

Spezifikation Portal Verbund Protokoll		Konvention	
		PVP 1.7.0	
		Empfehlung	
Kurzbeschreibung:	<p>Das Portalverbundsystem ermöglicht das Zusammenwirken von Stammportalen zur Registrierung von Benutzern mit ihren Zugriffsrechten und Anwendungsportalen zur Überprüfung des berechtigten Zuganges zu Anwendungen.</p> <p>Die Authentifizierung und Autorisierung kann delegiert werden.</p> <p>Der Aufwand für die Verwaltung der Benutzer wird reduziert und ein Single Sign-On unterstützt.</p>		
Autor:	Rainer Hörbe (BMI-ITMS)	Projektteam / Arbeitsgruppe:	Arbeitsgruppe behördenübergreifende Autorisierungssysteme

Stelle:	vorgelegt am:	angenommen am:
IKT-Board		zugestimmt 05.11.2002
Städtebund		zur Kenntnis genommen
Gemeindebund		offen
Länder		teilweise zugestimmt

Zweck

Das Protokoll definiert die Kommunikation zwischen Portalen im Portalverbundsystem der österreichischen Verwaltung. Darüber hinaus ist es für den Einsatz zwischen Behörden und Nicht-Behörden auf Grund bilateraler Vereinbarungen vorgesehen.

Im Folgenden wird dafür die Bezeichnung PVP verwendet.

Es ist eine Liste von Key-Value-Paaren, die den Client einer Request/Response-Transaktion authentisieren, autorisieren und seine Verrechnungsdaten übergeben. PVP kann mit verschiedenen Protokollen verwendet werden, wie HTTP und SOAP. Im Abschnitt ""Die mitgelieferten Benutzerdaten SOLLEN vom Anwendungsportal protokolliert werden, und es SOLL überprüft werden, ob die Rechte des Benutzers in der Menge der für die Organisation gültig Rechte enthalten ist. wird die Bindung an das HTTP-Protokoll definiert.

Das Protokoll ermöglicht eine delegierte Benutzerverwaltung. Authentifizierung und Autorisierung erfolgen am Stamm-Portal des Benutzers, das seinerseits den Benutzer über das Portalverbund-Protokoll am Anwendungsportal authentifiziert und autorisiert.

Begriffsbestimmung

Die Begriffe sind im Dokument „PV-Vereinbarung“ definiert.

Ergänzend dazu wird festgelegt:

Rechteprofil

Arbeitskontext einer Person, der mit spezifischen Berechtigungen verbunden ist. Z.B. Wachbeamter (Funktion A) hat Journaldienst (Funktion B mit erweiterten Berechtigungen)

Verrechnungsdaten

bestehen aus der Identifikation des Rechnungsempfängers, sowie der Menge der pro Benutzer und Anwendung möglichen Kostenstellen und Gebührenstufen.

Schreibweise

Diese Spezifikation verwendet EBNF (erweiterte Backus-Naur Form). EBNF beschreibt eine Grammatik, mit der die Menge der möglichen Zeichenketten einer „Sprache“ definiert wird.

Diese Schreibweise wird wie folgt definiert:

Name := Regel

Eine (Produktions-) Regel besteht aus einem oder mehreren Elementen. Ein Element ist Literal oder wiederum eine Regel. „:=“ heißt so viel wie „besteht aus“.

Regeln, die in RFC 2616 als „Basic Rules“ definiert sind, werden mit Großbuchstaben geschrieben, wie SPACE, TAB, CRLF, DIGIT, ALPHA, LWS...

Regeln können zur Klarstellung im Fließtext mit spitzen Klammern „<>“ geschrieben werden.

"Literal"

Literale sind durch Anführungszeichen markiert und bedeuten fixen Text, der nicht mehr weiter ersetzt wird. Der Text ist case-insensitive, wenn es nicht anders angegeben ist.

Kommentar

Text nach einem Semikolon bis zum Zeilenende wird als Kommentar betrachtet, z.B. ; Erklärung in die Spezifikation eingebettet

Regel-1 | Regel-2

Elemente, die durch einen vertikalen Strich ("| ") getrennt sind, sind Alternativen, z.B. "JA" | "NEIN"

!Regel-1 Regel-2!

Elemente innerhalb von Rufzeichen werden als einzelnes Element betrachtet. Z.B. kann die Regel <"bearbeite " !"alle " | "keine "! "Anfragen"> zu "bearbeite alle Anfragen" und "bearbeite keine Anfragen" führen. Die übliche Schreibweise mit runden Klammern „()“ wird hier nicht verwendet, um die Lesbarkeit von Parameterlisten zu verbessern.

*Regel +Regel {N}Regel {N-M}Regel

Das Zeichen vor einem Element bedeutet die Anzahl der Wiederholungen des Elements:

*	0 oder mehr
+	1 oder mehr
{N}	N
{N-M}	größer gleich N und kleiner gleich M

[Regel]

Eckige Klammern bedeuten, dass das Element optional ist.

#;Regel

Das #-Zeichen ist eine Kurzschreibweise für eine Liste mit Semikolon als Literal für das Trennzeichen. Die Form <n>#<t> bedeutet mindestens <n> Elemente, die von einem oder mehreren Trennzeichen <t>, und optional LWS getrennt sind.

(*LWS element *(*LWS ";" *LWS element))

kann dargestellt werden durch

1#;element

Null-Elemente sind erlaubt, werden aber nicht gezählt. #Element bedeutet 0 bis unendlich viele Elemente, 1#element 1 ein oder mehrere Elemente.

Grammatik des Portalverbund-Protokolls

Das Protokoll besteht aus eine Liste von Parametern, wobei jeder Parameter als Key-Value-Paar in der EBNF definiert ist:

```

pvp-parameters := pvp-Version pvp-Authentication [pvp-Authorization] [pvp-
    Accounting]
pvp-Version := "1.0" | "1.1" | "1.2"
pvp-Authentication := Auth-UserId Auth-Cn Auth-Gid [Auth-OuId]
    Auth-OuDomain Auth-Ou [Auth-Function] [Auth-SecClass]
pvp-Authorization := Auz-Roles
pvp-Accounting := Acc-InvoiceRecptId Acc-CostCenterIdList Acc-ChargeCodeList
Auth-UserId := "X-AUTHENTICATE-userId: " +CHAR ;
Auth-Cn := "X-AUTHENTICATE-cn: " +OCTET
Auth-Gid := "X-AUTHENTICATE-gvGid: " +CHAR
Auth-OuId := "X-AUTHENTICATE-gvOuId: " +OCTET
Auth-OuDomain := "X-AUTHENTICATE-gvOuDomain: " +CHAR
Auth-Ou := "X-AUTHENTICATE-Ou: " +OCTET
Auth-Function := "X-AUTHENTICATE-gvFunction: " +OCTET
Auth-SecClass := "X-AUTHENTICATE-gvSecClass: " "0" | "1" | "2" | "3"
Auz-Roles := "X-AUTHORIZE-Roles: "
    1#;Auz-Right["("##,Auz-RegionaleEinschränkung)"] [;]
Auz-Right := +OCTET
Auz-regionaleEinschränkung := Auz-Region"=" +OCTET
Auz-Region := "GKZ" | "DST" | "BL" ; Gemeindegkz., Dienststelle, Bundesland
Acc-InvoiceRecptId := "X-ACCOUNTING-InvoiceRecptId: " {5}CHAR1
Acc-CostCenterIdList := "X- ACCOUNTING-gvCostCenterId: "
    Acc- CostCenterId |
    Acc- CostCenterId ["<default>"] [, #,Acc-ChargeCode] ["<user defined>"]
Acc-CostCenterId := {1-25}!ALPHA | DIGIT | SPACE | "-" | "_" | "/"!
Acc-ChargeCodeList := "X- ACCOUNTING-gvChargeCode: "
    Acc-ChargeCode |
    Acc-ChargeCode ["<default>"] [, #,Acc-ChargeCode]
Acc-ChargeCode := DIGIT [DIGIT]
  
```

¹ Vorläufig, bis die Verwaltungskennzahl eingeführt wird

Beschreibung der Parameter

Name	Wert (einzeilig, Werte in [] optional)
X-Version:	"1.0" "1.1" "1.2"
X-AUTHENTICATE-UserID:	UserID, mit der der Benutzer am Stammportal authentisiert ist. LDAP: gvOrgPerson/uid
X-AUTHENTICATE-cn:	Name des Benutzers LDAP: gvOrgPerson/cn
X-AUTHENTICATE-gvGid:	Global Identifier des Benutzers LDAP: gvOrgPerson/gvGid
X-AUTHENTICATE-gvOuid:	Eindeutige Kennung für die Organisationseinheit des Benutzers LDAP: gvOrgUnit/gvOuid
X-AUTHENTICATE-gvOudomain:	Organisations-Domäne des Benutzers. Entweder Internet-Domäne (z.B. magwien.gv.at) oder LDAP: Domain/dn
X-AUTHENTICATE-Ou:	Dienststellenbezeichnung LDAP: gvOrgUnit/Ou
X-AUTHENTICATE-gvFunction:	entspricht Funktion in gvPersonFunction. Verpflichtend, wenn für eine Person Funktionen definiert sind. LDAP: gvPersonFunction/gvFunction
	Sicherheitsstufe des Benutzers nach der Spezifikation „Sicherheitsklassen“ der AG Auth. Fehlt dieser Header, wird die Sicherheitsklasse „1“ angenommen. ²
X-AUTHORIZE-roles ³ :	Anwendungsrechte, optional mit regionalen Einschränkungen. LDAP: gvApplicationRight/cn

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

³ Der Name 'Roles' wird wegen der Rückwärtskompatibilität beibehalten. Da der Begriff 'Rolle' schon vielfältig besetzt ist, heißt das entsprechende Objekt im LDAP-Schema gvApplicationRight

X-ACCOUNTING-InvoiceRecptId:	ID des Rechnungsempfängers (ASCII) Verwaltungskennzeichen der benutzerseitigen Organisation (bis zur deren Definition eine durch die BRZG vergebene eindeutige Nummer)
X-ACCOUNTING-CostCenterId:	Kostenstellencode des Benutzers Beispiele: ABC123<default>,DEF456 Der Benutzer hat die Kostenstellen ABC123 und DEF456 zur Auswahl, wobei ABC123 der Vorgabewert ist. ABC123 Der Benutzer hat die Kostenstelle ABC123 fix vorgegeben. ABC123<default>, DEF456,<user defined> Der Benutzer hat die Kostenstellen ABC123 und DEF456 zur Auswahl, wobei ABC123 der Defaultwert ist. Außerdem kann er weitere Kostestellen frei eingeben.
X-ACCOUNTING-ChargeCode:	Numerischer Code für Transaktionsgebühr, wobei 0 gebührenfrei bedeutet. Beispiele: 1 Der Benutzer hat die Gebührenstufe in der Anwendung fix vorgegeben 0<default>,1 Der Benutzer hat die Gebührenstufe 0 in der Anwendung vorgegeben, kann aber (über eine Auswahlliste) auch den Wert 1 eingeben.

- Die mitgelieferten Benutzerdaten SOLLEN vom Anwendungsportal protokolliert werden, und es SOLL überprüft werden, ob die Rechte des Benutzers in der Menge der für die Organisation gültig Rechte enthalten ist.
-
- Wenn für eine Anwendung bereits eine andere Verrechnungsart spezifiziert ist, als unter pvp-Accounting oben definiert, wird für die Anwendung eine Übergangsfrist verlautbart, bis die hier definierte Verrechnungsart verbindlich ist.

Protokollbindung HTTP

In diesem Abschnitt wird definiert, wie das PVP an das HTTP-Protokoll (RFC 2616) gebunden wird.

- Die PVP-Parameter werden über benutzerdefinierte HTTP-Header mitgegeben.
- Bei Trennzeichen ",;()=" in den Werten der HTTP-Header (z.B. X-AUTHORIZE-roles) SOLLTE Whitespace vermieden werden, KANN aber vorkommen.
- HTTP MUSS mit TLS oder SSL3.0 gesichert werden, wobei Client-Zertifikate verpflichtend sind.
- Wenn die Verrechnungsdaten vom Stamm- oder Anwendungsportal protokolliert werden sollen, muss die Anwendung die vom Benutzer eingegebenen Werte als die Cookies `x-gvCostCenterId` und `x-gvChargeCode` übergeben, damit sie für das Anwendungsportal lesbar sind. Die Cookies bleiben nur für die Dauer einer HTTP-Transaktion erhalten.
- Jede HTTP-Transaktion wird für sich authentifiziert, da das HTTP-Protokoll stateless ist. Ein Session-Ticket Mechanismus wie bei Kerberos ist nicht vorgesehen.⁴

Beispiel für einen HTTP Header bei einem (gebührenbefreiten) Request eines Stammportals:

```
POST /bmi.gv.at/portal/servlet/ HTTP/1.1
Host: portal.bmi.gv.at
Accept-Encoding: gzip, deflate
User-Agent: XYZ-Portal
Connection: close
X-Version: 1.2
X-AUTHENTICATE-UserID: 4711240761@gemeinden.stmk.gv.at
X-AUTHENTICATE-cn: Max Mustermann
X-AUTHENTICATE-gvGID: 4711240761
X-AUTHENTICATE-gvOuID: A5
X-AUTHENTICATE-gvOudomain: beispielgemeinden.stmk.gv.at
X-AUTHENTICATE-Ou: Meldeamt Herzeigegeemeinde A
X-AUTHENTICATE-gvFunction: Beispielbehoerde
X-AUTHENTICATE-gvSecClass: 2
X-AUTHORIZE-roles: Beispielrecht (GKZ=60477,GKZ=60479);
Content-Type: application/x-www-form-urlencoded
Content-Length: 788
```

In diesem Fall ist der Benutzer berechtigt, das Recht *Beispielrecht* für die Gemeinden 60477 und 60479 auszuüben.

⁴ Um keinen Performance-Nachteil zu erhalten, wird server-seitig ein Caching der Authentisierungs-Transaktion empfohlen.

Zertifikate

Bis zur Verfügbarkeit der Portal-PKI (für das Portalverbundsystem festzulegende Zertifikate) werden die SSL-Zertifikate bilateral zwischen den Portalbetreibern vereinbart.

Portal-Architektur

Die TCP-Verbindungen der Clients zur Anwendung werden über das Stammportal des Benutzers geführt, der als Gateway Richtung Ziel-Adresse eingerichtet ist.

Das Anwendungsportal kann als Reverse Proxy eingerichtet sein, oder als Modul im Anwendungsserver.

Fehlermeldungen

HTTP-Code	Beschreibung
402	Für diese Funktion ist eine Verrechnung erforderlich, aber das Header-Feld XXXX fehlt (XXXX ist eines aus X-ACCOUNTING-gvInvoiceRecptId, X-ACCOUNTING-gvCostCenterId oder X-ACCOUNTING-gvChargeCode)
440	Mandatory PVP-Header XXXX fehlt
441	Werte in X-AUTHORIZE-roles haben ungültiges Format
442	Kein zuässiges Recht in X-AUTHORIZE-roles
450	X-ACCOUNTING-gvInvoiceRecptId: ungültiger Wert oder Verrechnungskonto gesperrt
451	Ungültiger Wert für X-ACCOUNTING-gvChargeCode
461	Sicherheitsklasse (gvSecClass) muss mindestens 1 sein
462	Sicherheitsklasse (gvSecClass) muss mindestens 2 sein
463	Sicherheitsklasse (gvSecClass) muss 3 sein

Fehlerbedingungen sind im Text möglichst detailliert zu beschreiben, etwa durch die Referenz des betroffenen Headers und die Art der Bedingung (z.B. „Header x-Version fehlt“, „Wert für gvSecClass zu groß“)

URL-Aufbau für Anwendungsportale

Im Pfad wird die Domäne des Anwendungsportals wiederholt, um eindeutige Pfade zu gewährleisten. Dadurch kann ein Stammportal mit einem Virtuellen Host betrieben werden.

Z.B. : <https://portal.org-b.gv.at/org-a.gv.at/app1/>

