Zugriff auf ldap.gv.at über SOAP und PVP

Konvention

ldap-soap-pvp 1.0.0

Empfehlung

Kurzbeschreibung:	Für andere Zugriffsarten als den öffentlichen Lesezugriff auf ldap.gv.at soll die Authentifizierung und Autorisierung über die Portalverbund-Infrastruktur erfolgen. Hier wird die dazu notwendige Protokollbindung spezifiziert.		
Autor:	Rainer Hörbe (LFRZ)	Projekt:	Arbeitsgruppe Q-PV
Beiträge von:	Peter Pfläging (Wien), Peter Pichler (LFRZ)		

Version 1.0.0 : **05.11.2007** Fristablauf: **30.11.2007**

Inhalt

1 Ziel

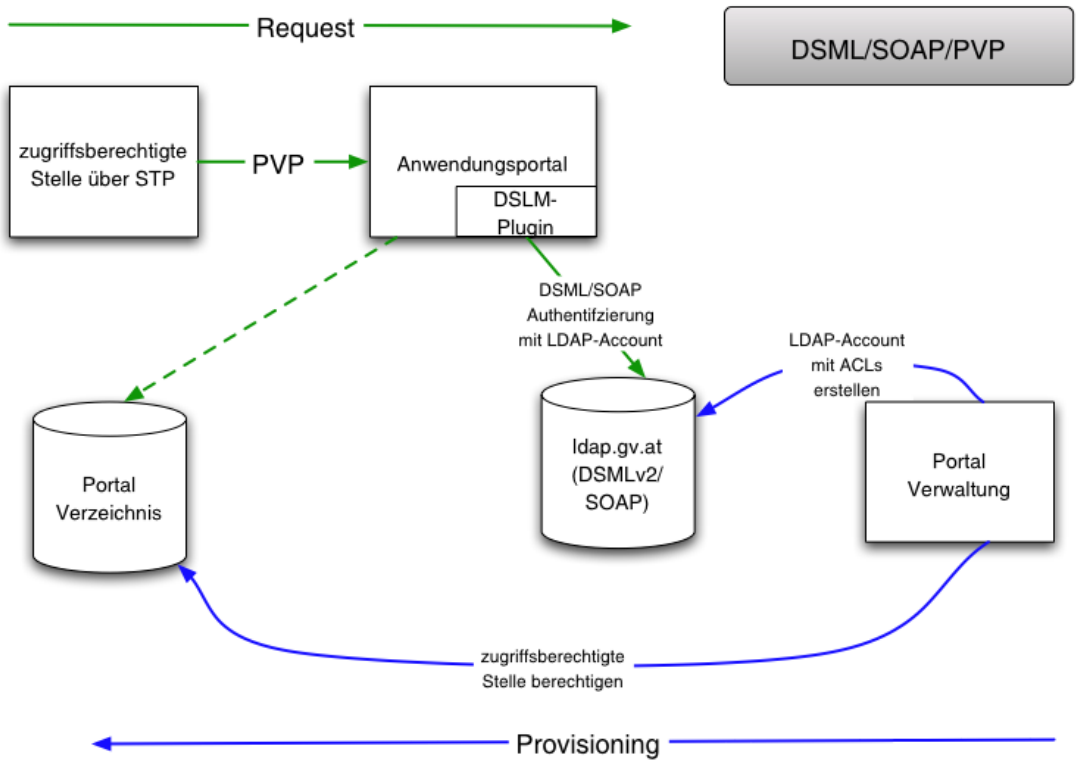
Die meisten LDAP-Server unterstützen heute den Zugriff auf das Verzeichnis über DSMLv2 mit SOAP [OASIS-DSML], wie z.B. Novell e-Directory, Sun One DS und IBM Tivoli DS. Diese Spezifikation soll diesen Zugriffsweg über die PVP/SOAP-Bindung zu ldap.gv.at eröffnen.
Der gleiche Mechanismus kann auch für den Zugriff auf Portalverzeichnisse verwendet werden.

2 Umsetzung

Um den Aufwand für die Implementierung gering zu halten, erfolgt die Umsetzung der Rechteprüfung am Directory Server mittels ACLs, da die Rechteprüfung im Portal (Request und Response gegen Recht) nicht trivial zu implementieren ist.

Dass heißt, dass für jedes LDAP-Rechteprofil ein LDAP-User-Account definiert wid, dessen Credentials dem Anwendungsportal bekannt sind. Das Rechteprofil wird mittels ACLs implementiert. Außerdem wird den Benutzern (= zugriffsberechtigten Stellen) im Anwendungsportal das Recht eingeräumt dieses LDAP-Rechteprofil zu nutzen.

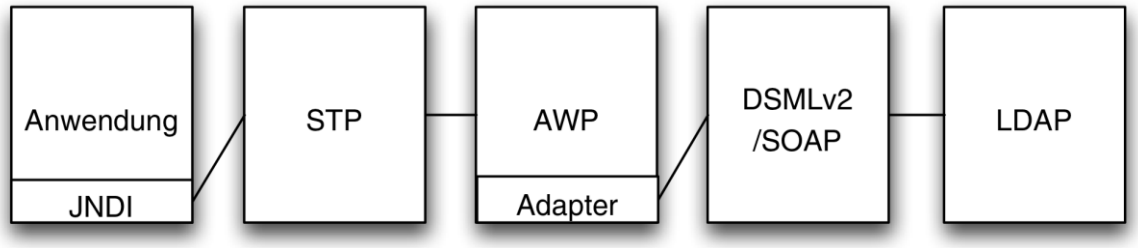
Requests von Benutzern mit diesem LDAP-Rechteprofil sind vom Anwendungsportal als der jeweilige Benutzer am LDAP-Server anzufragen. Das Anwendungsportal prüft, ob die zugriffsberechtigte Stelle mit dem richtigen LDAP-Rechteprofil anfragt.



2.1 Ablauf eines Zugriffs

Voraussetzungen:

- Im AWP ist das DSML-Service des LDAP-Servers als Anwendung „*LDAP.GV.AT*“ definiert.
- Für die Anwendung *LDAP.GV.AT* ist ein Recht „*ldapuser*“ definiert, dass den Rechteparameter „*authId*“ haben muss.
- Im AWP ist eingerichtet, dass die Anwendung beim Recht *ldapuser* den Rechteparameter „*authzId=uid=xyz,ou=principals,dc=local*“ mitsenden darf.
- Im LDAP-Server ist der Account *uid=xyz,ou=principals,dc=local* eingerichtet, das AWP besitzt die Credentials (Passwort). Der Account besitzt ACLs entsprechend den Berechtigungen der zugriffsberechtigten Stelle.



Request:

1. SOAP-Request der Anwendung[1] an das STP: suche Einträge im Verzeichnis, die den Kriterien folgendes LDAP-URLs entsprechen: ldaps:///dc=gv,dc=at??sub?objectclass=gvApplication
2. STP fügt den PVP-Token hinzu mit dem Recht ldapuser(authzId=uid=xyz,ou=principals,dc=local)
3. APW prüft im ersten Schritt, ob die zugriffsberechtigte Stelle die Berechtigung ldapuser(authzId=uid=xyz,ou=principals,dc=local) haben darf.
4. AWP prüft im zweiten Schritt, ob ldapuser(authzId=uid=xyz,ou=principals,dc=local) dem Content entspricht. Dazu muss im AWP (Application-Plugin) geprüft werden, ob ein entsprechendes AUTH-Element im SOAP-Body vorhanden ist, und eines einfügen, falls es nicht vorhanden ist.

Referenzen

[OASIS-DSML]
DSMLv2 approved OASIS Standard in April 2002
www.oasis-open.org

[1] In einer Java-Umgebung können mit JNDI LDAP-Zugriffe automatisch auf DSMLv2 umgesetzt werden. Somit kann aus Anwendungssicht weiterhin LDAP programmiert werden, obwohl der Zugriff über SOAP und PVP läuft.