

Spezifikation Portal Verbund Protokoll (vormals BMI-Gateway Protokoll)		Konvention	
		PVP 1.5.3	
		Entwurf öffentlich	
Kurzbeschreibung:	Der Portalverbund ermöglicht Betreibern von Applikationsportalen die Delegation von Authentisierung und Autorisierung an andere Portale. Dadurch wird der Aufwand für die Verwaltung der Benutzer reduziert und Single Sign-On unterstützt.		
Autor:	Rainer Hörbe (BMI-EDVZ)	Projektteam / Arbeitsgruppe:	Arbeitsgruppe behördenübergreifende Autorisierungssysteme

Stelle:	vorgelegt am:	angenommen am:
IKT-Board	4.4.2002	4.4.2002
Städtebund	12.2.2002	25.3.2002
Gemeindebund	12.2.2002	
Länder	12.2.2002	9.4.2002

Zweck

Dieses Dokument spezifiziert das Protokoll zur Kommunikation von Portalen in Portalverbund. Es ist eine spezifische Verwendung des HTTP-Protokolls.

Bis zur Version 1.4 war die Bezeichnung BMI-Gateway-Protokoll. Da nun das Protokoll unabhängig vom BMI eingesetzt wird, wurde die Bezeichnung geändert.

Das Protokoll ermöglicht eine delegierte Benutzerverwaltung. Authentisierung und Autorisierung erfolgen am Heimat-Portal des Anwenders, das seinerseits den Benutzer über das Portalverbund-Protokoll am Applikationsportal authentisiert und autorisiert.

Anwendungsfälle

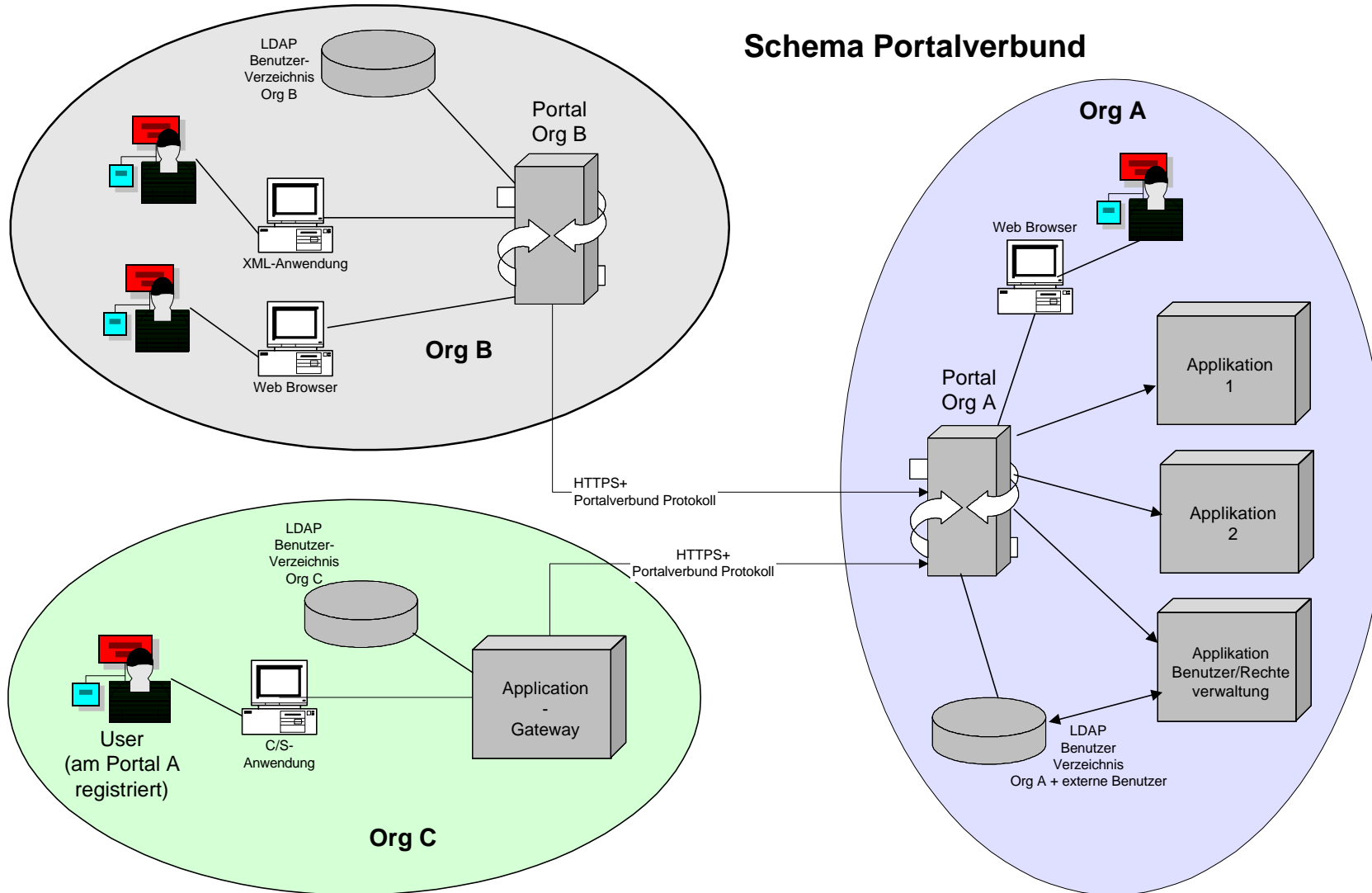
Sämtliche TCP-Verbindungen der Clients werden über das Heimat-Portal des Benutzers geführt, der als Reverse Proxy Richtung Ziel-Adresse eingesetzt ist.

Im nachfolgenden Schema ist aufgezeichnet, welche Anwendungsfälle für das Portalverbundsystem definiert sind. Dazu gibt es folgende Erläuterungen:

- Die Organisation A betreibt ein Portal, um die Applikationen 1, 2 und Benutzerverwaltung verfügbar zu machen. Die Benutzerverwaltung ist nur für Benutzer der Organisation A verfügbar, die beiden anderen im Portalverbund. Aus der Sicht eines Anwenders in der Org. B ist es ein Applikationsportal, aus der Sicht des Anwenders der Org A das Heimatportal
- Die Organisation B betreibt ein Portal und eine Benutzerverwaltung, um die Applikationen der Organisation A für ihre internen Anwender verfügbar zu machen. Die Applikations-Clients sind sowohl Webbrowser als auch Anwendungsprogramme.
- Die Adressen (URL) der Applikationen werden von den Portalen aufgelöst. Wenn ein Org-B User auf die Applikation 1 zugreifen möchte könnte das wie folgt aussehen:
 - Benutzer meldet sich am Heimatportal an: <https://portal.org-b.gv.at/> und bekommt ein Menü mit den zur Verfügung stehenden Applikationen angezeigt.
 - Benutzer wählt Applikation 1 und adressiert damit <https://portal.org-b.gv.at/org-a.gv.at/app1/>
 - Das Portal der Org B setzt den Namen des virtuellen Hosts im HTTP-Request auf portal.org-b.gv.at um (auch für Redirect-Responses) und leitet den HTTP-Request, erweitert um die HTTP-Header des Portalverbund-Protokolls weiter an <https://portal.org-a.gv.at/org-a.gv.at/app1/>¹. Dabei authentisiert sich das Portal B mittels X.509 Client-Zertifikat am Portal A.
Organisation C betreibt kein Portal, sondern einen Applikations-Gateway, der sich nach außen wie ein Portal verhält.

¹ Der Grund, warum im Pfad die Domäne des Applikationsportals wiederholt wird ist, dass dann mit einem virtuellen Host mehrere Applikationen betrieben werden können, ohne dass es zu Kollisionen der Pfadnamen kommen kann.

Schema Portalverbund



Begriffsbestimmung

Portal, Applikationsportal

HTTP-Server, der für andere HTTP-Server die Aufgaben der Authentisierung und Autorisierung übernimmt. Im Sinne der Spezifikation für HTTP 1.1 (RFC 2068) ist ein Portal ein Gateway²

Heimatportal

Portal, an dem ein Benutzer registriert ist.

Dezentrale Benutzerverwaltung

Ein Applikationseigner überträgt einer Organisation das Recht, für ihr Personal Authentisierung und Autorisierung selbst vorzunehmen. Dadurch braucht ein Benutzer nur an einem Portal (Heimatportal) registriert sein, und kann dennoch auch auf Applikationen anderer Portale im Verbund zugreifen.

Portalverbund

Zusammenschaltung von Applikationsportalen, um eine dezentrale Benutzerverwaltung zu ermöglichen.

Applikations-Gateway

Applikationsserver, der das Portalverbund-Protokoll verwendet und auf eine dezentrale Benutzerverwaltung zugreift, aber kein HTTP-Server ist.

Funktion

Siehe LDAP-Schema

Eigenschaften des Portalverbund-Protokolls

- Das Protokoll definiert die Kommunikation zwischen Portalen im Portalverbund der österreichischen Verwaltung
- Das Protokoll baut auf dem HTTP-Protokoll in der Version 1.1 (RFCs 2068 und 2616) auf
- HTTP MUSS mit TLS oder SSL3.0 gesichert werden, wobei Client-Zertifikate verpflichtend sind
- Die Authentisierungs- und Autorisierungsinformationen MÜSSEN über benutzerdefinierte HTTP-Header mitgegeben werden
- Das Protokoll ist unabhängig vom Content bei Request und Response
- Grundsätzlich wird jede HTTP-Transaktion für sich authentisiert, da das HTTP-Protokoll stateless ist. Ein Session-Ticket Mechanismus wie bei Kerberos ist nicht vorgesehen.

² "Gateway: Server which acts as an intermediary for some other server. Unlike a proxy, a gateway receives requests as if it were the origin server for the requested resource; the requesting client may not be aware that it is communicating with a gateway."

- Die mitgelieferten Benutzerdaten SOLLEN vom Applikationsportal protokolliert werden, und es SOLL überprüft werden, ob die Berechtigung für die Organisation gültig ist.
- Ein Zugriff auf einen externen LDAP-Dienst ist für HTTP-Requests des Portalverbund-Protokolls nicht notwendig. Für die Aufgaben der Revision ist eine Abfragemöglichkeit über HTTP/XML am Portal vorgesehen. Die entsprechende Spezifikation ist im Dokument "PVP-Revision" zu finden. Die Datenstruktur der Berechtigungsabfragen ist eine Ableitung des hier definierten Schemas.
- Der Abschnitt „Delegation“ im Teil 2 der Spezifikation des LDAP-Schemas bezieht sich auf ein zukünftiges Delegationsschema, das mit dem hier beschriebenen Protokoll nicht umgesetzt wird.

Verbindungsaufbau

Eine Transaktion des Gateways, stellvertretend für einen authentisierten Benutzer, besteht aus folgenden Schritten:

1. Aus dem Pfad oder virtuellem Host des Client-URL wird der URL des Applikationsportals bestimmt.
2. Der HTTP-Header "Host" wird auf den Namen des Applikationsportals umgesetzt
3. Aufbau einer HTTPS-Verbindung mit dem Applikationsportal
4. Beim Aufbau der SSL-Verbindung wird überprüft, dass je ein gültiges Client- und Server-Zertifikat vorhanden ist.
5. Der HTTP-Request des Clients wird um die unten definierten Header erweitert, wobei in der 2. Spalte die Felder mit M gekennzeichnet sind, die vorhanden sein MÜSSEN.
6. Wenn der Response den HTTP-Code 30x (Redirect) hat, wird der HTTP-Header "Location" auf den Host-Namen aus dem URL des Client-Requests umgesetzt.
7. Der Response wird an den Client weitergeleitet.

HTTP-Header

Name		Wert (einzeilig, Werte in [] optional)
X-Version:	M	1.1
X-AUTHENTICATE-UserID:	M	UserID, mit der sich der Endanwender am Application-Gateway authentisiert hat. (uid in gvOrgPerson)
X-AUTHENTICATE-cn:	M	Common Name (cn in gvOrgPerson)
X-AUTHENTICATE-gvGID:	M	Global Identifier des Benutzers (gvGID in gvOrgPerson)
X-AUTHENTICATE-gvOuID:		gvOuID des Objekts, auf welches das Attribut gvOu in gvPersonFunction oder gvOrgPerson zeigt
X-AUTHENTICATE-gvOudomain:	M	Organisations-Domäne (Internet-Domäne abgeleitet aus dc des Domain-Objekts, unterhalb dessen der Benutzer verwaltet wird, z.B. magwien.gv.at)
X-AUTHENTICATE-Ou:	M	Dienststellenbezeichnung: ou des Objekts, auf das das Attribut gvOu in gvPersonFunction oder gvOrgPerson zeigt
X-AUTHENTICATE-gvFunction		entspricht gvFunction im Objekt gvPersonFunction. Verpflichtend, wenn für eine Person Funktionen definiert sind
X-AUTHENTICATE-gvSecClass		1, 2 oder 3. Sicherheitsstufe des Anwenders nach der Spezifikation „Sicherheitsklassen“ der AG Auth. Fehlt dieser Header, wird die Sicherheitsklasse 1 angenommen. ³
X-AUTHENTICATE-mail:		E-Mail Adresse des Anwenders

³ Ausnahme: Beim Server portal.bmi.gv.at ist der Default-Wert 2, um Rückwärtskompatibilität mit bestehenden Anwendungen zu gewährleisten. Neue angeschaltete Portal müssen den Header mitliefern.

X-AUTHORIZE-roles ⁴ :	Recht1 [(regionale Einschränkungen1)]; Recht2 [(regionale Einschränkungen2)]; (Recht ist cn in gvApplicationRight)
----------------------------------	---

- Bei den Headern (Schlüssel und Werte) besteht kein Unterschied zwischen Groß- und Kleinschreibung.
- Bei den Trennzeichen "; ; ()=" in den Werten der HTTP-Header (z.B. X-AUTHORIZE-roles) SOLLTE Whitespace vermieden werden, KANN aber vorkommen.

Beispiel für einen HTTP Header bei einem Request eines Application-Gateways

```
POST /bmi.gv.at/portal/servlet/ HTTP/1.1
Host: portal.bmi.gv.at
Accept-Encoding: gzip, deflate
User-Agent: Mozilla
Connection: close
X-Version: 1.1
X-AUTHENTICATE-UserID: 4711240761@gemeinden.stmk.gv.at
X-AUTHENTICATE-cn: Max Mustermann
X-AUTHENTICATE-gvGID: 4711240761
X-AUTHENTICATE-gvOuID: A5
X-AUTHENTICATE-gvOudomain: gemeinden.stmk.gv.at
X-AUTHENTICATE-Ou: Meldeamt Herzeigegemeinde A
X-AUTHENTICATE-gvFunction: Meldebehörde
X-AUTHENTICATE-gvSecClass: 2
X-AUTHORIZE-roles: ZMR-Update(GKZ=60477,GKZ=60479,GKZ=60480);
Content-Type: application/x-www-form-urlencoded
Content-Length: 788
```

In diesem Fall ist der Benutzer berechtigt, die Rolle Meldebehörde für die Gemeinden mit den Gemeindegkennzahlen 60477, 60479 und 60480 auszuüben.

⁴ Der Name 'Roles' wird wegen der Rückwärtskompatibilität beibehalten. Da der Begriff 'Rolle' schon vielfältig besetzt ist, heisst das entsprechende Objekt im LDAP-Schema jetzt gvApplicationRight

Zertifikate

Bis zur Verfügbarkeit einer behördenweiten Public-Key Infrastruktur werden die SSL Client-Zertifikate bilateral zwischen den Portalbetreibern vereinbart. Server-Zertifikate SOLLTEN von öffentlichen CAs (Thawte, ..) beschafft werden.

Das gilt sowohl für HTTPS als auch LDAPS Verbindungen.

History

30.3.2001/V1.3: Domains unter .at zulässig (statt .gv.at); Einleitung überarbeitet

26.4.2001/V1.4: Einzelauthentisierung ins GW Protokoll eingearbeitet.

11.12.2001/V1.5:

- Zerlegung des BMI-GW-Protokolls in das Portalverbund-Protokoll und BMI-spezifische Erweiterungen
- Überarbeitung der Einleitung
- neuer Header X-AUTHENTICATE-gvSecClass
- neuer Header X-AUTHENTICATE-gvFunction
- Funktionen von Rollen entfernen (nur BMI-intern)
- zentrale Authentisierung (X-AUTHENTICATE-Password) entfernt (ist eine Erweiterung des BMI)
- X-AUTHENTICATE-Behoerdenkennzahl: wurde entfernt, da es von der Applikation selbst mitgegeben werden muss, und dem Portal nicht bekannt ist
- genauere Beschreibung wie die HTTP-Header dem LDAP-Schema entsprechen

31.1.2002/V1.5.1: Korrektur von Schreibfehlern; Dokumentformat an Vorlage des Forums E-Government-Länder angepasst

19.2.2002/V1.5.2: Entfernung der Zugriffe über LDAPS aus der Zeichnung „Schema Portalverbund“, da im Dokument PVP-Revision spezifiziert wurde, dass die Revisionsabfrage über HTTP/XML erfolgt.

8.7.2002/V1.5.3: Seite 7: Auch der Strichpunkt wird als Trennzeichen angegeben und im Beispiel für einen HTTP-Request wird der Wert für X-AUTHORIZE-ROLES mit Strichpunkt abgeschlossen.