen Browserfenster geöffnet wird. Dieses Attribut wird ignoriert, wenn gvOpenWindowJavaScript nicht leer ist.	bool
gvOpenWindowJavaScript	Syntax: String Beschreibung: Dieser JavaScript-Code öffnet das Anwendungsfenster, wenn die Anwendung im Menü	ces

	ausgewählt wird. Dadurch können Parameter wie die Fenstereigenschaften angegeben werden. *self.child=window.open("start.htm","ZMR", "resizable=yes, status=yes");* *if(self.child!= null) {* *if (self.child.opener==null)* *self.child.opener = self;* *self.child.moveTo(0,0);* *self.child.resizeTo(((screen.width > 1024)?1024:screen.width),* *((screen.height > 768)?768:screen.height));* *self.child.focus();* *}*	
gvValidVHosts	Liste von DNS-Namen (virtuelle Hostnamen des Stammportals) Enthält diese Liste Einträge, so gilt dieses gvApplicationProxy-Objekt nur für Stammportal-Anfragen an einen der hier konfigurierten virtuellen Hostnamen des Stammportals. Ist die Liste leer, so ist das Objekt unabhängig vom verwendeten Hostnamen gültig.	L, ces
gvHideMenuitem	Steuert die Anzeige von Anwendungen im Menü. Attribut nicht vorhanden oder false.. zeigt Menüeintrag an true... Menüeintrag wird nicht angezeigt	Bool

gvApplicationRight	Rechte und deren Parameter für Objekte der Klassen gvOrgPerson, gvPersonFunction (s. [LDAP-gv.at])	
dn: cn=…,gvApplId=…,ou=Applications,.. *(cn=ZMR-Anfrage,gvApplId=ZMR,gvOuId=AT:B:999,dc=at)*		
Attribut	**Beschreibung (Beispiel)**	**Eigen-schaft**
~~gvApplId~~ (deprecated)	~~Wie in gvApplication~~ Dieses Attribut wurde mit Version 1.6.2 als veraltet/deprecated erklärt. Es gilt der Wert, der übergeordneten gvApplication.	~~M, cis(32)~~
cn	Bezeichnung der Berechtigung	M, L, cis(64)
gvSecClass	0 bis 3 Mindestens erforderliche SecClass für dieses Recht (siehe [SecClass]). SecClass ist nur dort zu setzen und von Bedeutung, wo es in der Sicherheitsvereinbarung (gvLegalContract) definiert ist.	int(1)
gvRoleSyntax	Regulärer Ausdruck in PERL-Syntax, um Rechteparameter zu überprüfen. Dieses Attribut ist für die Rechteprüfung im Anwendungsportal vorgesehen. Eine im PVP-Token übergebene Parameterliste zu einem Recht muss mit einem regulären Ausdruck der Liste einen Treffer erzeugen. Diese Prüfung eröffnet die Möglichkeit das Vorhandensein von Rechteparametern zu erzwingen oder zu verhindern. Beispiel: *(GKZ=|d{5,5})(,GKZ=|d{5,5})** Das bedeutet, dass mindestens ein Key-Value-Pair vorhanden sein muss, wobei der Key "GKZ" ist und Value eine 5-stellige Ganzzahl. Mithilfe dieses regulären Ausdrucken können Formatvorgaben für Rechteparameterwerte definiert werden (z.B. nur nummerische Werte)	L, ces(1024)
gvRightsCodomain	Definiert zulässige Rechteparameter. Jeder Eintrag repäsentiert eine mögliche Kombination von Parametern. (siehe auch Beispiele weiter unten) Die Syntax für einen gvRightsCodomain Eintrag ist weiter unten angeführt. Die Reihenfolge von PVP-Parametern ist beliebig. Es dürfen keine zwingenden Reihenfolgen aus gvRightsCodomain Definitionen abgeleitet werden. Details zur Bedeutung und Beispiele siehe unten	L, ces(1024)
gvSingularRight	Default: TRUE	bool

	Gibt an, ob das Recht der Vorgabe "Kumulierbarkeit und Separierbarkeit von Parameter" aus der Konvention "Rechtemodellierung für Portalanwendungen (PVRechte 1.0.0)" entspricht. Portale bzw. die Benutzerverwaltungen der Portale SOLLEN solche Rechte kumulieren. (Zu einem Recht zusammenfassen und die Parameter aneinanderhängen)	
gvDecommissionDate	siehe gvApplication	Generalized Time
description	Beschreibung	L, cis(1024)

gvRightsCoDomain

Dieses Attribut definiert die Syntax für Rechteparameter. Der Wert „NONE" gibt an, dass keine Rollenparameter angegeben werden dürfen. Ansonsten muss eine Liste von Parameterbeschreibungen definiert werden. Eine Parameterbeschreibung besteht aus einem Parameternamen aus Kennzeichen für Pflicht- bzw. Mehrfachparametern und einer durch ein „=" getrennten Definition der möglichen Parameterwerte. Nach dem Parameternamen kann durch Angabe von „+" erklärt werden, dass der Parameter mehrmals vorkommen darf, durch Angabe von „§" wird definiert, dass der Parameter befüllt werden muss. Nach dem Parameternamen wird eine Liste mit möglichen Parameterwerten definiert. In dieser Liste können zwei verschiedene Arten von Sonderfällen vorkommen: Der Wert „…" legt fest, dass eine freie Eingabe möglich sein soll. Ein in eckige Klammer eingeschlossener Wert (z.B. [GKZ@AT:B:112]) legt fest, dass an dieser Stelle die Werte einer benannten Parameterliste eingefügt werden sollen. Jede dieser drei Möglichkeiten (Parameterwert, freie Eingabe, Listenreferenz) ist sowohl für sich als auch in Kombination mit den anderen Möglichkeiten gültig. Jeder Parametername kann nach der Werteliste mit einer Beschreibung versehen werden.

Eine Referenz auf eine Parameterliste wird aufgelöst, indem global (im gesamten Directory-Tree) nach einem Objekt vom Typ gvNamedParameterList gesucht wird, dessen Attribut cn dem angegebenen Namen entspricht. Alle Einträge des Attributes gvParameterListValues der gefundenen Objektes sind mögliche Werte für den Rechteparameter.

Wenn mögliche Parameterwerte oder deren Beschreibung eines der folgenden Zeichen enthalten, so muss dieses durch Voranstellen eines $ Zeichens kodiert werden:

Zeichen	Beschreibung
,	Beistrich; Kodierung $,
(	Öffnende runde Klammer; Kodierung: $(
)	Schließende runde Klammer; Kodierung: $)
[	Öffnende eckige Klammer; Kodierung: $[
]	Schließende eckige Klammer, Kodierung: $]
$	Dollar-Symbol; Kodierung $$
.	Punkt; Kodierung $.
{	Öffnende geschwungene Klammer; Kodierung: ${
}	Schließende geschwungene Klammer; Kodierung: ${

Kodierungsbeispiel

Eine Parameterliste (a$,,b$),c$[,d$.$.$.,e$$) bedeutet, dass „a," „b)" „c[" „d…" und „e$" mögliche Parameterwerte sind.

Syntax

```
gvRightsCodomain := parameterList | "NONE"
    // NONE->Keine Parameter.
parameterList := parameter [";" parameterList]
parameter := paramKey ["+"] ["§"] "=" tokenList ["," description]
    // "+"…Der Parameter kann mehrfach vorkommen
    // "§"…Der Parameter muss angegeben werden.
paramKey := +CHAR
description := "desc=" QUOTE descriptionText QUOTE
descriptionText := +CHAR
tokenList := "(" tokenItems ")"
tokenItems := token ["," tokenItems] | "…"
    /// "…" beliebiger Wert
token := "[" reference "]" | +ILCHAR ["{" value-description "}"]
value-description ::= +CHAR
reference := namedParamterListName "@" gvOuId
parameterListName := +CHAR
gvOuId := +CHAR
ILCHAR.::= <druckbares ISO-Latin Zeichen nach ISO8859-15; dezimal
33-126 und 168-255>
CHAR.::= <druckbares ASCII Zeichen dezimal 33-126>
```

Bespiele für gvRightsCoDomain

1. Als Rollenparameter ist gvOuId mit beliebigen Werten erlaubt (optional):

   ```
   gvOuId=(…)
   ```

2. Als Rollenparameter ist ein Bundesland in Form einer GKZ anzugeben (mandatory):

   ```
   GKZ§=(10000, 20000, 30000, 40000, 50000, 60000, 70000, 80000,
   90000)
   ```

3. Als Parameter können mehrere akademisch Titel angegeben werden:

   ```
   Titel+=(DI,Mag,Dr,…)
   ```

4. Kombination von Angaben; es kann eine OuId und es muss ein Bundesland angegeben werden

   ```
   gvOuId=(…);
   GKZ§=(10000,20000,30000,40000,50000,60000,70000,80000,90000),
   desc="Gemeindekennzahl Bundesland"
   ```

5. Kein Rollenparameter erlaubt

   ```
   NONE
   ```

6. Verwendung von benannten Parameterlisten; Als Parameterwert für den verpflichtend anzugebenden Parameter „GKZ" kann entweder der String „unbekannt" oder ein Wert aus der mit dem Namen „GKZ@AT:B:112" gvNamedParameterList Objekt verwendet werden.

   ```
   GKZ§=(unbekannt,[GKZ@AT:B:112])
   ```

7. Beschreibung von Parameterwerten

   ```
   GKZ+=(10000{Burgenland},20000{Kärnten},30000{Niederösterreich})
   ```

gvFederation	Unterstütze Federations müssen mithilfe dieser Klasse beschrieben werden Instanzen dieser neuen Objektklasse sollen unterhalb der neu eingeführten OrganizationalUnit (ou=Federations) geführt werden.	
dn: gvFederationName=..,ou=Federations,.. *(dn:* gvFederationName*=PV_PVV@gv.at,ou=Federations gvouid=AT:B:112,dc=at)*		
Attribut	**Beschreibung (Beispiel)**	**Eigen-schaft**
gvFederationName	Eindeutige Bezeichnung einer Federation im E-Mail-Adressen Format nach RFC 822 beziehungsweise als DNS Name. Das Zeichen SLASH darf nicht verwendet werden. *Für den Portalverbund der österreichischen Behörden gem. Portalverbundvereinbarung ist als gvFederationName der Wert portalverbund.gv.at festgelegt.* *Organisationsinterne Federations SOLLEN mit "intern@" + Domain-Name der Organisation. (z.B. intern@lfrz.at) bezeichnet werden.*	M, cis(1024)
gvMetaDataURL	Bezugspunkt für Metadaten dieser Ferderation	L, cis(1024)

gvNamedParameterList	Benannte Parameterliste Mögliche Werte für Rechteparameter	
dn: cn=...,ou=parameterLists, .. *(dn: cn=GKZ@AT:B:112,ou=parameterLists,gvOuId=AT:B:112,dc=at)*		
Attribut	**Beschreibung (Beispiel)**	**Eigen-schaft**
cn	Global eindeutige Kurzbezeichnungen der Liste im Format Listenname '@' gvOuId Durch die Angabe der gvOuId im Listennamen soll die Eindeutigkeit des Listennamens gewährleistet werden. (*GKZ@AT:B:112*)	M, L, cis(64)
gvParameter ListValues	Jeder Eintrag beschreibt einen möglichen Wert für einen Rechteparameter. Optional kann für jeden einzelnen Parameterwert eine Beschreibung angegeben werden. Syntax eines Eintrages der Liste: `possibleValue ["{"description"}"]` possibleValue...druckbares ISO-Latin (ISO8859-15; decimal 33-126 und 168-255) description... Beschreibungstext Die zu gvRightsCodomain angegebenen Kodierungsvorschriften für Sonderzeichen sind auch hier einzuhalten. Es ist zu beachten, dass die PVP Spezifikation für Parameterwerte nur druckbares ISO-Latin zulässt (ISO8859-15; decimal 33-126 und 168-255). *(gvParameterListValues: 10000{Burgenland}* *gvParameterListValues: 20000{Kärnten}* *gvParameterListValues: 30000{Niederösterreich})*	L, ces(128)
description	Lesbare Langbezeichnung der Liste (z.B. „Gemeindekennzahlen; 5 nummerische Stellen, gem. der Definition der Statistik Austria")	L, ces(32767)

gvParticipant	PV (Sub-) Teilnehmer. Dient zur Rechteverwaltung von zugriffsberechtigen Stellen in Anwendungsportalen.	
dn: cn=..,ou=Portal,.. *(dn: cn=klosterneuburg@noel.gv.at,ou=Portal,gvOuId=AT:B:112,dc=at)*		
Attribut	**Beschreibung (Beispiel)**	**Eigen-schaft**
cn	Bezeichnung der zugriffsberechtigen Stelle im RFC822-Format *(klosterneuburg@noel.gv.at)*	M, L, cis(64)
gvOuId	gvOuId (siehe gvOrgUnit.gvOuId) der zugriffsberechtigten Stelle (Participant; siehe auch Begriffsbestimmung PVP) *(gvOuId= AT:l9:9876)*	M, cis(32)
gvMaxRights	Definiert die maximal zulässigen Rechte eines Portalverbund(-)teilnehmers. Jeder Eintrag definiert eine Menge zugestandener Rechte (siehe auch Beispiele weiter unten). Es gibt verschiedene Formate für gvMaxRights-Einträge: **Format 1: „.*"** Ist zu einem gvParticipant „.*" als gvMaxRight eingetragen, so darf der Teilnehmer alle Anwendungen des Anwendungsportals mit beliebigen Parametern benutzen. Weitere Einträge in gvMaxRights sind nicht sinnvoll. **Format 2: dn-gvApplication** Ist der dn eines GvApplication Objektes eingetragen, so darf der Teilnehmer alle Rechte dieser Anwendung mit beliebigen Parametern benutzen. **Format 3: dn-gvApplicationRight „$.*"** Ist ein gvMaxRights-Eintrag, der aus dem DN eines GvApplicationRight-Objektes gefolgt vom String „$.*" vorhanden, darf das Recht mit beliebigen Paramtern verwendet werden. (auch ohne Parameter) *(cn=ZMR-Anfrage,gvApplId=ZMR,gvOuId=AT:B:112,dc=at$.*)* *(ZMR-Anfrage kann mit beliebigen Parametern verwendet werden)* **Format 4: dn-gvApplicationRight „$" [paramName „=" roleSyntax]** dn-gvApplicationRight… dn des ApplicationRights, welches für die zugriffsberechtige Stelle zulässig ist. (Es kann mehrere gvMaxRights Einträge mit demselben GvApplicationRight-DN geben.) roleSyntax… regulärer Ausdruck in PERL-Syntax, der *einen* möglichen Parameterwert ausdrückt. Ist keine roleSyntax definiert, kann das Recht ohne Parameter verwendet werden. *(cn=ZMR-Anfrage,gvApplId=ZMR,gvOuId=AT:B:112,dc=at$GKZ=47111)*	L, ces(32767)

	(Für die zugriffsberechtige Stelle ist "ZMR-Anfrage(GKZ=47111)" zulässig)	
description	Entsprechend gvOrgPerson	L, cis(1024)

Beispiele für gvMaxRights

cn=test,gvApplId=localtest,ou=Applications,gvOuId=AT:TEST:1,DC=AT$x=.+

Für den Parameter x, des Rechtes test der Applikation "localtest" darf der Participant beliebige, zumindest ein Zeichen lange Werte verwendet werden.

cn=test,gvApplId=localtest,ou=Applications,gvOuId=AT:TEST:1,DC=AT$GKZ=9|d|d|d|d

Der Participant darf als Parameter für das Recht "test" mit "9" beginnende, numerische, fünfstellige Gemeindekennzahlen verwenden

cn=test,gvApplId=localtest,ou=Applications,gvOuId=AT:TEST:1,DC=AT$

Der Portalverbundteilnehmer darf das Recht "test" der Anwendung "localtest" verwenden, ohne Parameter anzugeben. Ist kein solcher Eintrag vorhanden, darf das Recht nicht ohne Parameter verwendet werden.

*cn=test,gvApplId=localtest,ou=Applications,gvOuId=AT:TEST:1,DC=AT$.**

Der Portalverbundteilnehmer darf das Recht "test" der Anwendung "localtest", mit beliebigen Parametern verwenden. Die möglichen Parameter können aber zusätzlich durch gvApplicationRight.gvRoleSyntax beschränkt sein.

gvApplId=localtest,ou=Applications,gvOuId=AT:TEST:1,DC=AT

Der Teilnehmer darf auf die Anwendung „localtest" mit beliebigen Rechten und beliebigen Parametern zugreifen

*.**

Der Portalverbundteilnehmer darf auf alle Anwendungen mit beliebigen Rechten und Parametern zugreifen

gvPrincipal	Auxiliary Klasse als Erweiterung für gvOrgPerson, um für das Stammportal relevante Informationen abzulegen.	
Attribut	**Beschreibung (Beispiel)**	**Eigen-schaft**
gvPassword MustChange	1…Der Benutzer muss beim nächsten Login sein Passwort ändern. 0…Benutzer muss beim nächsten Login sein Passwort nicht ändern.	bool
gvPasswordExp	Beschreibt ob die Gültigkeit eines Passworts verfällt 1 – Gültigkeit Passwort ist zeitlich begrenzt (verfällt nach der letzten Änderung zuzüglich passwordMaxAge) 0 – Passwort ist ohne zeitliche Begrenzung gültig	bool
gvPassword History	Beschreibt verwendete Passwörter und deren Ablaufdatum im Format: YYYYMMDDHHMMSS{encryption method}[password] *passwordHistory: 20040909190821{SHA}FSG7BH6Aa6LK3UVISIzMytdgtQ8*	L, ces
gvPassword ExpirationTime	Zeitpunkt, nach dem das Passwort dieses Principals abläuft. Format: YYYYMMDDHHMMSS	Generalized Time
gvLastLogin	Zeitpunkt des letzten erfolgreichen Logins Format: YYYYMMDDHHMMSS	Generalized Time
gvPassword Locked	Kennzeichen, ob durch falsche Eingabe des Passworts die UserID/PW-Authentifizierung gesperrt ist.	bool
gvRights	Liste der dem Benutzer gewährten Rechte pro Anwendung im Stammportal einschließlich der dazugehörigen Parameter. Wird auch zum Aufbau von Menüs verwendet. Das Format ist: Syntax: gvRights ::= App-dn „$" Auz-Roles App-dn… DN des gvApplication bzw. des gvApplicationProxy Objekts der Anwendung in kanonisierter Schreibweise, für das Rechte eingeräumt wurden. Auz-Roles… PVP Rechte im HTTP-Format des PVP Parameters X-AUTHORIZE-roles (siehe Auz-Roles in der EBNF der PVP Spezifikation); Die für HTTP vorgesehenen Zeichenkodierungsregeln aus der PVP Spezifikation (In PVP 1.9.2 im Kapitel 9 Protokollbindung HTTP) gelten auch hier.	L, cis (32767)
gvParticipant OuId	gvOuId der zugriffsberechtigten Stelle (kein dn!)	cis(32)

gvUserPassword	Benutzerpasswort. Verwendung: Anmeldung am Portal Syntax: plaintext-password | „{x-sha-1:b64}" encrypted-password in base64-Darstellung[1]	ces
preferredLanguage	Für Registratur von Personen: Bevorzugte Sprache als ISO 639-1 Code (de=Deutsch, en=Englisch, fr=Französisch, jv=Javanisch, …) Default=de	ia5
gvPasswordRetryCount	Anzahl der Fehleingaben bei der Passwort-Authentifizierung. Zweck: Password Policy (Stammportal)	int
gvAdditionalName	Für Registratur von Personen ohne gvOrgUnit: Firmen- oder Organisationsbezeichnung.	ces
gvAccountLocked	Zum Sperren eines Accounts. Ist ein Account gesperrt, so sind für das Konto keine Anmeldungen mehr möglich. Wird vom Portal gesetzt, wenn ein Account zu lange nicht benutzt wurde. ()	bool
gvSecClass	administrative Sicherheitsklasse der Person. Wertebereich: [0..3] Für Personen ohne Sicherheitsvereinbarung MUSS 0 angegeben werden.	int(1)

[1] Best Practice ist, dieses Feld per ACL als „compare" zu definieren.

gvSystem	System Principal. Ein System Principal ist im Gegensatz zu einer Person ein Prozess oder ein System, kann sich aber dennoch authentifizieren und kann berechtigt sein. Im Stammportal können Anwendungen so Credentials und Rechte erhalten, die nicht eindeutig auf einen Endbenutzer zurückführbar sind.

dn: cn=.., ou=Systems,..
(dn: cn=bmiweb1.applikation1@bmi.gv.at,ou=Systems,gvOuId=AT:B:112,dc=at)

Attribut	**Beschreibung (Beispiel)**	**Eigen-schaft**
cn	Bezeichnung des System-Principals in der Form Anwendung.Subsystem@domain *(bmiweb1.applikation1@bmi.gv.at)*	M, L, cis(64)
uid	Innerhalb der Domäne eindeutige abgekürzte Bezeichnung des System-Principals in der Form Anwendung.Subsystem + Domain-Suffix im RFC822-Format *(bmiweb1.app1@bmi.gv.at)*	L, ces
gvOuId	gvOuId (siehe gvOrgUnit.gvOuId) der Organisationseinheit, die für das System datenschutzrechtlich verantwortlich ist (kein dn) (gvOuId= AT:l9:9876)	cis(32)
gvUserPassword	Entsprechend gvPrincipal	ces
gvRights	Entsprechend gvPrincipal	L, cis (32767)
gvSecClass	administrative Sicherheitsklasse des Systems	int(1)
gvParticipantOuId	gvOuId der zugriffsberechtigten Stelle (kein dn)	cis(32)
description	Entsprechend gvOrgPerson	L, cis(1024)

gvUserPortal	User Portal (Stammportal) Definiert für das Anwendungsportal eine Stammportalinstanz mit zugehörigen Zertifikaten und Berechtigungen	
dn: cn=..,ou=Portal,.. *(dn: cn=pvpportal@noel.gv.at,ou=Portal,gvOuId=AT:B:112,dc=at)*		
Attribut	**Beschreibung (Beispiel)**	**Eigen-schaft**
cn	Eindeutige Bezeichnung des Stammportals. Aufbau analog zu gvSystem. *(z.B: pvpportal@noel.gv.at)*	M, L, cis(64)
gvParticipants	Liste der zugriffsberechtigten Stelle (gvOrganisation), die das Stammportal benutzen, als gvOuId (siehe gvOrgUnit)	L, cis(32)
gvDefaultParticipant	gvOuId der zugriffsberechtigten Stelle des Stammportals - für Zugriffe mit PVP-Versionen vor 1.8. Ab PVP 1.8 muss die zugriffsberechtigte Stelle durch den PVP Parameter participantId explizit angegeben werden. Zweck: Kompatibilität zu PVP 1.7.	cis(32)
gvSupportedPvpProfile	PVP Version und Profile, welche von diesem Stammportal unterstützt wird (Werte wie gvApplication)	L, cis(1024)
description	Entsprechend gvOrgPerson	L, cis(1024)
gvPortalHotlineMail	E-Mail-Adresse Portalhotline (wie Attribut mail im Objekt gvOrgPerson)	L, IA5(256)
gvAdminContactName	Vor- und Nachname(n) für administrative Kontaktperson	L, cis(256)
gvAdminContactMail	E-Mail-Adresse administrativer Kontakt (wie mail in gvOrgPerson)	L, IA5(256)
gvAdminContactTel	Telefonnummer (wie telephoneNumber in gvOrgPerson)	L, tel(32)
gvMaxSecClass	Maximale gvSecClass, die Benutzer eines Portal erreichen können (z.B. 0). Anwendungsfälle sind vor Allem Test- und Entwicklungsportale. Das AWP bzw. der SP müssen den Wert von gvSecClass des Benutzers dementsprechend hinuntersetzen. Ist das Attribut nicht gesetzt, wird die gvSecClass nicht limitiert.	int(1)

gvUserPortal wird von Anwendungsportalen verwendet und repräsentiert ein Stammportal. Instanzen dieser neuen Objektklasse solle unterhalb der neu eingeführten OrganizationalUnit (ou=Portal) geführt werden.

Portale mit gvMaxSecClass

Für Anwendungsfälle wie den Test- und die Entwicklung von Portalsoftware oder die Entwicklung von Applikationen gibt es die Möglichkeit, Stammportale mit dynamischer

Berechtigungsvergabe einzurichten, wo sich z.B. Benutzer selbst Rechte für Anwendungen zuweisen können. Bei diesen Portalen wird ein niedriger Wert oder 0 in gvMaxSecClass gesetzt. Anwendungsportale und Serviceprovider müssen bei Zugriffen eines Portals die gvSecClass auf den Wert von gvMaxSecClass heruntersetzen. Dadurch wird sichergestellt, dass von diesen Portalen keine Zugriffe auf Rollen mit hohen Sicherheitsklassen erfolgen können. Zusätzlich muss beim gvApplication-Objekt das Attribut gvMaxSecClassAllow auf true gesetzt sein.

gvUserPortal FederationInfo	Kindobjekt eines gvUserPortal Eintrages. Mithilfe von Einträgen dieses Typs wird angegeben, in welchen SAML Federations ein Stammportal auftritt, und mit welcher Entity-ID das Stammportal in den SAML 2 Metadaten der jeweiligen Federation geführt wird.	
dn: gvFederationName=..,cn=…ou=Portal,.. *(dn:* gvFederationName*=PVV@gv.at,cn=pvpportal@noel.gv.at,ou=Portal,gvOuId=...)*		
Attribut	**Beschreibung (Beispiel)**	**Eigen-schaft**
gvFederationName	*Federation, in der das Stammportal auftritt*	M, cis(1024)
gvSamlIdpEntityId	SAML 2 Entity-ID (Eindeutiges Kennzeichen in den SAML Metadaten)	L,cis(1024)

gvX509Certificate	Zertifikate	
dn: x509SerialNumber=..+gvX509IssuerDns=..[, +gvX509CaQualifier=…], cn=..,ou=Portal,.. *(dn*: *x509SerialNumber=123+gvX509IssuerDns=Class2PublicPrimaryCA.verisign.com,cn=pvpportal@noel.gv.at,ou=Portal,gvOuId=AT:B:112,dc=at)*		
Attribut	**Beschreibung *(Beispiel)***	**Eigen-schaft**
X509SerialNumber	1.3.6.1.4.1.10126.1.5.3.2 Die Definition von Integer für x509serialNumber ist für Novell's eDirectroy und IBM Tivoly Directory nicht praktikabel, weil es zu restriktive Längenbeschränkungen gibt. In diesen Schemen ist das Attribut als String definiert. Wird die Seriennummer als String abgelegt, so ist die Nummer als Dezimalzahl abzubilden. (Nicht als Hexadezimalzahl)	M, int
X509IssuerDnsName	Dieser Wert dient als Teil des dn dazu für ein Zertifikat einen eindeutigen RDN zu erzeugen. Im Gegensatz zu gvX509Issuer-Canonical gibt es mit diesem Attribut keine Probleme mit Längenbeschränkungen bei manchen Server-Implementierungen	M, IA5(76)

gvX509CaQualifier	Mehrere CAs eines Zertifizierungsdienstanbieters können den gleichen IssuerDnsName haben. Um den (theoretischen) Fall auszuschließen, dass Zertifikate unterschiedlicher CAs eines ZDA mit gleicher Seriennummer zur gleichen Organisation zurgeordnet werden, kann diese Attribut in den RDN aufgenommen werden.	IA5(20)
gvX509IssuerCanonical	Kanonisierte Form von x509Issuer	M, cis(1024)
x509validityNotBefore	1.3.6.1.4.1.10126.1.5.3.5	Generalized Time
x509validityNotAfter	1.3.6.1.4.1.10126.1.5.3.6	Generalized Time
x509FullCrl DistributionPointURI	1.3.6.1.4.1.10126.1.5.3.32	ia5
x509userCert	*Nicht verwenden.* *1.3.6.1.4.1.10126.1.5.4.76 Die Syntax (Certificate (1.3.6.1.4.1.1466.115.121.1.8) ist in eDirectory und IBM-Tivoly Directoryserver nicht implementiert. Dieses Attribut wird daher durch gvX509userCert ersetzt.*	
gvX509userCert	Ersetzt das Attribute x509userCert	binär
x509subject	1.3.6.1.4.1.10126.1.5.3.7	dn
x509keyUsage	1.3.6.1.4.1.10126.1.5.3.15 "digitalSignature" / "nonRepudiation" / "keyEncipherment" / "dataEncipherment" / "keyAgreement" / "keyCertSign" / „cRLSign" / "encipherOnly" / "decipherOnly"	ia5
x509subjectDnsName	1.3.6.1.4.1.10126.1.5.3.18 (Internet domain name of the entity associated with this public-key)	ia5
x509extKeyUsage	1.3.6.1.4.1.10126.1.5.3.30	oid

Auf die Verwendung der Klassen x509base, definiert in [crl-schema] und x509PKC, definiert in [pkc-schema] wurde verzichtet, da die Verwendung eines x509issuer mit der distinguished-name Syntax bei LDAP-Servern mit Prüfung der referentiellen Integrität dazu führt, dass umfangreiche Strukturen aufgebaut werden müssen.

Weiters wird vermieden, dass ein Issuer im RDN zur Verwendung eines geschachtelten DN führt, was in LDAP komplex und bei einer SQL-Implementierung erst recht nicht trivial ist. Um das Problem zu umgehen, wird der Issuer in einer kanonisierten Form als String verwendet. Dazu wird die allgemeine Regel für die Kanonisierung von DN-Attributen in ldap.gv.at verwendet, und das Resultat dann im Attribut gvX509IssuerCanonical gespeichert.

(6) Referenzen

[crl-schema]	http://www.ietf.org/proceedings/03jul/I-D/draft-ietf-pkix-ldap-crl-schema-01.txt
[pkc-schema]	http://www.rediris.es/ldap/doc/draft-klasen-ldap-x509certificate-schema-03.txt
[SecClass]	Sicherheitsklassen für den Zugriff von Benutzern auf Anwendungen, SecClass 2.1.0. http://www.ref.gv.at/KONVENTIONEN.1116.0.html
[LDAP-gv.at]	Spitzenberger, Martin/Hörbe, Rainer/Wollendorfer, Robert/Liehmann, Michael: Spezifikation LDAP-gv.at 2.4.0. http://www.ref.gv.at/KONVENTIONEN.1116.0.html

(7) Anhänge

(7.1) LDAP.gv.at Attribute der Bürgeranmeldung

gvApplication	Anwendung, wie sie im Anwendungsportal definiert ist.

dn: gvApplId=...,ou=Applications, ..
(dn: gvApplId=ZMR,ou=Applications,gvOuId=AT:B:999,dc=at)

Attribut	**Beschreibung (Beispiel)**	**Eigen-schaft**
gvAdministrativeSectorID	Verwaltungsbereich: Nur Benutzer aus diesem Bereich dürfen die Anwendung benutzen. Wert gemäß Bereichsabgrenzungsverordnung. Ist dieses Attribut leer, so kann die Anwendung unabhängig vom Verwaltungsbereich des Benutzers verwendet werden. Beim Zugriff über Bürgeranmeldung erhält die Applikation die bPK des angemeldeten Benutzers für den hier angegebenen Bereich.	L, cis(5)

gvApplicationRight	Rechte und deren Parameter für Objekte der Klassen gvOrgPerson, gvPersonFunction (s. [LDAP-gv.at])

dn: cn=…,gvApplId=…,ou=Applications,..
(cn=ZMR-Anfrage,gvApplId=ZMR,gvOuId=AT:B:999,dc=at)

Attribut	**Beschreibung (Beispiel)**	**Eigen-schaft**
gvCitizenRight	Kennzeichnet ein Bürgerrecht. Wenn dieses Attribut auf „true" gesetzt ist, erhalten Bürger die sich über eine Bürgerkarte anmelden dieses Recht zugewiesen. Dieses Attribut kann verwendet werden, um einen öffentlichen Zugang von Bürgern auf eine Anwendung zu ermöglichen.	bool

(7.2) Kanonisierung von DN-Attributen

Die Kanonisierung von Distinguished Names ist eine Regel um eine einheitliche Schreibweise von DNs in Attributen zu erreichen. Dadurch wird der Vergleich von DNs in Anwendungsprogrammen vereinfacht

Um den Vergleich von DNs als Textvergleich zu ermöglichen, dürfen keine unterschiedlichen Syntaxvarianten verwendet werden. Die Kanonisierung erfolgt nach folgenden Regeln:

- Optionale Leerzeichen müssen weggelassen werden (bei , = +)
- Hochkomma darf nicht verwendet werden um Sonderzeichen zu kodieren.
- Attribute sind durch ihre Namen und nicht durch ihre OID anzugeben (z.B. sn=Pichler" und nicht „2.5.4.4=Pichler"). Der Name ist in Kleinbuchstaben anzugeben.
- LDAP-Sonderzeichen sind durch \ + Sonderzeichen darzustellen, aber nicht durch \ + Hexcode etc. Folgende Sonderzeichen müssen kodiert werden: "," "=" "+" "<" ">" "#" ";" "\", QUOTATION(ASCII decimal 34)

Beispiel:

Der DN

CN=VeriSign Class 2 Public Primary Certification Authority - G3, OU="(c) 1999 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US

lautet im kanonisierten Format:

cn=VeriSign Class 2 Public Primary Certification Authority - G3,ou=(c) 1999 VeriSign\, Inc. - For authorized use only,ou=VeriSign Trust Network,o=VeriSign\, Inc.,c=USHistorie

(7.3) Änderungshistorie

V 1.0.0, 3.3.2006, Martin Spitzenberger

- Neuerstellung als Konventionsentwurf

V 1.0.1, 30.8.2010, Martin Spitzenberger

- gvUrlMapping:
  - Zusätzlicher Parameter: „optional"
  - Anpassung der Erläuterung
- gvRoleSyntax: Korrektur Erläuterungstext und Beispiel
- gvSystem.gvOuId, gvUserPortal.gvParticipants: Ausdruck Org-ID durch Referenz ersetzt
- gvParticipant.gvOuID, gvUserPortal.gvDefaultParticipant: Korrektur des Beschreibungstextes
- gvRightsCoDomain:
  - Ergänzung um Parameter zu beschreiben
  - Korrektur des Erläuterungstextes
- gvParticipant.gvMaxRights: Korrektur der Form 4
- Attribute für die Bürgeranmeldung im Anhang
- Multivalue Attribute gemäß RFCs

V 1.0.2, 10.02.2012, Harald Hahn und Peter Pichler

- gvApplication Beispiel: ZMR Anwendung durch eine Musteranwendung ersetzt.
- gvUrl: Datentyp uri ist kein LDAP V3 definierter Datentyp. Wurde durch ces ersetzt.
- gvRightParameters: wird gelöscht.
- gvRightsCodomain: Stringlänge auf 1024 festgelegt.
- gvNamedParameterList: Fehler im rdn ausgebessert.
- Beispiele vereinheitlicht
- Bei der Übernahme in das Anhangkapitel ist ein Fehler passiert. Das Attribut gvCitizenRight gehört zur Objektklasse gvApplicationRight. Nicht zu gvApplication
- gvRights: Es sind keine Escape-Character für Rechteparameter genannt. In PVP 1.9 wuden Kodierungsregeln definiert, die es auch erlauben Beistrich und die schließende Klammer in PVP Parametern zu verwenden. Die Kodierungsregeln sollen genannt werden.
- gvRightsCodomain: Syntax aus der Tabelle genommen und ILCHAR an Ende der Syntax verschoben.
- Die Definition „Kanonisierte Schreibweise von DN's ist nicht mehr aktuell.
- gvExtensionItem bei den allgemeinen Attributen definiert und bei den einzelnen Objektklassen entfernt.
- "Rechtemodellierung für Portalverbundanwendungen" (PVRechte 1.0.0) (gvRightsCoDomain, gvSingularRight)

V 1.6.0, 31.1.2014, Harald Hahn und Peter Pichler

- Komplettüberarbeitung Einleitungskapitel – Ergänzungen für PVP-2 (UML Diagramme mit richtigen Klassennamen, erklärende Texte zu den UML Diagrammen, erweitert um neue Klassen, DIT Tree Beschreibung aktualisiert)
- Neue Typen: gvFederation, gvApplicationFederationInfo, gvUserPortalFederationInfo
- Neue gvApplication Attribute: gvSupportedPvpProfile
- gvRights hat ein caseExactMatching, dies soll durch ein caseIgnoreMatching ersetzt werden. Impliziert wahlweise Groß- und Kleinschreibung des DN und/oder der Rechte bzw. Parameter.
- Anmerkung x509serialNumber: Die Definition für x509serialNumber ist für Novell's eDirectroy und IBM Tivoly Directory nicht praktikabel.
- Anmerkung Attribut x509IssuerDnsName, Ungültigerklärung von OID
- gvUserPortal wird erweitert um gvPortalhotline, gvAdminContactName, gvAdminContactMail, gvAdminContactTel, gvSupportedPvpProfile
- Klasse gvX509CaCertificate entfernt (Konzept unvollständig und nie umgesetzt)
- Anpassungen von Texten und Beispielen, im Sinne von "Rechtemodellierung für Portalverbundanwendungen" (PVRechte 1.0.0) (gvRightsCoDomain, gvSingularRight)

V 1.6.1, 14.4.2015, Harald Hahn und Peter Pichler

- In der Skizze zum Kapitel 4.4 (Neue Typen für PVP2 und SAML) war noch eine Beziehung zwischen gvFederation.gvFederationName und gvApplication.gvTargetFederationName mit einem Pfeil dargestellt, obwohl das Attribute gvApplication.gvTargetFedertionName im Rahmen des Abstimmungsprozesses wieder entfernt wurde. Der Pfeil wurde entfernt.
- In der Versionshistorie waren zur Version 1.6 noch folgende neue gvApplication Attribute aufgeführt, die im Rahmen der Abstimmung wieder entfernt wurden: gvTargetFederationName, gvTargetFederationSamlSpEntityId, gvTargetPvpProfile
  Die Versionshistorie für Version 1.6 wurde entsprechend korrigiert.

V 1.6.2, 21.12.2017, Sub-AG-PVP

- gvApplication.gvApplId Zeichensatz auf druckbare ASCII erweitert
- Neue Attribute gvUserPortal.gvMaxSecClass und gvApplication.gvMaxSecClassAllowed
- gvUserPortalFederationInfo.gvSamlIdpEntityId und gvApplicationFederationInfo.gvSamlSpEntityId wurden von Single-Value auf Multi-Value (L) geändert. (Grund Stamm- bzw Anwendungsportale, die über mehrere Hostnamen angeboten werden)
- gvApplicationRight.gvApplId deprecated erklärt
- Fehler im gvMaxRight Beispiel für Rechte ohne Parameter korrigiert ($-Zeichen ergänzt)
- X509IssuerDnsName – Anmerkung zur vor 1.6.0 falsch definierten OID entfernt
- Layout Änderungshistorie vereinfacht (Tabellen mit Texten in unsichtbaren Bereichen entfernt)
- Layout an das anderer AGIZ Spezifikationen angepasst