



Bürger via Portalverbund		Whitepaper
		PVP-citizen 1.0
		Ergebnis der AG
Kurzbeschreibung	Um Bürger welche sich an einem Portal authentifiziert haben, an eine entfernte Applikation oder ein entferntes Portal via PVP weiterreichen zu können, bedarf es über das PVP hinaus gehende Definitionen. Dieses Dokument soll diese festlegen, um sie dann später in ein erweitertes PVP Konzept zu integrieren.	
Autor(en):	Peter Pfläging	Projektteam / Arbeitsgruppe
		AG-IZ
Beiträge von:		

Einleitung

Das Portalverbundprotokoll (bis Version 1.9) ist auf die Bedürfnisse einer Organisationskommunikation ausgerichtet. So geht das Protokoll typischerweise von Organisationszugehörigkeiten aus. Genauso wird auch in fast allen Fällen von einer expliziten Berechtigungsvergabe ausgegangen.

Ein weiterer Unterschied zwischen der Kommunikation von Organisationen untereinander im Gegensatz zu Kommunikation von Bürgerportalen ist auch, dass in der Kommunikation zwischen den Portalen nicht der besondere Schutz der Personendaten gilt, der heute im DSGVO und in der Bereichsabgrenzungsverordnung für den Bürger zu beachten ist.

Keine Beachtung wird in diesem Dokument der Tatsache gegeben, dass auch andere Einstufungen im Sicherheitsbereich für Bürger gegenüber Organisationen zu treffen sind¹.

PVP für Bürgerportale

Prinzipiell ist PVP (Version ab 1.8.9) für Bürgerportale ohne weiteres geeignet. Man sollte nur auf folgendes achten:

1. PVP 1.x ist ein „Reverse Proxy“ Protokoll. Das bedeutet, dass der Bürger bei der Verwendung einer Applikation, die nicht im eigenen Portal liegt, nicht umgeleitet wird, sondern die Fremdapplikation in das Portal eingebettet wird. Daher sollte man auch beim Layout auf einheitliche Sichten achten.
2. Einige Definitionen aus dem PVP-Token sind für Bürger nicht anwendbar und sollten daher mit sinnvollen Einheitswerten gefüllt werden, sofern sie verpflichtende Attribute sind. Diese Attribute nicht zu befüllen würde das Protokoll verletzen.
3. Es muss klar sein, dass ein Stammportal für Bürger, welches mehrere Bereiche nach Bereichsabgrenzungsverordnung bedient, keinerlei Informationsverknüpfung zwischen den Bereichen und der Person verspeichern darf.
4. Theoretischerweise müssen Bürger, welche sich an allgemeinen Verfahren beteiligen (d.h. Verfahren ohne explizite Berechtigungen) nicht im Portal verspeichert werden. Hier werden die Login Daten (z.B.: die Daten, welche über MOA-ID) erfasst werden, nur in den PVP-Token überführt und anschließend weiterversendet.
5. Sollte im Gegenzug eine explizite Berechtigung notwendig sein, so wäre der Benutzer in der Portalverwaltung pro Bereich einmal anzulegen. Auf

¹ Eine Erweiterung der geltenden Regeln aus SecClass 2.1 erfolgt an anderer Stelle.

diese Weise kann man die Kombination Bürger+Bereich für eine Applikation berechtigen, es findet aber kein „sammeln“ von Bereichen statt. Als Nachteil muss allerdings auch angemerkt werden, dass damit im schlechtesten Fall der Benutzer 37 mal (=Anzahl der Bereiche) im System existiert.

Beispiel für einen PVP 1.9 konformen Request


```
POST /at.gv.abc.anwendung1/citizen HTTP/1.1
Host: awp.abc.gv.at
Accept-Encoding: gzip, deflate
User-Agent: Mozilla (5.0 Linux)
X-Version: 1.9
X-AUTHENTICATE-participantId: AT
X-AUTHENTICATE-cn: Peter Pfläging
X-AUTHENTICATE-gvOuid: AT
X-AUTHENTICATE-gvSecClass: 1
X-AUTHENTICATE-gvGid: none
X-AUTHENTICATE-mail: peter@pflaeging.net
X-AUTHENTICATE-tel: 0
X-AUTHENTICATE-bpk:
vbPK:c1tWDirXH3BQ95bUKNUXFaxKoY4o1t01n59XwE2WCgsSujAEWslYQmn5rEZVNfBkjjqdGIcOORN
2sbi8PSQS+3h131e7uO+U2KoXA/jN3VwESLA1I0sbabTUCHY1nBz1ublLrjCyI/sJ0uDLw8UQNEbhChZ
pwKCPSSp9thLzKQI=
X-AUTHORIZE-roles: No_Role
Content-Type: application/x-www-form-urlencoded
Content-Length: 788
```

Erklärung:

Headerfeld	Erklärung
X-AUTHENTICATE-participantId	Ein Bürger ist keinem expliziten Participant zugeordnet, daher sollte hier der Nation Code stehen. In unserem Fall also erst einmal AT
X-AUTHENTICATE-cn	Der Common Name (muss natürlich NICHT eineindeutig sein)
X-AUTHENTICATE-gvSecClass	Kann nur 1 sein (nach SecClass 2.1): Der Bürger kommt vielleicht mit Wissen und Besitz (BKU) aber nicht von einem gemanagten Gerät. Daher kann er seine eigenen Personenbezogenen Daten manipulieren, aber nicht mehr
X-AUTHENTICATE-gvGid	Hier sollte für den Bürger ein fixer Eintrag „none“ stehen. Die Eineindeutigkeit eines Bürgers wird über sein verschlüsselte bPK erreicht (siehe Feld: X-AUTHENTICATE-bpk).
X-AUTHENTICATE-mail	Kann „null“ sein, oder eine gültige e-Mail Adresse.

X-AUTHENTICATE-tel	Ist typischerweise „0“ (notwendig, daher Pflichtfeld in PVP 1.9)
X-AUTHENTICATE-bpk	Hier steht die verschlüsselte bPK nach PVP 1.9
X-AUTHORIZE-roles	Wir befinden uns in einem allgemeinen Verfahren, daher wird typischerweise so etwas wie „No_Role“ hier eingetragen.

Informationen zur Signatur

	Unterzeichner	CN=Peter Pflaeging, OU=MA 14, O=Stadt Wien, C=AT
	Datum/Zeit	Tue Nov 03 16:21:53 CET 2009
	Austeller-Zertifikat	CN=Stadt Wien CA Benutzer, O=Stadt Wien, C=AT
	Serien-Nr.	235
	Methode	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signatur)
Hinweis	Diese Signatur kann überprüft werden, wenn Sie das Dokument mit dem Adobe Reader öffnen!	